ROGA und LOPA.

Ein Vergleich zweier Methoden zur Risikobewertung von chemischen Prozessanlagen.

Sonderdruck aus TÜ, Technische Überwachung, Ausgabe 9 (2010)

www.tuv.com

TÜVRheinland®
Genau. Richtig.

Technische Überwachung
Anlagensicherheit · Arbeits- und Gesundheitsschutz · Umweltschutz

Sonderdruck aus Technische Überwachung, Ausgabe 9/2010

ROGA und LOPA – ein Vergleich zweier Methoden zur Risikobewertung von chemischen Prozessanlagen

Franz-Josef Bock, Klaus Haferkamp und Andreas Häberlein, Köln

Der nachfolgende Beitrag beschäftigt sich mit zwei Vorgehensweisen zur Durchführung von Gefahrenanalysen für chemische Prozessanlagen, wenn u. a. der Safety Integrity Level (SIL) für PLT-Schutzeinrichtungen festgelegt werden soll. Neben der Darstellung der ROGA- und der LOPA-Methode werden ihre grundlegenden Gemeinsamkeiten sowie ihre Unterschiede beschrieben.

Die Anforderungen an PLT-Schutzeinrichtungen werden in der DIN EN 61508/61511 [1] definiert. Zur Ermittlung der Qualität der Anforderungen an diese Schutzeinrichtungen ist die Bestimmung des erforderlichen Sicherheits-Integritäts-Levels (SIL) von besonderer Bedeutung.

Layer of **P**rotection **A**nalysis (LOPA) [2] ist ein etabliertes Werkzeug, mit dem für eine vorgegebene Gefahrenquelle das mit ihr verbundene Risiko abgeschätzt, Schutzebenen ermittelt und ihre Wirksamkeit bewertet und mit vorgegebenen Risiko-Toleranz-Kriterien verglichen werden kann. Die von den Autoren entwickelte und publizierte **R**isiko**O**rientierte **G**efahren**A**nalyse (ROGA) [3] dient der integrierten Bewertung des Arbeitsschutzes, der Anlagensicherheit beim Betreiben von Anlagen und des Schutzes der Umgebung der Anlage. Diese Methode umfasst die Ermittlung der Gefahrenquellen, die in einer Prozessanlage wirksam werden können sowie, ausgerichtet an den Anforderungen der Störfall-Verordnung, deren Risikobewertung in Form von Risikoklassen *RK*. Für diese Gefahrenquellen werden die seitens des Betreibers getroffenen technischen und organisatorischen Maßnahmen eruiert und mit Verfügbarkeitsklassen *ZK* bewertet.

LOPA – Layer of Protection Analysis

Bei LOPA handelt es sich um eine semi-quantitative Methode, mit der für vorgegebene Gefahrenquellen das mit ihnen verbundene Risiko abgeschätzt werden kann und bewertet wird, ob die in einer chemischen Prozessanlage installierten Schutzebenen bestimmte vorgegebene Risiko-Toleranz-Kriterien erfüllen. Die Durchführung einer LOPA beginnt mit der Auswahl eines unerwünschten Ereignisses (Brand, Explosion, Stofffreisetzung), das z. B. aufgrund einer vorausgegangenen HAZOP-Analyse oder einer anderen qualitativen Gefahrenanalyse ermittelt wurde. Für diese Gefahrenquelle wird das mit ihr verbundene Risiko abgeschätzt. Dann werden unabhängige Schutzebenen zur Beherrschung des Ereignisses identifiziert und evaluiert. Die erforderliche Qualität der Schutzebenen wird auf der Grundlage einer vorgegebenen Risikotoleranz festgelegt.

Die Durchführung einer LOPA erfolgt im Team. Dabei sind die Teilnehmer im Wesentlichen dieselben wie die bei einer vorausgehenden HAZOP-Studie. Das Team legt auch fest, für welche der in der HAZOP-Studie ermittelten Gefahrenquellen eine LOPA durchgeführt wird.

Bei der Erstellung einer LOPA für eine ausgewählte Gefahrenquelle, ein festgelegtes Ereignis, werden folgende Schritte durchlaufen:

Schritt 1: Identifizierung der Auswirkungen, um die mit der Gefahrenquelle, dem Ereignis, verbundenen Szenarien zu beschreiben. Im Anschluss an die Datenerhebung im Rahmen der Gefahrenanalyse werden für die ausgewählten Gefahrenquellen Szenarien gebildet und ihre Auswirkungen aufgezeigt. Die Auswirkung einer Gefahrenquelle wird hinsichtlich ihres Ausmaßes bewertet, je nach Vorgabe des Auftraggebers der Analyse z. B. die Größenordnung der Menge an freigesetzten Stoffen oder Energie. Dabei müssen Art und Tiefgang der Auswirkungsbetrachtungen mit den vereinbarten Risiko-Toleranz-Kriterien konsistent sein.

Schritt 2: Auswahl eines Szenariums. Die für die Gefahrenquelle ermittelten Szenarien werden, ausgehend von dem auslösenden Ereignis, mit allen für den Eintritt des Ereignisses erforderlichen Randbedingungen über das Versagen der Schutzebenen bis zu den ermittelten Auswirkungen beschrieben.

Schritt 3: Identifizierung der die Gefahrenquelle, das Ereignis, auslösenden Elemente und Festlegung ihrer Eintrittshäufigkeit. Die Gefahrenquelle, das auslösende Ereignis, muss unter Vernachlässigung aller Sicherheitsmaßnahmen zu der Auswirkung führen. Die Eintrittshäufigkeit muss die bekannten Aspekte des Prozesses und Hintergrundwissen berücksichtigen, die dem Schadensereignis und seiner Ursache zugrunde liegen. Sie wird vom Team festgelegt. Hierbei ist die Erfahrung der Teammitglieder besonders wichtig. Die Eintrittshäufigkeit wird in Ereignissen pro Jahr angegeben.

Schritt 4: Identifizierung der unabhängigen Schutzebenen – Independent Protection Layer (IPL) und Bestimmung der Ausfallwahrscheinlichkeit im Anforderungsfall. Die Ermittlung der Schutzmaßnahmen, die den Anspruch an eine unabhängige Schutzebene (IPL) erfüllen, ist das Herzstück der LOPA-Methode. Grundlagen für die Ableitung von unabhängigen Schutzebenen sind:

- die Auslegung des Verfahrens,
- das betriebliche Steuerungssystem (mit Einschränkungen),
- kritische Alarme und (alarmausgelöste) Bedienungsaktionen,
- sicherheitsgerichtete Steuerungen,
- technische störungsverhindernde Maßnahmen,
- technische störungsbegrenzende Maßnahmen.

In die LOPA-Analyse werden darüber hinaus auch die Schutzebenen aufgenommen, die nicht als IPL deklariert werden können. Allgemein werden unter nicht unabhängigen Schutzebenen technische Einrichtungen oder organisatorische Maßnahmen verstanden, die in Wechselwir-

kungen mit anderen Schutzebenen stehen. Sie werden bei der Risikobewertung nicht berücksichtigt.

Die Unternehmen geben Werte für die Ausfallhäufigkeit von IPL vor, aus denen der Wert ausgewählt werden kann, der dem Szenarium am ehesten entspricht. Jede IPL und ihre zugehörige Ausfallhäufigkeit (Ausfälle je Anforderung und Jahr) werden dokumentiert.

Schritt 5: Abschätzung der mit dem Szenarium verbundenen Eintrittshäufigkeit unter Berücksichtigung der Wirksamkeit der Schutzebenen. In diesem Schritt wird die Eintrittshäufigkeit eines Szenariums unter Einbeziehung der unabhängigen Schutzebenen betrachtet. Sie wird mathematisch ermittelt unter Einbeziehung der jeweils ermittelten Ausfallwahrscheinlichkeiten der IPL (s. Schritt 4) und der Eintrittshäufigkeit der Gefahrenquelle ohne Schutzebene (s. Schritt 3). Dieser Wert gibt also die Eintrittshäufigkeit eines Szenariums unter Einbeziehung aller Schutzebenen an.

Im LOPA-Verfahren werden aus der Erfahrung oder unter Bezug auf Dokumentationen nach Größenordnung geschätzte Werte verwendet, aber auch Indextabellen oder erfahrungsbasierte grafische Methoden.

Schritt 6: Abschließende Bewertung des mit dem Szenarium verbundenen Risikos. Bei der abschließenden Risikobewertung wird festgestellt, ob die Eintrittshäufigkeit unter Berücksichtigung der Schutzebenen unterhalb des tolerierbaren Risikos liegt. Ist dies der Fall, sind keine weiteren Schutzmaßnahmen notwendig. Sollte die Eintrittshäufigkeit unter Berücksichtigung der Schutzebenen über der des tolerierbaren Risikos liegen, müssen weitere Schutzmaßnahmen getroffen werden, bis das tolerierbare Risiko erreicht ist oder unterschritten wird.

ROGA – Risikoorientierte Gefahrenanalyse

Bei dem ROGA-Verfahren handelt es sich um eine von den Autoren entwickelte semiquantitative Methode zur Risikobeurteilung von chemischen Prozessanlagen. Es ist in zwei Teile gegliedert, die deduktive Gefahrenanalyse und die Bewertung, ob die ermittelten sicherheitsrelevanten Maßnahmen dem Stand der Sicherheitstechnik entsprechen, und i. d. R. als semiquantitative Risikoermittlung und -bewertung durchgeführt.

Die im ROGA-Verfahren angewandte deduktive Gefahrenanalyse wurde in mehreren vom Umweltbundesamt und von dem VdTÜV geförderten Forschungsvorhaben entwickelt [4 bis 7]. Durch die aus dem Begriff des Störfalls abgeleitete deduktive Vorgehensweise können die von einer Anlage potenziell ausgehenden Gefahrenquellen in Form einer Fehlerbaumstruktur dargestellt werden. Als Gefahrenquellen werden hier die Zustände oder Ereignisse in einer Anlage bezeichnet, bei denen ein Stoff aufgrund von nicht angemessener technischer Ausführung und/oder Organisation der Bedienung unmittelbar die Einschließung verlassen kann. Für diese direkt auf die Ausführung und Bedienung einer Anlage bezogenen Gefahrenquellen wird dabei als ergänzendes Gliederungsprinzip die Unterscheidung hinsichtlich

- der Ausführung der Komponenten,
- der Steuerung der Anlage und
- der Bedienung durch den Menschen

gewählt.

Unter Bezugnahme auf diese Gefahrenquellen werden dann die in der Anlage zu treffenden störfallverhindernden und -auswirkungsbegrenzenden Maßnahmen identifiziert.

Der zweite Teil ermöglicht es, mit vertretbarem Aufwand das Risiko des mit dem Wirksamwerden einer Gefahrenquelle verbundenen Gefahrenpotenzials und die Verfügbarkeit der Gegenmaßnahmen abzuschätzen.

Die Bewertung von sicherheitsrelevanten Maßnahmen entsprechend ihrer Zuverlässigkeit und, eingebunden in den Betrieb der Anlage, ihrer Verfügbarkeit, orientiert sich an den in der deutschen Normgebung zu PLT-Schutzeinrichtungen entwickelten Grundzügen, wie sie auch in die DIN EN 61508 eingeflossen sind. Auf der Grundlage ihres Ausfallverhaltens werden die in einer Anlage vorhandenen sicherheitsrelevanten technischen und organisatorischen Maßnahmen entsprechend dem Stand der Sicherheitstechnik und den Betriebserfahrungen mit Verfügbarkeitsklassen bewertet.

Die Ermittlung und Bewertung des mit einer Gefahrenquelle verbundenen Risikos erfolgt mithilfe des Risikografen, wie er in der Normung zur Bewertung von PLT-Schutzeinrichtungen eingeführt [8] und prinzipiell von *Jochum* [9] weiterentwickelt wurde. Dieser Risikograf wird herangezogen, um die Gesamtheit der Maßnahmen zur Beherrschung einer Gefahrenquelle zu bewerten. Mithilfe des Risikografen wird jeder Gefahrenquelle eine Risikoklasse zugeordnet.

Die Sicherheit der Anlage gegen das Wirksamwerden einer Gefahrenquelle ist gegeben, wenn die Risikoklasse des mit der Gefahrenquelle verbundenen Gefahrenpotenzials durch die Verfügbarkeitsklasse der Maßnahmenkette zu ihrer Beherrschung mindestens erreicht wird.

Beide Schritte zur Durchführung der Gefahrenanalyse nach ROGA erfolgen üblicherweise in einem Arbeitsschritt, können aber auch getrennt durchgeführt werden.

Zum Vergleich der verschiedenen sicherheitstechnischen Maßnahmen untereinander verwendet das ROGA-Verfahren wie bereits erwähnt eine semiquantitative Vorgehensweise zu ihrer Klassifizierung. Analog zu den Risikoklassen gibt es acht Verfügbarkeitsklassen. Die Verfügbarkeitsklasse gibt an, wie zuverlässig die Schutzmaßnahme beim Wirksamwerden einer Gefahrenquelle funktioniert. Der Wert der Verfügbarkeitsklasse einer Schutzmaßnahme entspricht dem Betrag des Logarithmus ihrer Ausfallwahrscheinlichkeit. Details hierzu sind in einer früheren Publikation beschrieben [3].

Aus der Anwendung des ROGA-Verfahrens auf chemische Prozessanlagen haben sich folgende Erkenntnisse ergeben:

Das ROGA-Verfahren ist geeignet, Gefahrenanalysen gemäß den Anforderungen der Störfall-Verordnung [10] durchzuführen und eine Klassifizierung von PLT-Schutzeinrichtungen zu ermöglichen.

Im ROGA-Verfahren wird mithilfe des Risikografen nicht nur das von einer PLT-Schutzmaßnahme abzusichernde Teilrisiko, sondern das Gesamtrisiko beim Wirksamwerden einer Gefahrenquelle betrachtet. Durch den Einsatz von PLT-Schutzeinrichtungen kann u. U. nur ein Teil des von einer Betrachtungseinheit ausgehenden Risikos reduziert werden. Daher werden alle Schutzmaßnahmen (PLT-Schutzeinrichtungen und Nicht-PLT-Schutzeinrichtungen) in die Bewertung mit einbezogen.

Die Nicht-PLT-Schutzeinrichtungen können technischer und nichttechnischer (z. B. organisatorischer) Art sein und sich gegenseitig ergänzen oder ersetzen, d. h. die Sicherheit des Systems kann durch verschiedene gleichwertige Wege erreicht werden. So kann beispielsweise eine Lösung mit einem hohen Anteil technischer Maßnahmen einer Lösung mit geringerem Anteil technischer Maßnahmen aber einem entsprechend höheren Anteil nichttechnischer Maßnahmen gleichwertig sein. Die schematische Visualisierung dieser Sachverhalte zeigt **Bild 1**.

Da beim ROGA-Verfahren sämtliche Größen des Systems (apparative Ausrüstung, Steuerung, menschlicher Eingriff)

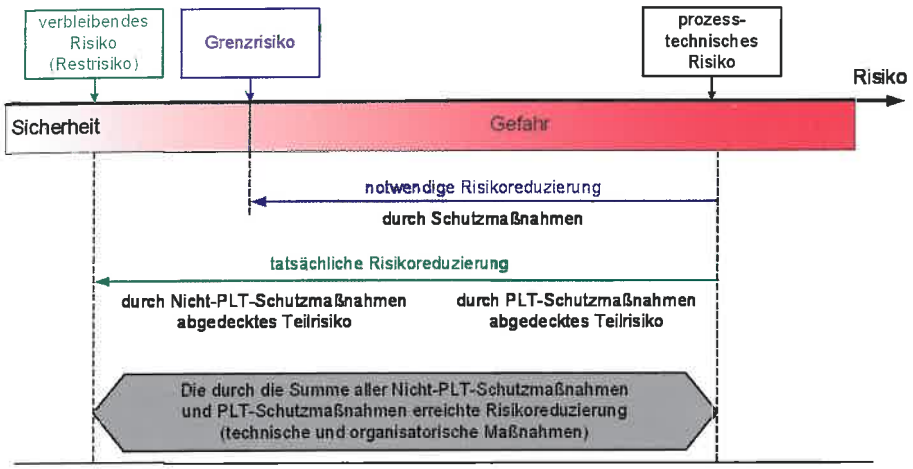


Bild 1 *Risikoreduzierung durch PLT- und Nicht-PLT-Schutzmaßnahmen.*

einbezogen werden, kann dieses Verfahren generell auf Mensch-Maschine-Systeme angewendet werden. Durch die Gegenüberstellung von Risiko- und Verfügbarkeitsklassen ist die Dokumentation der Ergebnisse übersichtlich und bietet eine überschaubare logische Darstellung des Erfüllungsgrads der Sicherheitsanforderungen an die Anlage. Ferner bewirkt die Bewertung mit Verfügbarkeitsklassen eine zusätzliche Kontrolle der störfallverhindernden Maßnahmen, indem überprüft wird, ob sie in sich geschlossen und unabhängig sind.

Der Einsatz des ROGA-Verfahrens bedingt eine Klassifizierung sämtlicher relevanter Anlagenkomponenten in Verfügbarkeitsklassen, die mit einem Zeit- und Arbeitsaufwand verbunden ist. Daher eignet sich die semiquantitative Risikobewertung anhand des ROGA-Verfahrens i. d. R. nur für Betreiber von Anlagen, die der Störfall-Verordnung unterliegen. Die Anwendung des Risikografen selber ermöglicht eine sehr zügige Durchführung der Risikobewertung, da Risiko- und Verfügbarkeitsklassen schnell ermittelt werden können.

Zielsetzung des ROGA-Verfahrens ist die Bestimmung des in einer Anlage durch das Wirksamwerden einer Gefahrenquelle auftretenden Gesamtrisikos, einhergehend mit der Bewertung aller zur Beherrschung dieses Risikos getroffenen Maßnahmen. Dabei erfolgt die Risikoreduzierung sowohl durch PLT- als auch durch Nicht-PLT-Schutzmaßnahmen.

Die Bestimmung des Risikos erfolgt unter der Annahme, dass keine passiven und/oder PLT-Schutzeinrichtungen in der Prozessanlage installiert wurden. Der Bezugspunkt für die Wahl des Schadenausmaßes bei einer Verletzung, einer Gesundheitsschädigung oder Tod von Personen ist das Erreichen der Grenze ab der dies erfolgen kann. Die definierten Risikoklassen bestimmen die Qualität der Maßnahmen, mit denen das ermittelte Risiko unter das Grenzrisiko reduziert wird.

Vergleich zwischen *ROGA* und *LOPA*

Verfahren zur Ermittlung der Gefahrenquellen – Identifizierung der Auswirkungen von Ereignissen

Beim ROGA-Verfahren handelt es sich um ein qualitatives Gefahrenanalyse-Tool in das bei Bedarf ein Bewertungstool integriert werden kann, wohingegen LOPA lediglich aus einem Bewertungstool besteht.

Die in LOPA erzielten Ergebnisse hängen sehr stark von der verwendeten Methode ab, mit der die zu untersuchenden Ereignisse und die erforderlichen Schutzmaßnahmen ermittelt werden. Im Gegensatz zu LOPA ist das Bewertungstool bei ROGA von der Wahl der Gefahrenanalysemethode (PAAG, Checkliste,...) unabhängig. Es ist ein Ansatz, mit dem die Vorgaben des Gesetz- und Verordnungsgebers, die ein tolerierbares Risiko beschreiben, auf das reale Verhalten technischer Anlagen abgebildet werden kann.

Kriterien des tolerierbaren Risikos

Die Annahmen für die Festlegung der zulässigen Risiken sind in LOPA weitgehend betreiberspezifisch; betreiberübergreifende Festlegungen sind bisher nicht bekannt.

Die Festlegung der Risiko-Toleranz-Kriterien, die als Grundlage einer LOPA-Studie bekannt sein müssen, gehört nicht zum LOPA-Verfahren, sondern erfolgt vorab durch den Veranlasser der LOPA-Studie. Die festgelegten Risiko-Toleranz-Kriterien bestimmen z. B. Art und Tiefgang der Auswirkungsbetrachtungen. Beispiele aus ausgeführten Studien sind:

- freigesetzte Menge von Stoffen, Aggregatzustand, gefährliche Eigenschaft ohne direkten Bezug auf die Schädigung von Menschen,
- Abschätzung der Anzahl möglicher Verletzter/Toter,
- Abschätzung von Verletzten/Toten mit ergänzenden Randbedingungen aus dem Ausbreitungsverhalten des Stoffs nach Freisetzung,
- Ermittlung der Anzahl von Verletzten/Toten aufgrund einer detaillierten Auswirkungsbetrachtung.

Das Ergebnis einer LOPA-Studie ist also nicht allgemeingültig, sondern von den gewählten Risiko-Toleranz-Kriterien abhängig.

Bezüglich der Festlegung des tolerierbaren Risikos ist die ROGA-Methode konservativer als die LOPA-Methode. In ROGA wird das Risiko konsequent als Grenzwert formuliert, bis zu dem noch keine Schäden im Sinne der Störfall-Verordnung aufgetreten sind; die Festlegung des Risikos in der ROGA-Methode ist im Vergleich zu LOPA somit stringenter.

Wenn die Qualität von sicherheitsrelevanten Tätigkeiten, die in der chemischen Prozessanlage zum Einsatz kommen, im Vergleich zum tolerierbaren Risiko als nicht ausreichend sicher gilt, werden bei beiden Methoden eine höhere Verfügbarkeit oder ergänzende Maßnahmen gefordert. Ziel ist, das Risiko zu minimieren.

Identifizierung der das Ereignis auslösenden Elemente und Festlegung der Eintrittshäufigkeit

Die Identifizierung der das Ereignis auslösenden Elemente erfolgt in LOPA als eigenständiger Schritt. Hieraus folgend wird die Eintrittshäufigkeit des auslösenden Ereignisses festgeschrieben. In ROGA erfolgt aufgrund der Struktur der deduktiven Gefahrenanalyse die Identifizierung der Gefahrenquelle und der sie auslösenden Elemente in einem Arbeitsschritt. Die Auffindung ist unabhängig vom verwendeten Verfahren zur Ermittlung der Gefahrenquellen (s.o.).

Die Festlegung der Eintrittshäufigkeit für die das Ereignis auslösenden Elemente wird in LOPA vom Team vorgenommen. Dabei werden betreiberspezifische Erfahrungen berücksichtigt.

In ROGA wird die Abschätzung des mit dem Wirksamwerden einer Gefahrenquelle verbundenen Risikos durch das Gefahrenanalyse-Team anhand der vier Parameter des Risikografen geführt:

- der durch das Schadensausmaß erfasste Bereich *S*,

- die Häufigkeit *A* mit der sich Personen im Bereich *S* aufhalten,
- das Vorhandensein und die Wirksamkeit *G* das Schadensereignis zu erkennen und seine Auswirkungen auf das betroffene Objekt (Person/Umwelt) auf ein erträgliches Maß zu begrenzen und
- die Häufigkeit *W*, mit der die Ursache für das Eintreten der Gefahrenquelle in der Anlage gegeben ist, gemessen an der Anzahl der erforderlichen Fehlzustände.

Ergebnis ist das mit dem Wirksamwerden der Gefahrenquelle verbundene Risiko, dargestellt als Risikoklasse als Funktion von vier Parametern [3]:

$$RK(X_j) = RK(X_j)\,[S_k, A_m, G_m, W_n] \quad (1)$$

$k = 1$ bis 4, $m = 1$ bis 2, $n = 1$ bis 3

X_j ist der Zahlenwert der Risikoklasse *RK* der Gefahrenquelle *j*. Die Festlegung der Eintrittswahrscheinlichkeit eines Ereignisses ist in *ROGA* somit Bestandteil der Bestimmung der Risikoklasse.

Die Risikoparameter sind dem Verhalten der schadensbestimmenden Größe, hier dem freigesetzten Stoff, angepasst und so definiert, dass sie nach einiger Erfahrung für die zu betrachtenden Gefahrenquellen hinreichend schnell ermittelt werden können. Dabei berücksichtigen die Parameter Größen, die zum einen hinsichtlich des tolerierbaren Risikos aus der Störfall-Verordnung abgeleitet werden können, zum anderen spiegeln sie hinsichtlich des tatsächlich vorhandenen Risikos das Verhalten der Anlage wider.

Damit zeigt sich, dass die Ereigniswahrscheinlichkeiten in ROGA mit den Annahmen, die in LOPA getroffen werden, nicht konsistent sind.

Identifizierung der Independent Protection Layer (IPL) und Bestimmung der Ausfallwahrscheinlichkeit im Anforderungsfall

Bei der Betrachtung von risikobehafteten Vorgängen stellt sich sehr häufig die Frage nach quantifizierbaren Ausfallwahrscheinlichkeiten für IPL. Dies ist bei der Beurteilung von Chemieanlagen umso schwieriger, da für das in derartigen Anlagen verwendete Equipment und das jeweils spezifische Umfeld der Anlage kaum statistisch signifikante und reproduzierbare Daten bezüglich Ausfall- bzw. Fehlerraten vorliegen. ROGA und LOPA sollen die Basis für klare Entscheidungen bezüglich der Spezifikation von IPL liefern. Im LOPA-Verfahren nach [2] wird bei der Festlegung von Ausfall- bzw. Fehlerraten auf allgemeine Datensammlungen, Unterlagen des Anlagenbetreibers und die Erfahrung des Teams verwiesen. Das macht eine allgemein verbindliche Zuweisung von Ausfallwahrscheinlichkeiten schwierig.

Im ROGA-Verfahren werden zur Ermittlung der Zuverlässigkeiten/Verfügbarkeiten der relevanten technischen und organisatorischen Maßnahmen die Maßnahmen verschiedener Kategorien, ergänzend hinsichtlich ihrer Zuverlässigkeit, untereinander verglichen. Die Ausfallwahrscheinlichkeit P_i einer Maßnahme i wird einer Verfügbarkeitsklasse $ZK(Y_i)$ entsprechend Gl.(2) zugeordnet.

$$ZK(Y_i) = -\log P_i \quad (2)$$

$$P_i = 10^{-Y_i}$$

Dabei ist Y_i der Zahlenwert der Verfügbarkeitsklasse *ZK* der Maßnahme *i*. Das bedeutet, dass durch Zuordnung einer Maßnahme zu einer Verfügbarkeitsklasse ihre Ausfallwahrscheinlichkeit mit einem Streubereich um den Faktor 10 abgeschätzt wird. Der so definierte Streubereich entspricht z. B. dem der Sicherheitsniveaus (SIL) der DIN EN 61508 [1].

Sowohl die LOPA- als auch die ROGA-Methode gestatten die Festlegung von SIL-Klassen für PLT-Schutzeinrichtungen. Die Ermittlung der SIL-Klassen erfolgt in LOPA in Abhängigkeit von der Festlegung der zulässigen Risiken durch den Betreiber. Bei der ROGA-Methode folgt die Ermittlung der SIL-Klassen von PLT-Schutzeinrichtungen den gesetzlich vorgegebenen Risiko-Toleranz-Größen, da sie sich an den Maßgaben der Störfall-Verordnung orientiert. Diese Maßgaben werden bisher bei der LOPA-Methode nicht berücksichtigt. Aufgrund dieses Sachverhalts hat die LOPA-Methode in ihrer Anwendung gegenüber der ROGA-Methode – zumindest in Deutschland – einen deutlichen Nachteil. Insgesamt kann jedoch festgestellt werden, dass die Bewertung der IPL in LOPA konsistent ist mit der in ROGA; beide Methoden sind konform mit der DIN EN 61508/61511.

Abschätzung der Eintrittshäufigkeit des Ereignisses mit Wirksamkeit der Schutzebenen durch Anwendung mathematischer Methoden und Bewertung des Risikos

In LOPA wird das mit dem betrachteten Ereignis verbundene Risiko als Produkt der Ausfallwahrscheinlichkeiten der IPL und der Eintrittshäufigkeit des Szenariums dargestellt. Man erhält einen Wert, anhand dessen Aussagen über die Eintrittshäufigkeit eines Szenariums möglich sind, wenn alle unabhängigen Schutzebenen gleichzeitig versagen.

In der ROGA-Methode werden den Maßnahmen jeweils nach ihrer Ausführung und Eignung Verfügbarkeitsklassen *ZK* zugeordnet. Insgesamt wird gefordert, dass die Summe der Verfügbarkeitsklassen $ZK(Y_i)$ der Maßnahmen *i* (Verfügbarkeitsklasse der Maßnahmenkette) mindestens der für die Gefahrenquelle *j* ermittelten Risikoklasse $RK(X_j)$ entspricht (Gl.3).

$$RK(X_j) \le \sum_i ZK(Y_i) \quad (3)$$

Bei dieser Vorgehensweise werden sowohl die technischen als auch die organisatorischen sicherheitstechnisch relevanten Maßnahmen in Form einer Maßnahmenkette bewertet.

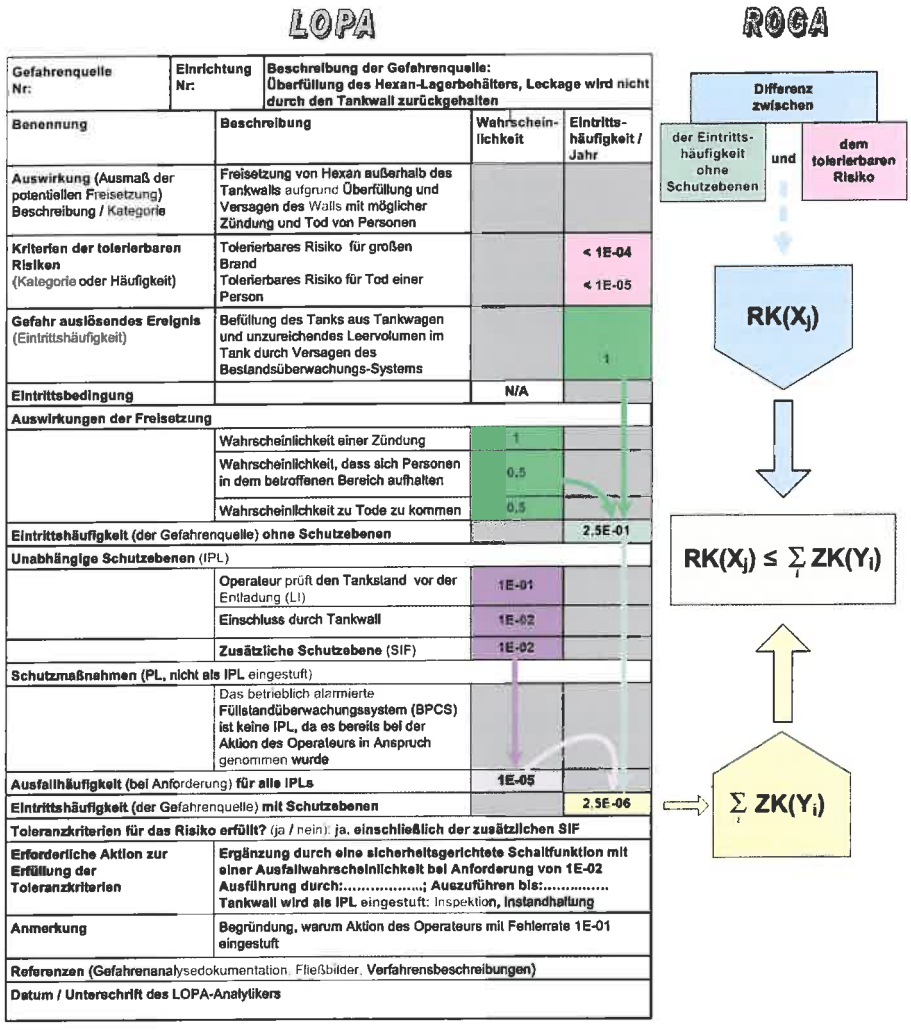
Die formale Zuordnung der in ROGA definierten Risiko- und Verfügbarkeitsklassen zu den in LOPA verwendeten Begriffen ist in **Bild 2** aufgezeigt.

Bei Ausfall von Betriebsüberwachungseinrichtungen (**b**asic **p**rocess **c**ontrol **s**ystem, BPCS) stehen keine Funktionen und Alarme dieses Systems mehr zur Verfügung. Ein wesentlicher Nachteil in LOPA ist die Tatsache, dass MSR-Schutzeinrichtungen durch mehrere Betriebsüberwachungseinrichtungen ersetzt werden können. Dies ist in ROGA nicht erlaubt, denn nach den in diesem Verfahren festgelegten Grundsätzen für die Gestaltung sicherheitstechnischer Maßnahmenketten ist es nicht gestattet, eine MSR-Schutzeinrichtung durch eine Kombination von Betriebsüberwachungseinrichtungen zu substituieren.

Im Gegensatz zu LOPA wird in ROGA die technische Auslegung der Anlage als IPL definiert. Dies ist von Vorteil, ja sogar notwendig, um die Zuverlässigkeit der Auslegung der Anlage unter Berücksichtigung der Anforderungen des Regelwerks sicherheitstechnisch bewerten zu können.

Häufig in LOPA gemachte Fehler, die zu einer Fehlanwendung führen

LOPA ist wie bereits erwähnt ein leistungsfähiges Tool für die Erstellung einer semiquantitativen Risikobewertung. Gleichwohl muss erwähnt werden, dass im Rahmen der Erstellung einer LOPA-Risikoanalyse häufig Fehler auftreten können, die zu einer Überschätzung des Risikos im Sinne einer zu konservativen Betrachtung führen [11]. Damit verknüpft ist eine Überinstrumentierung der Prozessanlage einschließlich der damit verbundenen Kosten für den Lebenszyklus des PLT-Equipments. Eine nicht konservative Abschätzung des Risikos für das Eintreten eines Szenariums kann dagegen zu einer Unterbewertung der Sicherheitstechnik führen, was sich in einer mangelhaften Ausführung/Ausrüstung der Prozessanlage mit Schutzeinrich-



Gefahrenquelle Nr:	Einrichtung Nr:	Beschreibung der Gefahrenquelle: Überfüllung des Hexan-Lagerbehälters, Leckage wird nicht durch den Tankwall zurückgehalten		
Benennung		**Beschreibung**	**Wahrschein-lichkeit**	**Eintritts-häufigkeit / Jahr**
Auswirkung (Ausmaß der potentiellen Freisetzung) Beschreibung / Kategorie		Freisetzung von Hexan außerhalb des Tankwalls aufgrund Überfüllung und Versagen des Walls mit möglicher Zündung und Tod von Personen		
Kriterien der tolerierbaren Risiken (Kategorie oder Häufigkeit)		Tolerierbares Risiko für großen Brand Tolerierbares Risiko für Tod einer Person		< 1E-04 < 1E-05
Gefahr auslösendes Ereignis (Eintrittshäufigkeit)		Befüllung des Tanks aus Tankwagen und unzureichendes Leervolumen im Tank durch Versagen des Bestandsüberwachungs-Systems		1
Eintrittsbedingung			N/A	
Auswirkungen der Freisetzung				
		Wahrscheinlichkeit einer Zündung	1	
		Wahrscheinlichkeit, dass sich Personen in dem betroffenen Bereich aufhalten	0,5	
		Wahrscheinlichkeit zu Tode zu kommen	0,5	
Eintrittshäufigkeit (der Gefahrenquelle) ohne Schutzebenen				2,5E-01
Unabhängige Schutzebenen (IPL)				
		Operateur prüft den Tankstand vor der Entladung (LI)	1E-01	
		Einschluss durch Tankwall	1E-02	
		Zusätzliche Schutzebene (SIF)	1E-02	
Schutzmaßnahmen (PL, nicht als IPL eingestuft)				
		Das betrieblich alarmierte **Füllstandüberwachungssystem (BPCS) ist keine IPL, da es bereits bei der Aktion des Operateurs in Anspruch genommen wurde**		
Ausfallhäufigkeit (bei Anforderung) für alle IPLs			1E-05	
Eintrittshäufigkeit (der Gefahrenquelle) mit Schutzebenen				2,5E-06
Toleranzkriterien für das Risiko erfüllt? (ja / nein): **ja, einschließlich der zusätzlichen SIF**				
Erforderliche Aktion zur Erfüllung der Toleranzkriterien		**Ergänzung durch eine sicherheitsgerichtete Schaltfunktion mit einer Ausfallwahrscheinlichkeit bei Anforderung von 1E-02** **Ausführung durch:.....; Auszuführen bis:.....** **Tankwall wird als IPL** eingestuft: Inspektion, **Instandhaltung**		
Anmerkung		**Begründung, warum Aktion des Operateurs mit Fehlerrate 1E-01 eingestuft**		
Referenzen (Gefahrenanalysedokumentation, Fließbilder, Verfahrensbeschreibungen)				
Datum / Unterschrift des LOPA-Analytikers				

Bild 2 *Formale Zuordnung der in ROGA festgelegten Risiko- und Verfügbarkeitsklassen zu den in LOPA verwendeten Elementen.*

tungen äußern kann. Typische Fehler, die bei Ausführung einer LOPA-Studie gemacht werden können sind:

- die Nichtbeachtung von organisatorischen Maßnahmen, die für den sicheren Betrieb der Prozessanlage erforderlich sind, auch wenn sie einer Qualitätskontrolle unterliegen,
- die Außerachtlassung von voneinander abhängigen Fehlern bei der MSR-technischen Ausführung von Messeinrichtungen und deren Signalverarbeitung,
- die Verwendung von statistischen Ausfallraten, die für die realen Beanspruchungen technischer Einrichtungen in der betrachteten Anlage nicht zutreffend sind,
- die Ignorierung von Zeitfaktoren – im Sinne der Bewertung der tatsächlichen Dauer der Betriebsphasen technischer Einrichtungen sowie im Sinne der zur Verfügung stehenden Zeit für alarmorientierte Handlungen seitens des Anlagenpersonals,
- die Nichtbeachtung von Betriebserfahrungen über Handlungsgewohnheiten von Operatoren,
- die unzureichende ganzheitliche Berücksichtigung des Einflusses von ergänzend geforderten IPL auf die Prozessanlage bzw. -anlagenabschnitte (Wechselwirkungen innerhalb des verfahrenstechnischen Ablaufs), da LOPA üblicherweise nicht in die eigentliche Gefahrenanalyse integriert ist.

Die Nichtberücksichtigung dieser Sachverhalte können in einer LOPA-Studie zu falschen Aussagen führen. In einer ROGA-Studie werden sie dagegen streng einbezogen, da aufgrund der Integration des ROGA-Bewertungsmechanismus in die Gefahrenanalyse, die identifizierten Gefahrenquellen, ihre Auswirkungen und die Gegenmaßnahmen systematisch erfasst werden. Näheres hierzu kann [3] entnommen werden.

Zusammenfassung

LOPA als semiquantitatives Verfahren zur Risikobewertung spricht im Zusammenhang mit dem von ihm verwendeten Risikobegriff von Ausfallwahrscheinlichkeiten und impliziert damit begrifflich, dass es sich um genau berechenbare Werte handelt. Tatsächlich werden aber im Rahmen der Bewertung durch das Team Häufigkeiten abgeschätzt. Der Schätzung werden verallgemeinerte Daten und insbesondere die Erfahrungswerte der Teammitglieder zugrunde gelegt. Dies bedeutet, dass eine Bewertung innerhalb des Spektrums der z. B. ingenieurtechnischen und/oder naturwissenschaftlichen Erfahrung des Teams erfolgt und ggf. komponenten- oder anlagenbezogene Aspekte unberücksichtigt bleiben, die nicht in den Erfahrungsbereich der Teammitglieder fallen. Dies kann dazu führen, dass bei LOPA-Studien durch verschiedene Teams z. B. gleichwertige Sicherheitsfunktionen in Anlagen oder Prozessen an verschiedenen Standorten unterschiedlich bewertet werden. Eine konsistente Bewertung von Schutzebenen verschiedener technischer Ausführungen, z. B. im Rahmen von unternehmensinternen Vorgaben, ist jedoch zwingend erforderlich. Die Tatsache, dass i. d. R. bei LOPA nicht experimentell ermittelte Werte sondern Schätzungen vorliegen, zeigt sich durch die Verwendung des Begriffs „Häufigkeit" statt „Wahrscheinlichkeit". Die Verwendung von statistisch nicht signifikanten Daten für die Festlegung von Ausfallraten kann in LOPA mithin zur Fehleinschätzung der Zuverlässigkeit von sicherheitstechnischen Maßnahmen in der betrachteten Anlage führen. Im Prinzip ist diese Fehleinschätzung auch in ROGA möglich, sie wird jedoch durch die Kontrolle anhand eines erfahrungsbasierten Katalogs von sicherheitstechnischen Maßnahmen und deren Kombinationen reduziert.

Die Anwendung des HAZOP-Verfahrens [12] in der üblichen Form als qualitative Analysemethode ermöglicht die quantitative Klassifizierung von PLT-Schutzeinrichtungen (SIL) nicht. Eine derartige Klassifizierung kann erst gewährleistet werden, wenn dem HAZOP-Verfahren ein Bewertungstool nachgeschaltet wird. Im Vergleich zu LOPA gestattet das ROGA-Verfahren in einem Schritt sowohl die Erstellung einer qualitativen Gefahrenanalyse als auch die Durchführung einer semiquantitativen Bewertung des Risikos und folglich die Klassifizierung von PLT-Schutzeinrichtungen in SIL-Klassen.

Durch die Gegenüberstellung von Risiko- und Verfügbarkeitsklassen ist die Form der Dokumentation in einer ROGA-Studie sehr übersichtlich und bietet eine überschaubare logische Veranschaulichung des Erfüllungsgrads von adäqua-

ten Schutzmaßnahmen. Ferner bewirkt die Bewertung der störfallverhindernden Maßnahmen mit Verfügbarkeitsklassen eine zusätzliche Kontrolle dieser Maßnahmen, da darin die Prüfung eingeschlossen ist, ob sie in sich geschlossen und unabhängig sind.

Bevor das ROGA-Verfahren eingesetzt werden kann, ist eine Klassifizierung sämtlicher relevanter Anlagenkomponenten in Verfügbarkeitsklassen notwendig. Die Festlegung der Verfügbarkeitsklassen beruht auf umfangreichen Erfahrungen, die wir bei der gefahrenanalytischen Behandlung von Prozessanlagen gewonnen haben sowie auf den Abstimmungen mit den durch den Betreiber der Anlage gemachten Erfahrungen.

Das Ergebnis einer ROGA-Studie ist unter Berücksichtigung der sonstigen sicherheitsrelevanten Maßnahmen in einer Anlage eine angemessene SIL-Klassifizierung der PLT-Schutzeinrichtungen. Der für die Anwendung des ROGA-Prozesses notwendige Zeitbedarf ist, da integriert in die Gefahrenanalyse, im Gegensatz zum Zeitaufwand, der für eine LOPA-Studie angesetzt werden muss, deutlich geringer.

Wenn die beiden Verfahren HAZOP und LOPA in einem gemeinsamen, aufeinander abgestimmten Analysegang durchgeführt werden, kann die Kombination dieser beiden Verfahren zeitlich und inhaltlich als weitgehend gleichwertig mit dem ROGA-Verfahren angesehen werden.

Sowohl das ROGA-Verfahren als auch die Kombination aus HAZOP- und LOPA-Verfahren sind nicht ausschließlich auf eine Klassifizierung von PLT-Schutzeinrichtungen ausgerichtet, sondern können generell zur Durchführung von Risikoanalysen angewendet werden.

Die Störfall-Verordnung fordert, dass Anlagen so erstellt und betrieben werden müssen, dass Störfälle vernünftigerweise ausgeschlossen werden können. Sollte dennoch ein Störfall eintreten, müssen dessen Auswirkungen begrenzt werden. Das bedeutet, dass i. d. R. störfallverhindernde und -auswirkungsbegrenzende Maßnahmen getrennt untersucht und insbesondere jeweils geschlossen als solche dokumentiert werden müssen. Diese Unterscheidung wird im LOPA-Verfahren nicht getroffen. Der Grund hierfür ist wahrscheinlich die Tatsache, dass das LOPA-Verfahren im amerikanischen Raum entwickelt wurde und dort oft zum Einsatz kommt. Das ROGA-Verfahren stellt dagegen eine gute Plattform dar, um den Nachweis zu erbringen, dass der Betreiber insgesamt ausreichende technische und organisatorische Maßnahmen getroffen hat, um den sicheren Betrieb seiner Anlage zu gewährleisten. Zudem ist das ROGA-Verfahren im Besonderen geeignet – und das ist der wesentliche Unterschied zu LOPA – , den Nachweis zu erbringen, dass der Betreiber seine Anlage den Anforderungen der Störfall-Verordnung entsprechend betreibt. Bei der Erstellung von Gefahrenanalysen für chemische Prozessanlagen sind daher die spezifischen Gegebenheiten der diskutierten Verfahren zu berücksichtigen. TÜ 914

Dr. rer. nat. **Franz-Josef Bock**,
B. Eng. **Andreas Häberlein**, TÜV Rheinland Industrie Service GmbH, Köln, Geschäftsfeld Chemieanlagen/Anlagensicherheit.
Dr.-Ing. **Klaus Haferkamp**, Köln, vormals TÜV Rheinland Industrie Service GmbH, Köln, Geschäftsfeld Chemieanlagen/Anlagensicherheit.

Die Autoren danken Frau D. Bock für ihre Unterstützung bei der grafischen Aufarbeitung und Erstellung der Bilder sowie für ihre Hilfe beim Korrekturlesen.

Literaturverzeichnis

[1] DIN EN 61508: Funktionale Sicherheit sicherheitsbezogener elektrischer / elektronischer/programmierbarer elektronischer Systeme, Teil 0: 2005, Teile 1-5: 2002, Teile 6-7: 2003, insbesondere DIN EN 61508-5: 2002 – Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität (safety integrity level). DIN EN 61511: Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie, Teile 1-3: 2005, insbesondere DIN EN 61511-3: 2005 – Anleitung für die Bestimmung der erforderlichen Sicherheits-Integritätslevel.

[2] Layer of protection analysis –Simplified process risk assessment. AIChE – Center for Chemical Process Safety of the American Institute of Chemical Engineers, New York 2001.

[3] *Bock, F.-J.; Haferkamp, K.; Mistele, J.; Shahvardian, A.*: ROGA – Eine neue Methode der risikoorientierten Gefahrenanalyse zur Erfüllung der Anforderungen der Störfall-Verordnung – Teil 1; TÜ 47 (2006) Nr. 10, S. 39-44 und Teil 2; TÜ 47 (2006) Nr. 11/12, S. 27-32. Presented at 13th International Symposium on Loss Prevention and Safety Promotion in the Process Industries, Bruges, Belgium 6-9 June 2010.

[4] *Jäger, P.; Haferkamp, K.*: A checklist for the systematic examination of storage and production facilities with high risk potenzial. 7th International Symposium on Loss Prevention and Safety Promotion in the Process Industries. Taormina, Italy 4-8 May 1992.

[5] *Haferkamp, K.; Hein, M.; Rudolph, E.; Wietfeld, P.*: Ermittlung des aktuellen Standes der Sicherheitstechnik und der Lücken im Bereich der Sicherheitsvorschriften für Anlagen, die der StörfallV unterliegen, Bd. 1 bis 3, UFO-PLAN Nr. 10409212, Berlin 1987.

[6] VdTÜV Forschungsbericht Nr. 315: Aufstellen eines Leitfadens zur Erstellung und Prüfung von Sicherheitsanalysen nach § 7 Störfall-Verordnung; insbesondere Teil 6: TÜV Rheinland, TÜV Norddeutschland, TÜV Südwestdeutschland: Anlagenspezifische Gefahrenquellen, Störfalleintrittsvoraussetzungen und Sicherheitsvorkehrungen (Beispielsammlung). Bonn 1990.

[7] *Haferkamp, K.; Jäger, P.*: Analyse von Gefahrenquellen im Betrieb. TÜ 34 (1993) Nr. 1, S. 8-14.

[8] DIN V 19250: 1994, zurückgezogen 2004, Sicherheitsbetrachtung mit Risikograf aufgenommen in DIN EN 61511-3. Berlin: Beuth-Verlag 2005. VDI/VDE 2180: Sicherung von Anlagen der Verfahrenstechnik mit Mitteln der Prozessleittechnik (PLT) Blätter 1-4: 2007, Blatt 5: 2010, insbesondere Blatt 1: 2007 – Einführung, Begriffe, Konzeption.

[9] *Jochum, C.*: Gefahrenanalyse zur Bewertung des Gefahrenpotenzials von prozessbezogenen Anlagen. Fb 895. Bremerhaven: Wirtschaftsverlag 2000.

[10] Zwölfte Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes (Störfall-Verordnung – 12. BImSchV) in der Fassung der Bekanntmachung vom 8. Juni 2005. BGBl. I Nr. 33 vom 16. Juni 2005, S. 1598.

[11] *Study, K. A.; Champion, J. W.*: LOPA misapplied: Common errors can lead to incorrect conclusions. Process Safety Progress 28 (2009) Nr. 4, S. 300-307.

[12] Hazard and operability studies – Application guide, IEC 61882, 2001.

TÜVRheinland®
Genau. Richtig.

TÜV Rheinland
Industrie Service GmbH
Am Grauen Stein
51105 Köln
Tel. +49 1806 252535-1400*
Fax +49 1806 252535-1499*
is@de.tuv.com
www.tuv.com