



Moderne Prozess- und Anlagensicherheit – Themen, Trends und Perspektiven

Digitalisierung der Anlagensicherheit und Risikoanalyse

FOKUS

Die Sicherheit von Prozessen und Anlagen rückt in den Fokus – Pandemien, Kriege und bilaterale Spannungen verschieben die strategische Ausrichtung von Unternehmen. Und der Fachkräftemangel fordert neue Wege, z.B. für Sicherheitsanalysen und Audits. Diese zeigen neue Regelwerke und Projekte, die gerade in der Entwicklung sind. Der Stand der Technik wird fortgeschrieben, u.a. mit Regelwerken wie der DIN-EN-ISO-4126-10, TRBS1115-1, NIS II, die Betreiber von Anlagen in 2024 sicherlich beschäftigen werden.



Keywords

- Prozessanlagensicherheit
- Druckentlastungseinrichtungen
- SIL, HAZOP
- Digitalisierung
- Künstliche Intelligenz

Die Revision der DIN-EN-ISO-4126-10:2024 zur Auslegung von Druckentlastungseinrichtungen ist überfällig gewesen. Der Teil 10 wurde seit 14 Jahren nicht überarbeitet. Jetzt ist er grundlegend geändert worden. Statt bisher rund 40 Seiten sind es nunmehr fast 80 Seiten geworden. Und noch etwas ist neu: Die Norm ist als CEN Norm harmonisiert und setzt in wesentlichen Teilen erstmals den Stand der Technik im europäischen Raum. Und ist damit verpflichtend geworden. Bereits der Titel verrät, dass jetzt nicht nur Sicherheitsventile, sondern zum ersten Mal auch Berstscheiben mit den Zu- und Abströmleitungen als Sicherheitseinrichtung für druckführende Systeme nach dieser Norm ausgelegt werden können. Und der Inhalt ist erheblich überarbeitet: Ein erweitertes Modell (HNE-CSE), was besonders bei siedenden Flüssigkeiten wesentlich andere Ergebnisse liefert, das Aufwallen in Behältern ist nicht mehr nur homogen angenommen, kryostatische Behälter werden betrachtet und eine Korrektur für die Viskosität von Flüssigkeiten ist dazu gekommen. Dies sind nur einige der Neuerungen im Regelwerk. Leider sind die Gleichungen in der Norm nicht leicht zu lösen, für viele Anwender wird dies zur „schweren Kost“. Schnell erfassen lassen sich die ganzen Neuerungen in dem Kompakt-Seminar ISO4126:2024 von CSE Engineering⁽¹⁾. Das Rechenprogramm CSE-Prozar enthält bereits alle Neuerungen der Norm. Die Norm wird sicher dazu führen, dass die Auslegung vieler Sicherheitsventile und Berstscheiben überarbeitet wird.

TRBS 1115-1 – Security jetzt auch nach BetriebsSV

Die Zeiten sind unsicherer geworden – Kriege prägen das Tagesgeschehen. Cyberphysikalische Angriffe haben massiv zugenommen. Und sie sind deutlich stärker in Richtung technischer Anlagen ausgeprägt. Leider fehlt bei Betreibern von Anlagen oft das Grundverständnis für die Bedrohungslage – wer soll eine Anlage für Biogas, Windkraft oder die Produktion schon angreifen? Das dies oft automatisch geschieht ist noch nicht angekommen. Umso wichtiger ist, dass der Gesetzgeber stufenweise die Anforderungen verschärft. Nach der KAS51 aus der Kommission für Anlagensicherheit, die dem Schutz der Öffentlichkeit (Mensch und Umwelt) dient, ist jetzt noch die TRBS 1115-1 hinzu gekommen. Streng genommen enthält sie das gleiche Anliegen, nur sollen hier die Arbeitnehmer über die Betriebssicherheitsverordnung geschützt werden. Ärgerlich ist, dass die Themen für Betreiber nicht harmonisiert sind, denn die Sicherheit sollte erhöht, die Bürokratie dagegen reduziert werden. Im Laufe dieses Jahres wird die europäische NIS II-Richtlinie in deutsches Recht umgesetzt wer-

den. Chemiebetriebe können neuerdings unter die kritische Infrastruktur fallen und haben dann erweiterte Meldepflichten. Oft sind die Themen im Bereich Schutz von Infrastruktur vor cyberphysikalischen Angriffen für Anlagenbetreiber neu und nur wenig fassbar. Sie passen nicht in die Welt der Sicherheitsanalysen aus dem Bereich Safety mit ihren regelmäßigen Auditierungen. Dabei lassen sich die Anforderungen aus allen Regelwerken gemeinsam umsetzen. Viele bereits vorhandene Dokumente können in diese Analysen eingebunden werden. Mit Hilfe von Dienstleistern ist dies meist weniger aufwendig als erwartet – allerdings sollten diese Dienstleister ein gutes Verständnis von Safety mitbringen.

HAZOPs erweitert für den Bereich Security

Heutige, klassische Risikoanalysen (HAZOPs) sind zu stark auf den Bereich Safety beschränkt. Aufwendige Analysen in großen Teams kennzeichnen diese Prozesse. In regelmäßigen Auditierungen, z.B. alle 5 Jahre, wiederholen sich Teile des Prozesses. Nach Seveso III müssen Eingriffe Dritter berücksichtigt werden, also auch die cyberphysikalischen Angriffe. Doch wie soll das gehen? Hier trifft Verfahrenstechnik auf die IT, genauer auf die OT (Operational Technology). Die Disziplinen „ticken“ unterschiedlich und haben verschiedene, fachspezifische Vorgehensweisen. Eine neue Option ist die Erweiterung der klassischen HAZOPs um den Bereich Security. Dazu müssen jedoch für sicherheitstechnische Funktionen in den Anlagen passende Sicherheitsanforderungen definiert werden. Die SIL aus der funktionalen Sicherheit und die SLT-Level müssen harmonisiert werden. Es reicht nicht aus, die R&I Fließbilder der Anlagen durchzugehen – die Netzwerkpläne aus dem OT-Bereich werden ebenso wichtig. Die Methode „safety related Cyberphysical Safety Evaluation“ (sCSE) für HAZOPs mit allen Safety und Security Aspekten ist entwickelt. Derzeit wird versucht, die Methode teilautomatisiert umzusetzen.

Cyberangriffe modelliert mit einem digitalen Zwilling

Was nützt der Schutz vor Cyberangriffen, wenn nicht getestet werden kann, ob er ausreicht? Jeder Betreiber von Anlagen fühlt sich unwohl bei dem Gedanken an solche Tests. Ob die Anlage danach noch wie gewohnt weiterläuft, ist nicht sicher. Doch die Maßnahmen, die notwendig sind um KAS51, TRBS1115, NIS II etc. zu erfüllen, sollten nach Ereignissen und auch in regelmäßigen Abständen einem Test unterzogen werden. Aus den Diskussionen im Industrie-Erfahrungsaustausch CeSIS entstand der Ansatz, den OT-Bereich von Anlagen zu virtualisieren und einen digitalen Zwill-

ing zu bauen. Der Aufwand ist recht groß und die Netzpläne sowie die Assets müssen digital erfasst werden. Doch die Vorteile der virtuellen Darstellung einer Anlage können enorm sein. Am CSE Center of Safety Excellence soll eine Anwendung entwickelt werden, mit der ein OT-Zwilling gebaut werden kann für Cybertests – einerseits in den Unternehmen selbst, aber auch als externe Dienstleistung.

KI-basiertes Wissensmanagement

Wer wünscht sich nicht, dass die Anforderungen aus den Regelwerken über eine künstliche Intelligenz (KI) auf den eigenen Betrieb übertragen werden und mit einer Checkliste die Sicherheit lückenlos und vollständig umgesetzt werden kann? Es ist schwer einen Überblick über die Regelwerke und Änderungen lassen sich fast nicht mehr nachhalten. Der Stand der Technik ist in vielen Regelwerken, Richtlinien und Publikationen dezentral abgelegt und ändert sich dynamisch.

Dies Entwicklung gilt grundsätzlich für unser Wissen. Dazu ist das Wissen häufig in verschiedenen Datenbanken und Formaten (Texte, Fließbilder, Graphiken, etc.) gespeichert, oder nur implizit in den Köpfen von ExpertInnen vorhanden. Eine zeitgemäße und effektive Nutzung des gesamten Wissens ist fast nicht möglich und nur einem kleinen Kreis von AnwenderInnen vorbehalten. Wie kann Wissen gespeichert und genutzt werden, um den Transfer an die nachfolgende Generation zu gewährleisten?

Die Art der Wissensaufbereitung und -repräsentation muss grundlegend geändert werden. Dazu muss das umfangreiche Fachwissen auf Basis bestehender Fachliteratur, Regelwerke und sonstiger Dokumente automatisiert aufbereitet, abstrahiert und gespeichert werden, um es in neuen Kontexten einzusetzen und einer sehr viel breiteren Anwendergruppe nutzbar zu machen. In der Prozess- und Anlagensicherheit gibt es dazu eine Reihe von Projekten und erste Erfahrungsaustausche innerhalb der Industrie. KIBOD, ein Forschungsprojekt des CSE Center of Safety Excellence, ist ein Beispiel für diese Anwendungen.

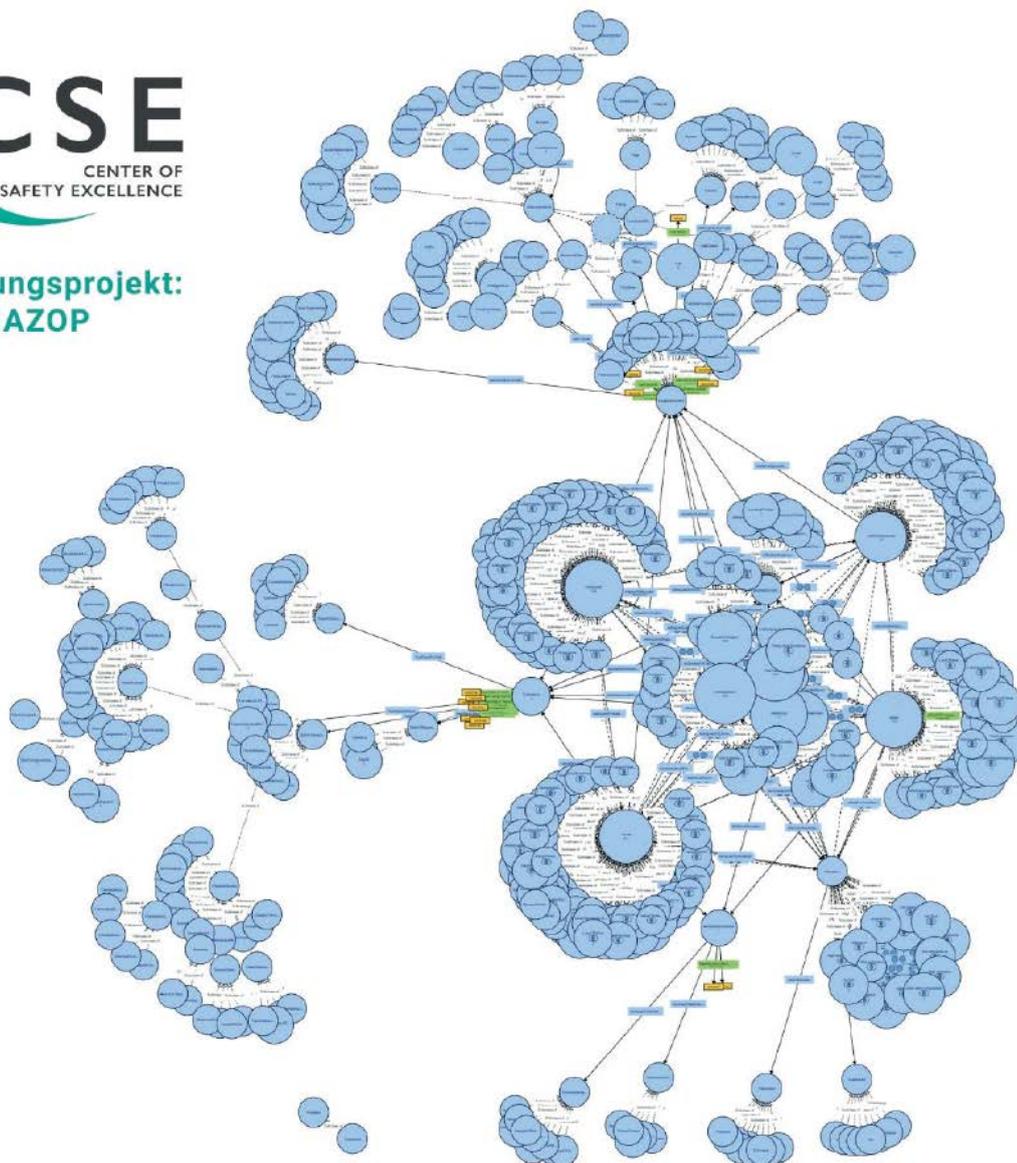
Im Gegensatz zu Natural Language Processing Systemen wie ChatGPT, die Texte probabilistisch zusammensetzen, ermöglicht es KIBOD, das Wissen semantisch zu erfassen, implizites Fachwissen zu integrieren und mit Hilfe von logischem Schließen aus der Ontologie deterministisch neue Kontexte korrekt zu bewerten.

MetA-HAZOP – automatisierte Gefahren- und Risikoanalysen

Doch mit KI-basierten Wissensdatenbanken lässt sich noch mehr erreichen. In der Sicherheitstechnik könnten bspw. gefährliche Anla-



**Forschungsprojekt:
MetA-HAZOP**



In MetA-HAZOP sollen Gefahren- und Auswirkungenanalysen (HAZOPs) automatisch erstellt werden. Dazu sind Wissenrepräsentationen (Ontologien) erforderlich.

genzustände viel effizienter und vollständiger erfasst werden. Und selbst die technische Risikoanalyse könnte automatisch durchgeführt werden. Derzeit machen dies interdisziplinäre Teams mit sechs bis zehn Experten und Expertinnen unterschiedlicher Fachgebiete. Aufgrund des Umfangs und der Komplexität der technischen Anlagen dauern Risikoanalysen typischerweise mehrere Monate mit entsprechend hohen Kosten. Die Ergebnisse der Analysen hängen stark von der Erfahrung der Teilnehmer, der Moderation sowie der Kommunikationskultur ab. Künftig wird es immer weniger Experten geben, die über das notwendige Wissen verfügen. Deshalb wird in verschiedenen Projekten, z.B. an der Universität Dortmund und am CSE Center of Safety Excellence versucht, den Prozess der HAZOP zu automatisieren. Im Projekt MetA-HAZOP soll dies mit einer Ontologie, basierend auf bereits bestehenden HAZOPs, erfolgen. Es werden sehr viele HAZOP-Tabellen aus der Industrie dazu verwendet, dieses

Wissen in einer Ontologie zu repräsentieren, um daraus automatisch eine HAZOP-Tabelle zu für neue Anlage erstellen. Die Umsetzbarkeit ist in einer Dissertation vom CSE Center of Safety Excellence nachlesbar^[1].

Eine große Herausforderung in MetA-HAZOP ist die Abstraktion der Informationen und Daten auf ein Minimum, das es erlaubt, eine technische Risikoanalyse zuverlässig durchzuführen, ohne für die Anwendung unbedeutende Details zu berücksichtigen. Selbst vermeintlich einfache Kontexte können zu Fehlern führen: Ist die Farbe eines Apparates relevant für die Analyse? Wenn dadurch Energie absorbiert und in den Apparat eingetragen wird, muss sie berücksichtigt werden. Allerdings reicht es, die Eigenschaft „Absorption“ zu erfassen. Teilweise werden weder die Farbe noch die Eigenschaften angegeben, weil bestimmte Apparate „immer“ mit vorgegebenen Anstrichen versehen werden, ohne dass dies dokumentiert wird (implizites Expertenwissen).

Mit MetA-HAZOP wird die technische Risikoanalyse zuverlässig und voll automatisiert möglich. Damit einher geht eine enorme Reduktion des Zeit-, Kosten- und Personalaufwands, subjektive Einschätzungen entfallen und der Einfluss von Teamzusammensetzung und sonstiger Störfaktoren ist nicht mehr relevant. Die Projekte der automatisierten HAZOP werden bereits in Erfahrungsaustauschen der Industrie wie der European Group for Advanced HAZOP Studies (EuGaH) diskutiert.

**Quantitative Risikoanalysen (QRA)
INSPIREd**

Mit den typischen Risikomatrizen wird die Wahrscheinlichkeit für ein Ereignis längst in die deterministischen Gefahren- und Auswirkungenanalysen von Unternehmen integriert. Doch die Digitalisierung erlaubt sehr viel mehr. Spätestens mit der INSPIRE-Direktive der EU wurden Straßen, Häuser, Parks, Besiedlungsdichten, Leitungen im Boden digital erfasst und können

problemlos abgerufen werden. Es bietet sich an, diese Informationen in den Risikoanalysen zu nutzen? Besonders bei Gasleitungen, die oft vernetzt durch dicht besiedelte Gebiete führen, wäre das ein Quantensprung. Die Systeme dazu sind bereits entwickelt. Eine QRA in für technische Anlagen in dichter Besiedlung sollte zum Standard werden. Es sind weiterhin Konventionen erforderlich. Doch die Details der Analysen und damit die individuellen Maßnahmen, die zum Schutz von Menschen und Umwelt festgelegt werden können, erweitern die heutigen Sicherheitskonzepte deutlich. Auch die Öffentlichkeit könnte besser informiert werden. Die Systeme lassen sich auch für die Wartung und Instandhaltung nutzen – wie das Forschungsprojekt risk based Integrity Management (RiIM) zeigt.

Proaktive Alarm- und Gefahrenabwehrplanung (AGAP)

Sicherlich besteht noch Verbesserungsbedarf in der Gefahren- und Abwehrplanung. Die Chancen der Digitalisierung sind noch lange nicht genutzt. Einerseits werden in den HAZOPs alle vernünftigerweise nicht auszuschließenden Szenarien durchdacht. Jedoch werden diese Szenarien in den Gefahren- und Abwehrplänen bei den Feuerwehren im öffentlichen Bereich oft nicht hinreichend integriert. Das ist auch nicht notwendig in dünn besiedelten Gebieten. Doch bei dichter Bebauung, bspw. nahe

oder in Städten, muss dies Stand der Technik werden. Pläne zu den Anlagen, Verantwortlichkeiten und eine allgemeine Beschreibung der Szenarien sind nicht mehr zeitgemäß. Das wurde auch in der Kommission für Anlagensicherheit diskutiert. Die neuen digitalen Systeme erlauben bereits szenarienbasierte AGAPs. Im letzten Jahr wurde dazu in Kooperation mit der Berufsfeuerwehr Ludwigshafen ein neues Seminar Alarm- und Gefahrenabwehrplanung entwickelt^[2], bei dem die Methoden an Beispielen aus der Industrie gezeigt werden.

Blick in die Zukunft – Vision

Die Digitalisierung schreitet auch in der Prozess- und Anlagensicherheit voran. Sicherheitseinrichtungen werden intelligent und von Prozessen entkoppelt. Druckentlastung wird in Richtung Zero Emission entwickelt und die künstliche Intelligenz ermöglicht ein deutlich höheres Maß an Sicherheit. Dies zeigen die Beispiele der automatisierten HAZOPs (Meta-HAZOP), Wissensrepräsentationen wie KIBOD, aber auch die kombinierten Safety Security Analysen (sCSE) sowie die szenarienbasierten AGAPs. Selten hat es so viele Themen gegeben, die insbesondere auch junge Studierende an den Universitäten anziehen. Die Welt sicherer zu machen ist wieder en vogue und kann den Nachwuchs begeistern.

Referenzen

- [1] Berechnungsprogramm CSE-ProSAR <https://cse-prosar.de>
- [2] J. Single, „Automation of the hazard and operability method using ontology-based scenario causation models,“ Kaiserslautern, 2022.
- [3] Seminar Alarm- und Gefahrenabwehrplanung (AGAP); [https://cse-engineering.de/applied-safety/ alarm-und-gefahrenabwehrplanung-agap/](https://cse-engineering.de/applied-safety/alarm-und-gefahrenabwehrplanung-agap/)



Prof. Dr.-Ing. Jürgen Schmidt, Geschäftsführer, CSE Center of Safety Excellence

Wiley Online Library



CSE Center of Safety Excellence gGmbH, Pfinztal
 Professor Dr.-Ing. Jürgen Schmidt
juergen.schmidt@cse-institut.de
www.cse-institut.de · www.cse-engineering.de



DISCOVER ISPE GUIDANCE DOCUMENTS

Shape the Future of Pharma™ with the Gold Standard in Peer-Driven Insights

Keep up with the latest industry trends, technological advancements, and regulatory expectations. Written and reviewed by your industry peers, ISPE Guidance Documents provide best practices that help narrow the interpretation of regulatory standards and help you maintain a competitive edge in the market.

Are You Ready to Shape the Future of Pharma™?



ISPE.org/Guidance-Documents

The International Society for Pharmaceutical Engineering