Gesellschaft und Sicherheit (IV)

Anlagensicherheit und Sicherheitskultur

Sylvius Hartwig, Ehrenkirchen

Es ist ein Zeichen unserer Zeit immer mehr Entscheidungen und technisch-industrielle Abläufe von Algorithmen von Rechenanlagen durchführen oder kontrollieren zu lassen. Diese Algorithmen werden von sog. Experten der Mathematik oder IT als Auftrag entwickelt oder von sich aus zur eigenen Markterschließung, um dann in Anlagen oder Prozessen eingesetzt zu werden. Vergessen wird oft, dass diese Experten sui generis ihr Expertentum oft in ihrem Metier, also beispielsweise der Mathematik, aber nicht in der Prozesssteuerung, der Finanzbranche oder der Sicherheitstechnik haben – je nachdem wo die Algorithmen gebraucht werden. Die Algorithmen sind oft für den gedachten Anwendungsbereich gut durchgetestet, aber kaum für die nur mühsam bekannten Randbedingungen des Einsatzgebietes. Sie funktionieren dann genau dafür, wofür sie gedacht sind. Sie funktionieren aber nicht – zum Erstaunen der Anwender – für die bis dato nicht bekannte oder nicht erwartete Situation.

Ein gutes Beispiel aus dem heutigen Alltag ist der Crash an der New Yorker Börse (NYSE) in der 18. Kalenderwoche dieses Jahres. Es wurde wohl von einem Makler aus Versehen eine um mehrere Größenordnungen zu große Verkauforder eingetippt, was zur Folge hatte, dass der Kurs abrupt nachgab. Nun habe ich mir sagen lassen, dass mehr als die Hälfte aller Aktienaufträge (Kauf oder Verkauf) nicht mehr durch Personen gegeben werden, sonder durch Rechneralgorithmen, die z. B. bei Überschreiten eines Kursabfalllimits automatisch durch den Rechner große Verkaufsaufträge auf den Markt werfen, denn wer schnell verkauft, erleidet weniger Verluste. Das wiederum erzeugt erneut einen weiteren rapiden Kursabfall, der wiederum zu schnelleren Algorithmusreaktionen führt usw. bis zum Crash. Der Fehler lag also in der Tatsache, dass der Algorithmus von seiner Struktur her den fatalen Schritt nicht erkannte, da er nicht einprogrammiert war. Die Finanzgemeinde will natürlich diesen Fehler abstellen – das ändert aber nichts am Prinzip, dass Algorithmen

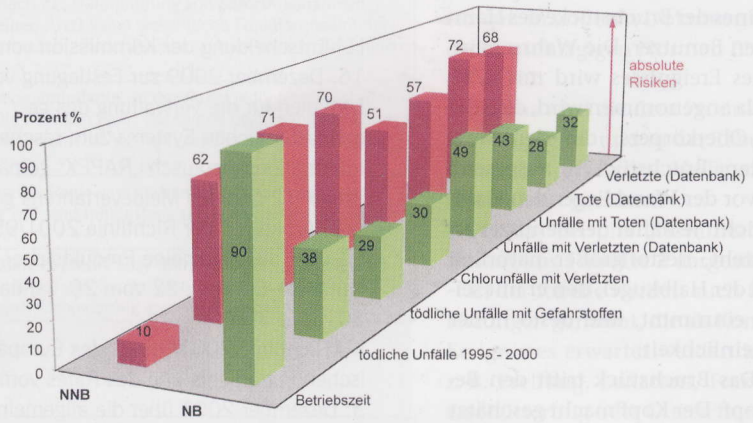

Bild 1 *Prozentualer Vergleich der Anzahl der Störfälle im normalen Produktionsbetrieb (NB) und im nicht normalen Betrieb (NNB) aus verschiedenen Datenbanken [1].*

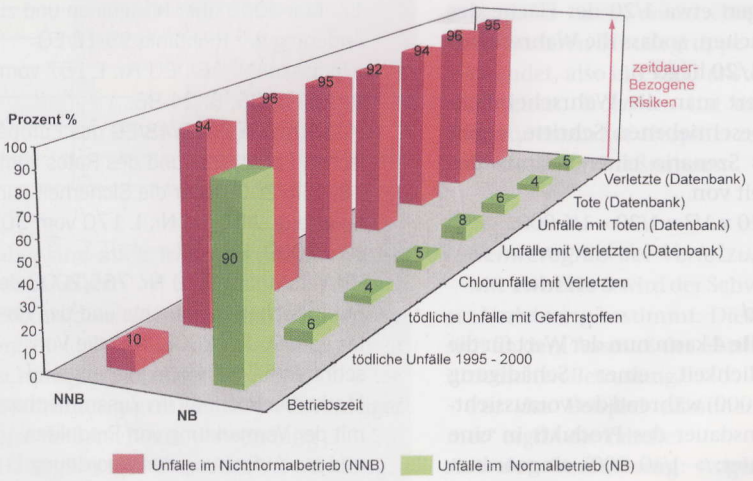

Bild 2 *Prozentualer Vergleich der Anzahl der Störfälle im normalen Produktionsbetrieb (NB) und im nicht normalen Betrieb (NNB), bezogen auf die durchschnittliche Zeit der Betriebszustände [1].*

zu undifferenziert oder dumm sind, Ungewöhnliches zu erkennen. Sie können diese Art von Schäden und Risiken nicht mindern, sondern sie erzeugen sie.

Das Beispiel der Eskalation an der Börse ist auch bei Katastrophen in der verarbeitenden Industrie zu sehen; nur dort wird es nicht so deutlich, da die Sachzusammenhänge schwieriger wahrzunehmen sind.

Diese Gefahr existiert auch in unserer mit Algorithmen in Steuerungsanlagen durchwucherten Industrie bei der Steuerung von Produktionsprozessen, die mit entsprechenden Risiken für die Anlage, das Werk oder im schlechtesten Fall den ganzen Konzern behaftet sind. Die Antwort auf dieses Risiko sind nicht bessere Algorithmen, sondern eine bessere und intelligentere Sicherheitskultur. Damit ist neben vielem anderen gemeint, die wichtigen Entscheidungen den Führungskräften mit intimer Kenntnis der Anlage zu überlassen

und nicht vorgenerierte Entscheidungen für hilfreich in der Risikobewältigung zu halten.

Heutige Anlagen sind in vielen Fällen durch Prozessoren gesteuert. Damit wird vielfach unterstellt, dass hiermit eine gute Voraussetzung zur Risikobewältigung einhergeht, denn in den sicheren Ablauf der Produktion sind üblicherweise hohe Investitionen getätigt worden. Ist die Produktion sicher, so ist die Anlage risikoarm – wird oft geschlussfolgert.

Um das zu untersuchen, haben wir aus eigenen Datenbanken und anderen zur Verfügung stehenden Informationen das Auftreten von Störfällen verschiedener Schwere einerseits im normalen Produktionsbetrieb (NB) und andererseits bei Wartung, Reinigung, Reparatur und nicht geplantem Stillstand (NNB) evaluiert [1]. In **Bild 1** ist aus verschiedenen Sachzusammenhängen und Datenbanken die Verteilung jeweils auf NNB und NB dargestellt. Zusätzlich ist für die normale ungestörte Betriebszeit als Durchschnitt ein Wert von 90 % angenommen und entsprechend für NNB 10 % (wie im ersten Säulenpaar angegeben). Deutlich zu sehen ist, dass im normalen Produktionsbetrieb weniger als die Hälfte der Unfälle auftreten, manchmal nur bis zu 28 oder 24 %. Berücksichtigt man dazu und normiert auf die entsprechende Betriebszeit (wie in **Bild 2** dargestellt), so ist offensichtlich, dass nur 4 bis 8 % des Gesamtrisikos auf Zeiten der normalen Produktion pro Zeiteinheit entfallen. Mit anderen Worten, in der Zeit nicht normaler Produktion ist das Risiko pro Zeiteinheit 20 mal größer als während der Produktion. Das Risiko der meisten Anlagen wird also durch die Zeit außerhalb des üblichen Produktionszyklus bestimmt. Im Gegensatz dazu wird der überaus größte Anteil der Investitionen für die Sicherheit allerdings für die Zeit der Produktion selbst investiert. Zusätzlich geben viele Betriebe die problematischen Schritte Wartung, Reinigung und Beheben von Stillständen an außerhalb des Betriebs liegende Kontraktoren, die mit der Anlage oft weniger vertraut sind. Bei unseren Untersuchungen [2] in zwölf Anlagen waren dies knapp 50 % mit deutlichem Schwerpunkt bei der Wartung (58 %) und am geringsten, da es ein Zeitproblem ist, bei ad hoc anfallenden Reparaturen. Allerdings hat sich nach unserem Kenntnisstand dieser Anteil der Fremdvergabe in der letzen Zeit aus Kostengründen noch erhöht. Das Argument ist die zeitliche Unterauslastung einer eigenen Mannschaft während der normalen Produktionszeit. Die Entscheidungsbasis ist schmalspurig auf die Kosten der Auslastung einer eigenen Wartungstruppe, aber nicht auf die Gesamtrisikolage und den damit zusammenhängenden Kosten bezogen.

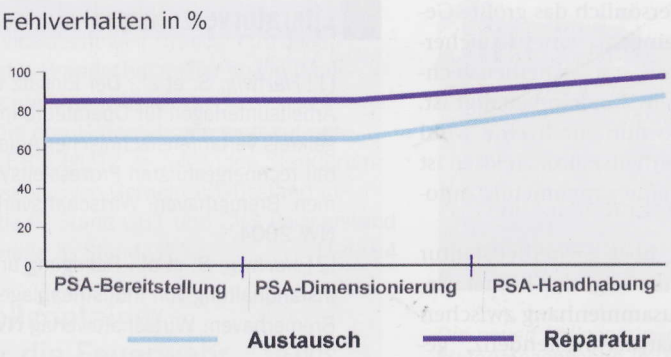

Bild 3 *Fehlverhalten bei Austausch von Armaturen und Reparaturen an offenen Systemen [2].*

Die Sicherheitskultur des Gesamtbetriebs und die Bewertung des Gesamtrisikos mit seinen Kosten funktioniert bei dieser Form der Arbeitsteilung nicht wirklich.

Die Parallelen zum Kurssturz in der 18. Kalenderwoche (übrigens der drastischste Kurssturz der je an der NYSE auftrat) ist deutlich. Einerseits haben wir durch Prozessoren gesteuerte hochautomatisierte Betriebsabläufe im normalen Produktionsbetrieb, wollen aber Störfälle ausschalten die, wie die Bilder 1 und 2 zeigen, wenig mit diesem normalen Produktionsablauf zu tun haben (wie die fälschlich eingegebene zu hohe Verkaufordner an der NYSE). Die Steuerungsmechanismen versagen, da die Randbedingungen der NNB-Zustände so wenig vorhersehbar sind, dass Automatisierung nicht weiterhilft.

In den NNB-Zuständen sind Fachleute mit großen Erfahrungen im Beherrschen ungewöhnlicher und seltener Zustände gefragt. Diese Fachleute wurden aber zum Teil aus Kostengründen „outgesourced", die auf Berechnungen der normalen Produktionskosten beruhen und nicht in Bezug auf die gesamten Betriebskosten.

Versucht man die Struktur dieser Risikoaussage im größeren Detail zu bestimmen, so ist das in der Allgemeinheit der bisher gemachten Aussage und in Bezug auf die Verschiedenartigkeit der Betriebe nicht möglich. Mehr Kenntnisse über die Produktionssparte und die verschiedenen Arten von Betrieben sind nötig. Deshalb sollen als Beispiel hier Untersuchungen, die wir in Betrieben mit der Verarbeitung gefährlicher Stoffe und dem Einsatz persönlicher Schutzausrüstung (PSA) durchgeführt haben, betrachtet werden.

Bild 3 zeigt die Situation bei Wartungsarbeiten in einer größeren Zahl von Betrieben und dem Einsatz von PSA. Das Fehlverhalten beim Einsatz von PSA kann nach drei verschiedenen Gesichtspunkten bewertet werden. Es sind dies die Bereitstellung von PSA, die Dimensionierung und die Handhabung. Hierbei sind verschiedene Hierarchien der Mitarbeiter angesprochen. Die Bereitstellung und die Entscheidung über die Anschaffung ist üblicherweise dem unteren Management vorbehalten, die Dimensionierung dem Sicherheitsingenieur bzw. der Sicherheitskraft und die Handhabung dem Mitarbeiter vor Ort.

Bild 3 basiert auf Untersuchungen in zwölf Betrieben [2], bei denen in der Verarbeitung gefährliche Stoffe auftraten. Es zeigt die Situation bei Reparatureinsätzen an offenen Systemen die ungefähr 95 % aller Fälle betrafen. Die Tätigkeit war der Austausch oder die Reparatur von Armaturen, also Tätigkeiten, bei denen mit sehr hoher Wahrscheinlichkeit das Auftreten und die Exposition von und mit gefährlichen Stoffen zu erwarten ist.

Die Höhe des Fehlverhaltens erklärt das hohe Risiko, das in NNB-Situationen zu erwarten ist. Erklärbar wird auch, warum Automatisierung hier in der Risikobewältigung oft nicht weiter hilft. Die Haltung der Mitarbeiter, also des Managements bis zum Arbeiter vor Ort, ist die entscheidende Einflussgröße.

Außerdem zeigte sich eine Abstufung des sicherheitstechnisch bedenklichen Handelns vom Management (48 %), über den Sicherheitsbeauftragten (57 %) bis zum Arbeitnehmer vor Ort (76 %). Charakteristischer Weise ist immer wieder zu sehen, dass

die Gruppe, die persönlich das größte Gesundheitsrisiko eingeht, unerfreulicherweise am stärksten am sicherheitstechnisch bedenklichen Handeln beteiligt ist. Eine Aufgabe, die nur durch eine wohl durchdachte Sicherheitskultur zu lösen ist und nicht durch eine zunehmende Automatisierung.

Bei Seminaren über Sicherheitskultur mit Führungskräften zeigt sich immer wieder, dass dieser Zusammenhang zwischen forcierter Automatisierungstendenz, gespeist durch den Willen zur weiteren Kostensenkung einerseits und der Notwendigkeit zur verstärkten Einbeziehung von Risikofachkräften in die Detaillösung von Sicherheitsproblemen andererseits, nur schwer akzeptiert wird, mit dem Resultat höherer Gesamtkosten. Es wird leider und zum Schaden des Gesamtbetriebs nicht gesehen, dass öfter ein geringerer Automatisierungsgrad geringere Kosten verursachen kann; berücksichtigt man auch die Störfallkosten (und die Kosten der Produktionsausfälle) im Bereich des nicht normalen Produktionsbetriebs. TÜ 911

Literaturverzeichnis

[1] *Hartwig, S.* et al.: Der Einsatz von Arbeitsunterlagen für Operateure im Regelkreis verfahrenstechnischer Anlagen mit rechnergestützten Prozessleitsystemen. Bremerhaven: Wirtschaftsverlag NW 2004.

[2] *Hartwig, S.* et al.: Reinigung und Instandhaltung von Industrieanlagen. Bremerhaven: Wirtschaftsverlag NW 2003.

Univ.-Prof. Dr. **Sylvius Hartwig**, Professor der Sicherheitstechnik an der Bergischen Universität Wuppertal, Ehrenkirchen.