

Ergebnisse der Österreichischen Arbeitsgruppe zur LOPA

Symposium
Anlagensicherheit 2011

Dr. Reinhard Preiss



Einleitung



- ✓ LOPA (Layer of Protection Analyse) - quantitatives Verfahren zur Risiko-Basierenden Bewertung gefährlicher prozessbedingter Szenarien
- ✓ Verfahren wird in EN 61508 (2010) und EN 61511 als anwendbare Methode zur Bewertung von Szenarien beschrieben
- ✓ Verfahren kommt historisch aus dem Englischsprachigem Raum
- ✓ Anwendung bei vielen großen Konzernen als standardisierte Methode zur Risikobewertung (damit auch in Österreich)
- ✓ Initiierung der Arbeitsgruppe 2008, zur
 - ✓ Erlangung eines gemeinsamen Verständnisses
 - ✓ Diskussion von Risikogrenzwerten
 - ✓ Grundlegenden Standardisierung der Anwendung



Teilnehmer an der Arbeitsgruppe



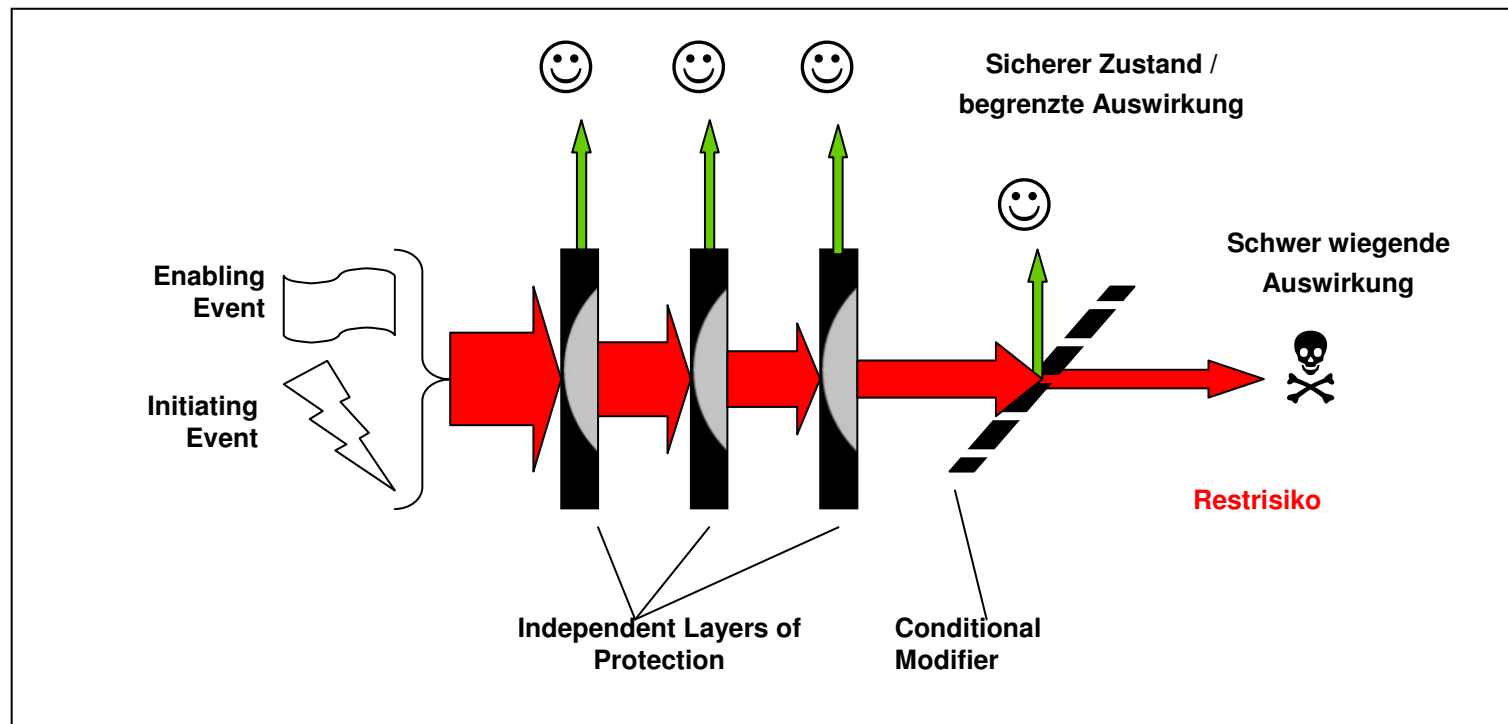
- ✓ 4 Vertreter von Behörden (BMWJF, Ländervertreter von Seveso II – Inspektionsbehörden)
- ✓ 8 Vertreter Industrie (Betreiber von Anlagen im Seveso II Regime)
- ✓ 1 Engineeringunternehmen mit Know-How auf dem Gebiet der Sicherheitstechnik
- ✓ TÜV Austria als Koordinator und zur Einbringung von Erfahrungen zum Thema Risikoanalyse

- ✓ Ursprüngliche Teilnehmer aus dem „Seveso II – Dunstkreis“, jedoch KEINE Limitierung der Methode auf derartige Anlagen



LOPA

- ✓ Betrachtung eines “Einzelszenarios” und des damit verbundenen Risikos
- ✓ Auslöser (IE) + Nebenbedingung (EE) + Versagen von Schutzmaßnahmen (PFD von IPLs) + Einflussfaktoren auf die Schwere des Schaden (CM) → Schwer wiegende Auswirkung

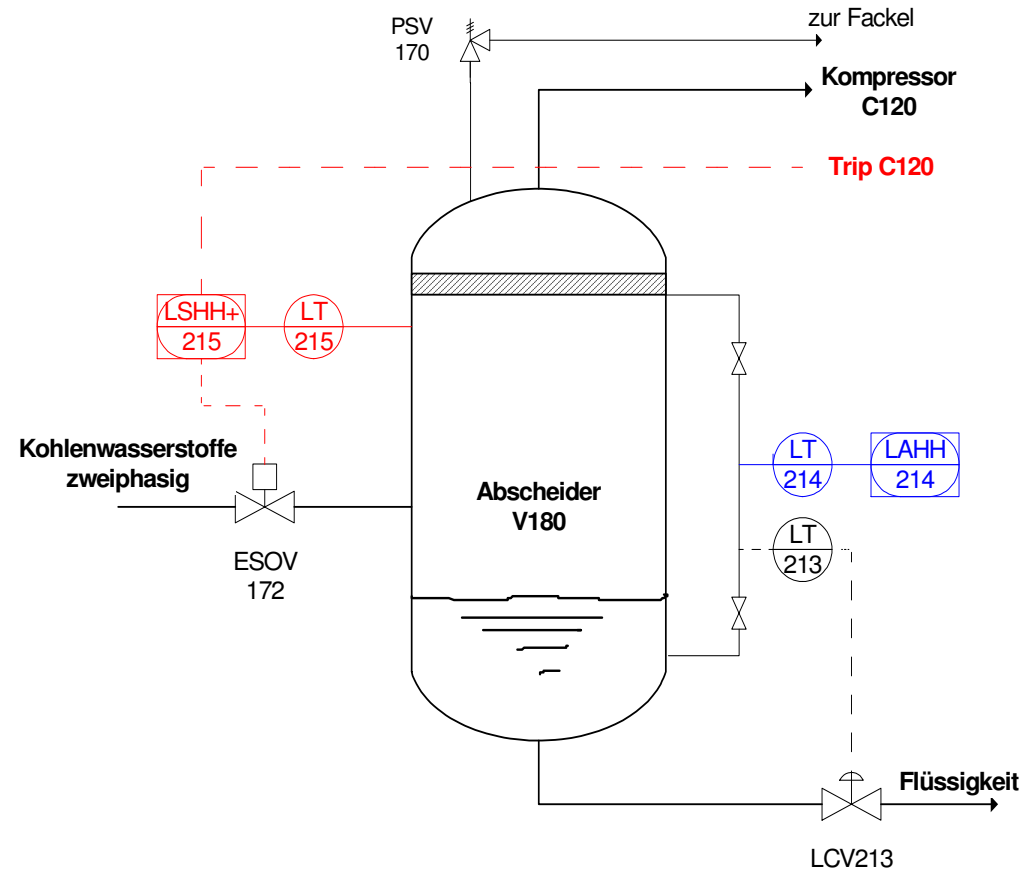




LOPA

✓ Bsp. Flüssigkeitsabscheider vor Kolbenkompressor

IE	+	Fehlfunktion LIC
EE	+	Anfall von Flüssigkeit
PFD IPL1	+	Versagen: Alarm und Eingriff
PFD IPL 2	+	Versagen: sicherheitsgerichtete Abschaltung
CM	+	Anwesenheit von Personal im Kompressorbereich
	↻	Verletzte / Tote durch massiven Kompressor-schaden mit Trümmerflug und Brand





Quantitatives Verfahren

✓ Toleranz- und Akzeptanzgrenzwerte (nur für LOPA Szenario)

Häufigkeit			
$10^{-2} - 10^{-3}$ [1/yr]			
$10^{-3} - 10^{-4}$ [1/yr]			
$10^{-4} - 10^{-5}$ [1/yr]			
$10^{-5} - 10^{-6}$ [1/yr]			
$10^{-6} - 10^{-7}$ [1/yr]			
Konsequenz Personenschaden	Verletzung mit > 24 Std. Krankenhaus und/oder reversible Beeinträchtigung / Verletzung	Irreversible Verletzungen (long term health effects) oder Todesfall innerhalb bzw. reversible Verletzungen außerhalb des Betriebsgeländes	Irreversible Verletzungen oder Todesfall außerhalb oder mehre Todesfälle innerhalb des Betriebsgeländes
Konsequenz Umweltschaden	Weitreichende Folgen möglich, lokale Intervention inner- oder außerbetrieblicher Stelle erforderlich UND reversibler Schaden	Weitreichende Folgen möglich, überregionale Intervention (z.B. Verständigung der Landeswarnzentrale) erforderlich UND reversibler Schaden	Irreversible Umweltschäden möglich, überregionale oder nationale Intervention erforderlich



Quantitatives Verfahren

✓ Toleranz- und Akzeptanzgrenzwerte (nur für LOPA Szenario)

- ✓ Roter Bereich:
Risiko nicht tolerierbar
- ✓ Gelber Bereich:
„ALARP“ nur für Bestandsanlagen anwendbar
- ✓ Grüner Bereich:
Risiko akzeptabel

Häufigkeit			
$10^{-2} - 10^{-3}$ [1/yr]	Red	Red	Red
$10^{-3} - 10^{-4}$ [1/yr]	Yellow	Red	Red
$10^{-4} - 10^{-5}$ [1/yr]	Green	Yellow	Red
$10^{-5} - 10^{-6}$ [1/yr]	Green	Green	Red
$10^{-6} - 10^{-7}$ [1/yr]	Green	Green	Green
	C1	C2	C3

- ✓ Existenz des „gelben Bereich“ bei Bestandsanlagen für nicht katastrophale Szenarien wird durch die Bestimmungen der GewO, §71a in Verbindung mit GewO Anlage 6 untermauert, womit auch auf Verhältnismäßigkeit und praktische Möglichkeiten zur technisch sinnvollen Umsetzung weiterer/moderner Maßnahmen Bezug genommen wird.



Quantitatives Verfahren

- ✓ Grenzwerte sind unter Anderem begründet durch
 - ✓ Ableitung von international üblichen Werten (z.B. HSE / UK)
 - ✓ Abgeleitetes Restrisiko aus EN 61511-3, Anhang D
 - ✓ MEM Prinzip aus EN 50126
 - ✓ EU-VO 352/2009 betreffend Sicherheitsmanagement im Eisenbahnwesen
 - ✓ RAPEX (Meldeverfahren der EU betreffend Produktsicherheit)

Häufigkeit			
$10^{-2} - 10^{-3}$ [1/yr]	Red	Red	Red
$10^{-3} - 10^{-4}$ [1/yr]	Yellow	Red	Red
$10^{-4} - 10^{-5}$ [1/yr]	Green	Yellow	Red
$10^{-5} - 10^{-6}$ [1/yr]	Green	Green	Red
$10^{-6} - 10^{-7}$ [1/yr]	Green	Green	Green
	C1	C2	C3



Anwendung des Verfahrens (1)

- ✓ Anwendung nicht nur zur SIL Klassifizierung von MSR Schutzeinrichtungen (alternativ zum Risikographen), sondern generell zur Evaluierung der Angemessenheit von Schutzmaßnahmen zur Absicherung von Szenarien mit potentiell hohem Schadensausmaß.
- ✓ Szenarien, die nicht durch systematisch erfassbare prozesstechnische Abweichungen bedingt sind, sondern durch Einflüsse wie Korrosion, unzureichende Wartung, Materialermüdung, Vibrationen, Erosion, etc., können durch eine Schutzebenenbetrachtung im Sinne der LOPA nicht sinnvoll dargestellt werden.
- ✓ Die angeführten Werte für Häufigkeiten sollen eine Größenordnung repräsentieren, der Multiplikator zur Zehnerpotenz soll keinesfalls eine zu hohe Genauigkeit vorspiegeln, d.h. es soll nur eine Ziffer als Multiplikator zur Zehnerpotenz, z.B. 2×10^{-1} [1/yr] verwendet werden.



Anwendung des Verfahrens (2)

- ✓ Zur Standardisierung der quantitativen Werte für die einzelnen Einflussgrößen werden konservative durchschnittliche Standardwerte, basierend auf Literaturangaben und der internationalen Praxis bei Anwendung des LOPA Verfahrens, angegeben.
- ✓ Sind bedingt durch praktische Erfahrung höhere Ausfallhäufigkeiten bekannt oder zu erwarten, so sind diese Werte zu verwenden.
- ✓ Eine Abweichung hin zu kleineren Ausfallhäufigkeiten wird aufgrund des semi-quantitativen Charakters des Verfahrens und der mit jeder Risikobetrachtung einhergehenden Unschärfe als nicht wünschenswert angesehen. Eine Abweichung ist daher nur in Fällen, wo eine detaillierte Analyse, etwa durch Anwendung der Methode des Fehlerbaums, eindeutig abweichende Ergebnisse liefert, zulässig.



Standardwerte – Techn. Init. Events



TÜV AUSTRIA GRUPPE

Ereignis (Initiating Event technischer Natur)	Häufigkeit [yr ⁻¹]	Anmerkung
Fehlfunktion einer Prozessregelung (dies umfasst alle möglichen Fehler der beteiligten Komponenten)	$\geq 10^{-1}$	Ein Wert $<10^{-1}$ ist durch die Anforderungen der EN 61511 bei Funktionen welche nicht für sicherheitstechnische Anforderungen klassifiziert sind, unzulässig.
Fehler eines Sensors / Stellgliedes (nicht Teil eines vollen Regelkreises) ^l	$\geq 10^{-1}$	
Ausfall Pumpe / Verdichter / Gebläse / Rührwerk / sonstiges rotating Equipment (keine Erfüllung der geforderten Funktion)	5×10^{-1}	Mit Werten aus RedBook, OREDA, RMR in Übereinstimmung
Innere Leckage eines Wärmetauschers (kein Rohrriss)	5×10^{-2}	
Rohrriss in einem Wärmetauscher	1×10^{-3}	Maximaler Wert nach Purple Book für höheren Druck auf der Rohrseite
Fehlerhaftes Öffnen eines Sicherheitsventils (z.B. Federbruch)	1×10^{-4}	Unter der Annahme regelmäßiger Wartung / Prüfung nach dem gesetzlichen Vorgaben (in Österreich)
Blockierter Filter	2×10^{-1}	Mit Werten aus Red Book, RMR, Purple Book in Übereinstimmung
Ausfall I-Luft bzw. Stromversorgung	Fallspezifisch zu evaluieren (abhängig von der Versorgungsarchitektur)	

Auszug



Standardwerte – Human Error

Komplexität	Häufigkeit (wie oft die Tätigkeit pro durchführender Person ausgeführt wird ^[1])	Stress	Fehlerwahrscheinlichkeit [case/cases], ist in Folge mit Häufigkeit pro Jahr zu multiplizieren
Einfach	Häufig (monatlich oder öfter)	Nein	1×10^{-3}
	Selten (weniger oft als monatlich)	Nein	1×10^{-2}
Komplex	Häufig (monatlich oder öfter)	Ja	1×10^{-2}
	Selten (weniger oft als monatlich)	Ja	1×10^{-1}
Komplex	Häufig (monatlich oder öfter)	Nein	1×10^{-2}
	Selten (weniger oft als monatlich)	Nein	1×10^{-1}
Komplex	Häufig (monatlich oder öfter)	Ja	1×10^{-1}
	Selten (weniger oft als monatlich)	Ja	1×10^0

Auszug

^[1] Es muss sichergestellt sein, dass diese Häufigkeit auf alle relevanten Personen zutrifft



Standardwerte – PFD von IPLs

IPL	Versagens - Wahrscheinlichkeit (PFD)
Automatische Reaktion über BPCS (Sensorik und Aktorik unabhängig vom Initiating Event) ⁰⁾	> 0,1 Entspricht EN 61511
Bedienereingriff (Aktorik unabhängig vom Initiating Event) nach Alarm (Alarm über BPCS, nicht verstellbar, Sensorik unabhängig von Initiating Event und anderen Schutzebenen), ausreichende Reaktionszeit und überschaubare Aktion (geringe Komplexität) vorausgesetzt	> 0,1
Von BPCS unabhängige MSR-Schutzmaßnahme, kein SIL Nachweis, Verwendung betriebsbewährter Komponente und wiederkehrende regelmäßige dokumentierte Überprüfung	0,1
Sicherheitsventil (bei Betrieb ohne bekannte Verschmutzung und regelmäßiger Wartung) , Ableitung an sichere Stelle	0,01 – 0,001
Rückschlagklappe, in Wartungsprogramm zur periodischen Überprüfung	≥ 0,1
Rückschlagklappe, keine periodische Überprüfung	1
Excess Flow valve (unterbricht Fluss im Falle eines zu hohen Werts, z.B. bei Schaugläsern, Schlauchbruchsicherung, Rohrbruchsicherung)	0,13 - 0,013
Ausfall einer sicherheitstechnischen Funktion in SIL 1	0.1 > PFD ≥ 0.01
Ausfall einer sicherheitstechnischen Funktion in SIL 2	0.01 > PFD ≥ 0.001
Ausfall einer sicherheitstechnischen Funktion in SIL 3	0.001 > PFD ≥ 0.0001

Auszug



Standardwerte – Conditional Modifier

Wahrscheinlichkeit der Zündung (Conditional Modifier) von freigesetzten brennbaren Stoffen	Besondere Bedingungen
1	Auslösendes Ereignis Kollision oder mechanischer Schaden mit Funkenbildung
1	Freigesetzter Stoff weist sehr niedrige Zündenergie auf (z.B. Wasserstoff) oder selbstzündendes Medium
0,1 – 0,3 (je nach Qualität des Zündschutzes)	Sämtliche Zündquellen im betroffenen Bereich nachgewiesener Weise vermieden (äquivalent der Ausrüstung einer Ex-Zone)
0,3 – 0,5	Vermeidung offenkundiger Zündquellen (z.B. elektrische Geräte, heiße Oberfläche), keine bekannten Zündquellen vorhanden
1	Keine explosionsgeschützten Geräte oder bekannte Zündquellen (z.B. heiße Oberfläche, Verkehrsfläche) im betroffenen Bereich
1	Sehr große Stofffreisetzung, sodass mit Verschleppung in weit entfernte Bereiche (z.B. mit KFZ befahren) zu rechnen ist.

Conditional Modifier: Anwesenheit von Personal im Gefahrenbereich	Besondere Bedingungen
Zeitanteil (Anteil der Betriebszeit der Anlage innerhalb derer die Gefährdung die möglich ist): $0,1 < CM \leq 1$	Das Verhalten von Personal bei Auftreten der relevanten Störung ist besonders zu berücksichtigen (Aufsuchen des Gefahrenbereichs, etc.)



Anwendungsbeispiele

- ✓ Behandlung von 9 typischen Anwendungsbeispielen aus der Prozessindustrie, teilweise in mehreren Varianten
- ✓ Ergebnisse zeigen, dass bei Verwendung der Standardwerte Schutzfunktionen, die dem üblichen Stand der Technik entsprechen, etabliert werden
- ✓ Vergleich der Ergebnisse mit Anwendung der Risikographen nach EN 61511-3, Anhänge D und E zeigen, dass
 - ✓ Anwendungsbereich der LOPA über jene der Risikographen hinausgeht
 - ✓ Die Szenarien durch Anwendung der LOPA besser analysiert und dargestellt werden können
 - ✓ Sofern eine Anwendung von Risikographen möglich ist, jener nach Anhang D im W. ähnliche Ergebnisse liefert
 - ✓ Der Risikograph nach Anhang E teilweise unsichere Ergebnisse für geringeres Schadensausmaß liefert



Zusammenfassung & Ausblick



- ✓ Das LOPA Verfahren wurde im breiten Kreis als sinnvolles Verfahren etabliert
- ✓ Die detaillierten Ergebnisse der Arbeitsgruppe werden als Guideline „Anwendung des LOPA Verfahrens..“ im Sommer / Herbst 2011 veröffentlicht werden
- ✓ Durch die Anwendungsbeispiele wird ein Katalog von typischen Fällen zur Verfügung gestellt
- ✓ Die Zusammenarbeit unterschiedlicher Stakeholder brachte fruchtbare Ergebnisse, diente der Wissenserweiterung aller Beteiligten und war durch gegenseitiges Vertrauen und Offenheit geprägt



TÜV AUSTRIA GRUPPE

**TÜV AUSTRIA
SERVICES GMBH**

**Geschäftsbereich Druckgeräte
Fachbereich Anlagensicherheit**

Dr. Reinhard Preiss

Email: pr@tuv.at

Mobile: +43-664-8271827