Thilo Paul-Stueve (Hrsg.): Mensch & Computer 2007 Workshopband. Weimar: Verlag der Bauhaus-Universität Weimar. 2007, S. 105

Alarmqualität und Anlagensicherheit

Martin Hollender

ABB Forschungszentrum Ladenburg

Zusammenfassung

Ein Alarm ist definiert als eine Meldung, die ein unmittelbares Eingreifen der Anlagenfahrer erfordert. In der industriellen Praxis ist es jedoch häufig leider so, dass ein Großteil der im Prozessleitsystem gemeldeten Alarme völlig bedeutungslos ist. Alarmraten von über 2000 Alarmen pro Anlagenfahrer und Tag sind keine Seltenheit. Diese Masse von Alarmen überfordert die Anlagenfahrer und entwertet das Alarmsystem, sodass auch wichtige Alarme übersehen werden. Somit können Alarme nicht genutzt werden, um sich anbahnenden Problemen rechtzeitig entgegenzuwirken. Die Probleme eskalieren und müssen Sicherheitsbarrieren wie die automatische Schutzabschaltung beanspruchen. Da auch diese Barrieren nicht perfekt sein können, bedeutet jede (unnötige) Inanspruchnahme ein zusätzliches (vermeidbares) Sicherheitsrisiko.

1 Einleitung

Hochautomatisierte sicherheitskritische Produktionsprozesse besitzen eine Vielzahl von Sicherheitsbarrieren (engl. Layers of protection), die das Risiko minimieren sollen. Keine dieser Barrieren alleine kann perfekt sein, aber in der Summe gewährleisten sie eine ausreichend hohe Sicherheit.

Die menschliche Kreativität und die Fähigkeit, auf unvorhergesehene komplexe Ereignisse reagieren zu können, machen die Anlagenfahrer zum unverzichtbaren Bestandteil des Sicherheitskonzepts. Dabei sollen die Anlagenfahrer Störungen bereits so frühzeitig entgegenwirken, dass diese nicht zu einem sicherheitskritschen Problem werden können. Je weniger automatisierte Schutzabschaltungen in Anspruch genommen werden müssen, desto besser. Außerdem ist das An- und Abfahren eines Produktionsprozesses häufig eine besonders kritische Phase und sollte wenn möglich vermieden werden.

Die Anlagenfahrer sollten aber nach Möglichkeit nicht direkter Bestandteil der Sicherheitskette sein (Beispiel: Falls der Anlagenfahrer einen Alarm übersehen würde, käme es zu einer gefährlichen Situation). Hier lassen sich mit Mitteln der Automatisierung in der Regel zuverlässigere Lösungen erreichen.

Es ist offensichtlich, dass ein gutes Alarmsystem eine wesentliche Unterstützung für die Anlagenfahrer ist und somit die Sicherheit erhöht. Leider ist die Qualität der Alarmsysteme in vielen Anlagen nur gering, in einigen Anlagen ist das Alarmsystem de facto unbrauchbar.

In modernen Leitsystemen lassen sich heute sehr einfach große Mengen von isolierten Einzelalarmen konfigurieren. Intelligente Feldgeräte bieten die Möglichkeit, eine Vielzahl zusätzlicher Alarme zu erzeugen. Zudem erfordert der ökonomische Druck einer globalisierten Weltwirtschaft eine Optimierung der Prozessführung, die aber vielfach ein Heranrücken an Stabilitätsgrenzen bedeutet. Dies alles führt dazu, dass bereits im Normalbetrieb sehr viele Alarme generiert werden (über 2.000 Alarme pro Tag und Bediener sind in vielen Anlagen keine Seltenheit). Bei Prozessstörungen sind es oft noch erheblich mehr. Bei dieser Masse von Alarmen kann von keinem Anlagenfahrer erwartet werden, dass er auf jeden einzelnen Alarm angemessen reagiert. Die Reaktion auf Alarme ist nur eine von vielen Aufgaben der Anlagenfahrer. Wichtige weitere Aufgaben sind beispielsweise die Überwachung und Optimierung des Prozesses, die Kommunikation mit Feldpersonal und die Koordinierung von Wartungsmaßnahmen. Unterbrechungen im Minutentakt durch (Fehl-)Alarme, die keinerlei Reaktion erfordern, wirken ermüdend und abstumpfend. Mit der Veröffentlichung der Richtlinie EEMUA 191 im Jahr 1999 hat sich die Erkenntnis durchgesetzt, dass das Alarmsystem die Möglichkeiten der Anlagenfahrer nicht überfordern darf.

2 Die aktuelle Situation in der Praxis

In den Leitwarten vieler heutiger Anlagen lassen sich leicht Symptome für schlechtes Alarmmanagement finden. Dazu gehören:

- Bildschirme sind ständig mit Alarmen gefüllt.
- Häufige Alarme im Normalbetrieb und noch mehr bei Störungen.
- Alarme bleiben für lange Zeiträume (Tage oder Wochen) unbearbeitet stehen.
- Alarme werden, ohne je aufgenommen worden zu sein, „blind“ quittiert.
- Anlagenfahrer empfinden das Alarmsystem nicht als Unterstützung ihrer Arbeit.
- Akustische Alarme werden wegen der konstanten Lärmbelästigung deaktiviert.

In Extremfällen wird das Alarmsystem von den Anlagenfahrern vollständig ignoriert, und die Anlage könnte besser gefahren werden, wenn im Leitsystem überhaupt keine Alarme konfiguriert worden wären! In großen sicherheitskritischen Anlagen wie Raffinerien oder Offshore-Plattformen ist Alarmmanagement oft gesetzlich vorgeschrieben. Sorgfältige Analysen von Unfällen wie der Explosion in der Texaco-Raffinerie in Milford Haven (1994) zeigen deutlich, dass schlechtes Alarmmanagement das Unfallrisiko erhöht. In Milford Haven mussten die Anlagenfahrer in den letzten 11 Minuten vor der Explosion auf 275 verschiedene Alarme reagieren. Aus diesem Grund schreiben einige Behörden wie die britische Health and Safety Executive (HSE) und das Norwegian Petroleum Directorate die Implementierung eines systematischen Alarmmanagements für sicherheitskritische Anlagen vor. Zu den Kern-

aussagen der Richtlinie EEMUA 191 gehört, dass jeder Alarm für den Anlagenfahrer nützlich und von Bedeutung sein sollte, wobei die langfristige durchschnittliche Alarmrate, die für einen Anlagenfahrer im Dauerbetrieb zumutbar ist, bei etwa einem Alarm in zehn Minuten liegen sollte. Außerdem sollten für jeden Alarm Handlungsanweisungen für die Anlagenfahrer vordefiniert werden.

3 Die Qualität von Alarmsystemen

Wesentliche Qualitätsparameter eines Alarmsystems ist die Quote der falsch positiven Alarme (ein Alarm wurde gemeldet, obwohl kein Handlungsbedarf durch die Anlagenfahrer bestand) und der falsch negativen Alarme (es wurde kein Alarm gemeldet, obwohl die Anlagenfahrer hätten eingreifen sollen).

Bei der Inbetriebnahme neuer Anlagen wollen Zulieferer falsch negative Alarme vermeiden, um sich vor Gewährleistungsansprüchen zu schützen: „lieber ein Alarm zu viel als einer zu wenig“. Dies führt bei vielen Neuanlagen zu einer hohen Rate an falsch positiven Alarmen.

Eine zu hohe Alarmrate (EEMUA 191 nennt 1 Alarm pro 10 Minuten und Anlagenfahrer im Normalbetrieb) führt zu einer Überforderung und mindert die Qualität des Alarmsystem erheblich, in Extremfällen wird das Alarmsystem unbrauchbar.

Während einer Prozessstörung wird häufig aufgrund einer einzigen Ursache eine Vielzahl von kausal verbundenen Folgealarmen erzeugt. Den in solchen Situationen häufig unter großem Stress stehenden Anlagenfahrern wird in kürzester Zeit eine Vielzahl verschiedener Alarme präsentiert. Ein gutes Alarmsystem leitet die Aufmerksamkeit der Anlagenfahrer auf die wichtigsten Alarme, die zuerst bearbeitet werden müssen. EEMUA 191 fordert, dass maximal 10 Alarme in den ersten 10 Minuten nach der Störung gezeigt werden sollen. Die Forderung nach einer Begrenzung der Alarmschwallraten ist mit am schwersten zu erfüllen. Moderne Leitsysteme wie das System 800xA von ABB bieten Features wie das „Alarm Hiding“, mit denen man Regeln aufstellen kann, um Alarme oder ganze Alarmgruppen in bestimmten Situationen zu „verstecken“. „Versteckte“ Alarme werden zunächst nicht angezeigt, auf sie kann aber bei Interesse leicht zugegriffen werden.

4 Alarmmanagement

Richtlinien wie EEMUA 191 oder NAMUR NA102 beschreiben, wie durch systematisches Alarmmanagement eine ausreichend hohe Alarmsystemqualität erreicht werden kann. In jeder Anlage sollte ein in sich konsistentes, anlagenweites Alarmkonzept als schriftliches Dokument vorliegen. Darin müssen die Methoden und Regeln zur Festlegung von Alarmkonfigurationsparametern (z. B. ihre Priorisierung) ebenso definiert sein wie die Rollen und Zuständigkeiten der Anlagenfahrer sowie das Änderungsmanagement für die Alarmkonfigurationsparameter.

Die Alarmmeldungen der Anlage sollten in einer Datenbank erfasst und in periodischen Abständen analysiert werden. Alarmmanagementwerkzeuge wie Power Generation Information Management (PGIM) können über den OPC A&E-Standard oder einen Druckeranschluss mit verschiedenen Leitsystemen verbunden werden. Mithilfe dieser Analyse lassen sich Aussagen über die Qualität des Alarmsystems machen und Angriffspunkte für Verbesserungsmöglichkeiten identifizieren.

Im nächsten Schritt werden die Verbesserungen mit dem besten Kosten/Nutzenverhältnis implementiert. Dazu gehört beispielweise:

- Tuning schwingender Regelkreise
- Abschaltung unnötiger Alarme
- Optimierung von Filter- und Hystereseparametern bei der Alarmgenerierung
- Umdefinition von Alarmen zu Meldungen

Da sich die Anlage mit der Zeit verändert, ist es wichtig, Alarmmanagement als routinemäßigen Bestandteil in den Betriebsabläufen zu verankern und kontinuierlich zu wiederholen.

Literatur

EEMUA 191 (2007): „Alarm Systems. A Guide to Design, Management and Procurement“, 2. Auflage 2007 (http://www.eemua.co.uk)

Hollender, M. Atkinson T. (2007): Alarms for operators. Proceedings OECD-CCA Workshop on Human Factors in Chemical Accidents and Incidents, Potsdam

Hollender, M. Beuthel C. (2007): Intelligente Alarmierung. ATP Automatisierungstechnische Praxis 6/2007

Hollifield, E. Habibi (2006): The Alarm Management Handbook, PAS, Houston

ISA RP18.2 (2008): Management of Alarm Systems for the Process Industries (Entwurf)

Namur NA102 (2005): Alarm Management

Norwegian Petroleum Directorate YA-711 (2001): „Principles for alarm system design“, (http://www.ptil.no/regelverk/R2002/ALARM_SYSTEM_DESIGN_E.HTM)