Beinahe-Unfall-Analysen im Elektrobereich: Potenzial oder heisse Luft?

An der 10. Fachtagung für Arbeiten unter Spannung (AuS) in Nieder- und Mittelspannungs-Netzen, veranstaltet durch EW Medien und Kongresse GmbH in Köln, wurden vom Autor dieses Beitrags Potenziale und Grenzen von Beinahe-Unfall-Meldesystemen bei AuS erörtert. Basis dafür ist eine kleine Umfrage im Juni 2015 bei Netzbetreibern und Industrie-Unternehmen in der Schweiz sowie ein Quervergleich mit Aviatik und Medizin.

Hansueli Homberger

Der Schreck, wenn beinahe ein Unfall passiert, hat einen unübertrefflichen Lerneffekt. Aber: Beinahe-Ereignisse sind dadurch charakterisiert, dass sie vertuscht werden können. Damit also aus individuellen Lernerlebnissen ein kollektiver Verbesserungsprozess wird, brauchen Betroffene Gründe, Beinahe-Ereignisse nicht zu vertuschen.

Die Kombination von systematischen Analysen bei Unfällen wie auch bei Beinahe-Unfällen ist ein effektiver Weg zur Senkung von Unfallzahlen. Entsprechend werden seit längerem in verschiedenen Branchen Beinahe-Unfälle erfasst. Eine Vorreiterrolle haben dabei Aviatik und Medizin. Ob und wie das für AuS und den Elektrosektor im Allgemeinen nützlich ist, hängt nicht zuletzt von begrifflicher Klarheit ab.

Erste Einordnungen

Unfälle und Beinahe-Unfälle sind zu unterscheiden von *unsicheren Situationen* (Zuständen, Handlungen[1]), aus denen sie hervorgehen. Weniger unsichere Situationen heisst potentiell kleinere Unfallwahrscheinlichkeit, wobei bei dieser Gleichung ein wichtiges qualitatives[2] Element nicht übersehen werden darf: Unfallprävention muss bei den gefährlichsten Situationen ansetzen, das heisst bei Situation mit hohem Schadenspotential und hoher Eintretenswahrscheinlichkeit. Beinahe-Unfall-Meldesysteme sind hilfreich für die Feinsteuerung der Unfallprävention, sind aber kein Ersatz für ein adäquates Sicherheitssystem, worin sie vielmehr zu integrieren sind.

Erweitert man die Betrachtung auf *Regelverstösse, Sanktionen und Anreize*, schälen sich weitere Grundsätze heraus: Müssen Sanktionen befürchtet werden wenn ein kritischer Vorfall auf einem Regelverstoss beruht – oder wenn die Betroffenen nur schon unsicher sind diesbezüglich – wird mit hoher Wahrscheinlichkeit nichts gemeldet. Und jedes nicht gemeldete Beinahe-Ereignis ist verschenktes Verbesserungspotenzial: Vielleicht ist das Problem ja gar nicht der Regelverstoss, sondern die Regel selber, weil unter Zeitdruck nicht umsetzbar, missverständlich formuliert, schlecht kommuniziert oder schlicht unlogisch. Weil die Meldung eigener Regelverstösse natürlich nicht automatisch von Sanktionen befreien kann,

[1] *Unsichere Handlungen* wurden 2000 vom US-Psychologieprofessor James Reason als letzte von mehreren Prozessebenen definiert, die Unfällen vorgelagert sind. Seine Betrachtung beginnt Reason gewissermassen auf der Managementebene, bei den *organisatorischen Einflüssen*, gefolgt von den Ebenen der *Überwachung,* der *unsicheren Vorbedingungen* und eben der unsicheren Handlungen. Seine Sicht, dass alle zur Unfallverhütung eingerichteten Barrieren löchrig seien, wurde unter dem Begriff *Swiss Cheese Model* bekannt. Quelle: Human Error: models and management; British Medical Journal, 2000 Mar 18; 320(7237): 768–770.

[2] Über Vor- und Nachteile qualitativer oder quantitativer Analysemethoden wird da und dort noch gestritten, während sich in der Forschung schon länger durchgesetzt hat, dass Analysedesigns mit *Mixed Methods* und *Triangulation* die Realität am Besten abbilden, dass also z.B. quantitative Erhebungen mit qualitativen Methoden vertieft werden und umgekehrt. Literaturbeispiele: 1. Flick, U. (2006). Qualitative Evaluationsforschung. Rheinbeck bei Hamburg, Rowolth Taschenbuch Verlag. 2. Atteslander, P. (2010 [1969]). Methoden der empirischen Sozialforschung. Berlin, Erich Schmidt Verlag.

braucht es klare Festlegungen, realistische Ziele, Transparenz, Konsequenz und nicht zuletzt Vertrauen, um in diesem Sinn unsichere Situationen zu vermeiden.

Zu unterscheiden ist weiter zwischen AuS und anderen Tätigkeiten im Umfeld elektrischer Anlagen. AuS ist Spezialistentätigkeit, ausgeführt von einem verhältnismässig kleinen, spezifisch geschulten und ausgerüsteten Personenkreis. Elektro-Arbeitsunfälle sind bei AuS selten im Vergleich mit so genannten *Arbeiten in der Nähe Spannung führender Teile*, die von einem erheblich grösseren und oft weniger qualifizierten Personenkreis in Industrie, Elektrohandwerk und Instandhaltung ausgeführt werden. Im Rahmen der hier beschriebenen Recherche wurden daher Erfahrungen mit Beinaheunfall-Meldesystemen nicht nur bei Netzbetreibern, sondern auch bei einigen global tätigen Industrieunternehmen erfragt.

Critical Incident Reporting Systems (CIRS) in Aviatik und Medizin

Die längste Erfahrung mit Beinahe-Unfall-Meldesystemen hat die Luftfahrt, charakterisiert durch viele exponierten Personen und entsprechend hohem Schadenspotential bei verhältnismässig tiefer Eintretenswahrscheinlichkeit. In dieser Konstellation liegen Unfallstatistiken oft im Bereich der Zufallsvariation. So entwickelten sich in der Aviatik bereits in den 70ern alternative Methoden der Risikofindung, wozu auch Beinahe-Unfallmeldesysteme gehören – *Critical Incident Reporting Systems* oder *CIRS*, wie sie auch genannt werden. Diese werden seit einiger Zeit zunehmend auch im Medizinsektor umgesetzt. Die wichtigsten Merkmale sind: 1.) Meldungen können *anonym* erfolgen, 2.) Es sind *grosse Personalbestände* involviert, 3.) Die Erfassungsmethodik ist mindestens teilweise *qualitativ* (Klartext-Fallbeschreibungen, Skizzen Fotos etc.)

Illustrativ für das Verständnis von CIRS ist – als Beispiel – das Formular, welches im Rahmen des US-amerikanischen *Aviation Safety Reporting System (ASRS)*[3] verwendet wird. 2013 wurden damit im Schnitt täglich über 300 Beinahe-Ereignisse erfasst. Die drei Seiten dieses Formulars sind zur Hälfte leer, was hohe Anforderungen an die Erfassungsmethodik stellt: Es muss einerseits, durch Inhaltsanalyse und Kategorienbildung vom Einzelfall auf generalisierbare Zusammenhänge geschlossen werden können, andererseits muss die Methodik so flexibel sein, dass neue Trends nicht übersehen werden.

Feedback von Praktikern aus Netzbetrieb und Industrie

Im Juni 2015 hat der Autor bei fünf Netzbetreibern und drei global tätigen Schweizer Industrieunternehmen anhand einer Kurzumfrage sondiert, in wie weit vorstehende Theorien in der AuS-Praxis und darüber hinaus im Elektrofach diskutiert oder umgesetzt werden. Ein Quervergleich im Plenum der AuS Tagung in Köln erhärtete einige Hypothesen und Trends, natürlich ohne statistische Aussagekraft. Zusammenfassend ergab sich, dass das Aufspüren und Bereinigen unsicherer Situationen zunehmend auf dem Radar der befragten Praktiker ist, dass Meldesysteme implementiert sind, und dass diese teilweise signifikant abweichen von Systemen wie sie in Aviatik und Medizin geläufig sind, besonders hinsichtlich Anonymität.

Dass es einen Zielkonflikt gibt zwischen dem Bedürfnis nach Persönlichkeitsschutz und dem Bedürfnis nach Verifizierung und vertiefter Abklärung, zeigt auch das erwähnte Formular des ASRS: Es verlangt Kontaktdaten der meldenden Person, bei zugesicherter Vertraulichkeit. Von den befragten Praktikern relativierten mehrere die Bedeutung von Anonymität, meist

[3] http://asrs.arc.nasa.gov/ (25.6.2015). Ergänzend: Connel, L. J., (2004), Cross Industry Applications of a Confidential Reporting Model. NASA / ASRS Publication #62

weil bei kleineren Betrieben oder dezentraler Organisationsstruktur die meldende Person einfach zu identifizieren ist. So schälte sich aus allen Interviews schnell die Zentralität von Vertrauen heraus, und zwar in dem Sinn, dass ein von persönlichem Vertrauen geprägtes Betriebsklima als valable Alternative zu (blindem) Vertrauen in anonymisierte Systeme gesehen wird[4].

Eher kontrovers wird die Kopplung von Ereignis-Meldesystemen mit Anreizen (Prämien etc.) oder Bonus-Malus-Systemen beurteilt. Einerseits, weil die Qualität von Meldungen kaum objektiv messbar ist – weil also wertvolle und eher redundante Meldungen schwer zu unterscheiden sind – andererseits weil gerade ein Malus möglicherweise Vertuschungen und Pseudo-Aktivitäten befördert[5]. Die Erhebung gibt Hinweise, dass in Einzelfällen Zielkonflikte bestehen, einerseits zwischen dem Bedürfnis des Managements nach einfachen, standardisierten Abläufen, und andererseits dem auf Praktiker-Ebene vorherrschenden Bedürfnis nach konkreten Lösungen für konkrete Probleme.

Fazit

Der *Schutz der meldenden Personen* vor negativen Konsequenzen gilt allgemein als elementar für den Erfolg von Beinaheunfall-Meldesystemen. In diesem Punkt decken sich die Feedbacks der AuS-Praktiker mit einschlägiger Literatur, zum Beispiel einer vom Safety Office des Zürcher Flughafens unterstützten Fallstudie, welche sich mit *Barrieren und Motivatoren* für das Meldverhalten befasst[6]. Diese Studie stützt auch ein anderes Umfrageergebnis: Der Erfolg von Meldesystemen wird massgeblich mitbestimmt von der *Reaktion auf Meldungen:* Reagiert das Management nicht oder unangemessen auf Inputs der Belegschaft, stirbt jede Art von Verbesserungssystem oder mutiert, im schlechteren Fall, zu einem Kanal für Denunzierungen und/oder zu einer Quelle von Misstrauen.

Ein oft gehörtes Stichwort bei dieser Erhebung war *Kultur*: Unternehmenskultur, Sicherheitskultur, etc. Das klingt gut, wird aber oft verschieden verstanden. Leitfragen können beispielsweise sein: *Wie trifft die Organisation ihre Entscheidungen? Was entscheidet darüber, ob Beinaheunfälle vertuscht oder nur unter Kollegen besprochen werden? Wie denken Mitarbeitende an der Front über Anonymität?* Insgesamt ist nicht anzuzweifeln, dass Beinahe-Unfälle auch im Elektrosektor Lektionen sind, und dass sich der Sicherheitslevel durch Meldesysteme anheben lässt. Bedingung dafür ist das Vorhandensein eines betrieblichen Sicherheitssystems, in welchem das Meldesystem komplementär zu sicheren Anlagen, guter Ausbildung, Instruktion und Ausrüstung und zu unabhängigen Sicherheitsaudits seine positiven Effekte optimal entfalten kann[7].

---

[4] Zum Nexus von Vertrauen und Misstrauen findet sich bei Luhmann bereits 1968 der Hinweis, dass es sich dabei nicht nur um Gegenteile handelt, sondern um *funktionale Äquivalente*. In Luhmanns Sicht bedingt die Entstehung von Vertrauen das Einbringen einer *riskanten Vorleistung*. Quelle: Luhmann, N., (1968; 53, 92), Vertrauen, Lucius & Lucius, Stuttgart. Bezug nehmend auch auf Thompson, J.W. (1963), The Importance of Opposites in Human Relations. Human Relations 16, 163-169.

[5] Gerade bei Beinahe-Unfällen muss eine hohe oder ansteigende Zahl von Meldungen nicht zwingend als Erfolgsmeldung, sondern kann genauso gut als Alarmzeichen gelesen werden.

[6] Bogdanovic, J. (2012), Incident Reporting: Motivatoren und Barrieren beim Berichten von kritischen Ereignissen. Master-Thesis, Fachhochschule Nordwestschweiz, FHNW.

[7] Ein Sicherheitssystem betreiben heisst: Risiken finden, risikomindernde Massnahmen umsetzen und Restrisiken tragen (oder versichern). Bei den risikomindernden Massnahmen wird dem Ersatz eines gefährlichen Stoffes, Arbeitsmittels oder einer gefährlichen Tätigkeit die höchste Wirksamkeit zugeschrieben (S-Massnahme, für Substitute = Ersatz). Gemessen an ihrer Wirksamkeit folgen dann technische (T) organisatorische (O) und persönliche (P) Massnahmen. Auf dieser Unterscheidung basiert das STOP-Prinzip der Unfallprävention. Mehr Information (Beispiel): http://www.suva.ch/startseite-suva/praevention-suva/arbeit-suva/sicherheitssystem-suva.htm (26.6.2015)

Bei AuS werden typischerweise sehr detailreiche Arbeitsanweisungen verwendet, was als Parallele zu Aviatik und Medizin gesehen werden kann. Die Rückmeldungen aus der Praxis geben keine Hinweise darauf, dass anonymisierte CIRS bei AuS mehr Nutzen versprechen als bei „normalen“ Tätigkeiten im Umfeld elektrischer Anlagen. Die Frage, ob anonyme oder persönliche Rückmeldekanäle mehr Erfolg versprechen dürfte vielmehr von der Grösse der Organisation abhängig sein.

Die klassischen Statistiken über Elektrounfälle bleiben natürlich für das Erkennen von Risiken zentral, wobei ein gewisser Grad von Blindheit für neuere technische Entwicklungen wie z.B. AuS bemängelt wird. Dieses Problem ist allerdings systemimmanent, weil für langfristige Vergleichbarkeit gewisse Betrachtungsfelder und Kategorien starr vorgegeben sein müssen. Häufig hört man von Praktikern, dass ganze Unfallberichte anonymisiert veröffentlicht werden sollten, um maximalen Nutzen in der Unfallprävention zu erreichen. Dass dieser Vorschlag auch bei Beinahe-Unfällen Gültigkeit haben könnte, ist nicht von der Hand zu weisen, wobei die erwähnten Fallstricke betreffen Persönlichkeitsschutz in Erinnerung zu rufen sind. Im Zweifelsfall ist es sicher nie falsch, die Einwilligung Betroffener zu erfragen, wenn die Publikation eines Fallbeispiels angedacht ist.

Es entstand an der 10. AuS-Fachtagung in Köln insgesamt der Eindruck, das Wertvollste an Beinahe-Unfall-Erfassungssystemen liege für den Elektrosektor in der etwas ungewohnten Perspektive, aus der auf altbekannte Herausforderungen geblickt wird: Die Idee erfordert einerseits ein Klima des Vertrauens innerhalb der Organisation (sonst wird eher vertuscht als gemeldet), andererseits kann der Fokus auf Beinahe-Ereignisse genau dieses Vertrauen auch befördern. Vor zu viel Euphorie sei allerdings gewarnt: Wie gezeigt können bereits kleine Fehler des Managements das angestrebte Vertrauensklima kippen lassen. Die Erfahrung zeigt, dass sich positive Effekte meist aus der Summe bescheidener, überlegter Einzelschritte ergeben.

28.6.2015, revidiert Nov. 2018

Hansueli Homberger verfügt über ein Meisterdiplom im Elektrogewerbe, das EKAS-Diplom als Sicherheitsfachmann sowie einen Master in Friedensförderung und Konfliktanalyse vom Advanced Study Center der Universität Basel. Er bietet seit 2013 als unabhängiger Berater Audit-Dienstleistungen, Trainings und mehr an (www.h-connect.ch). Davor war er 10 Jahre bei der akkreditierten Inspektionsstelle Electrosuisse als Sicherheitsdelegierter, Auditor, Berater für Elektro-Sicherheitskonzepte und Inspektor tätig, nach langjähriger Berufserfahrung im Elektro-Installationsgewerbe.