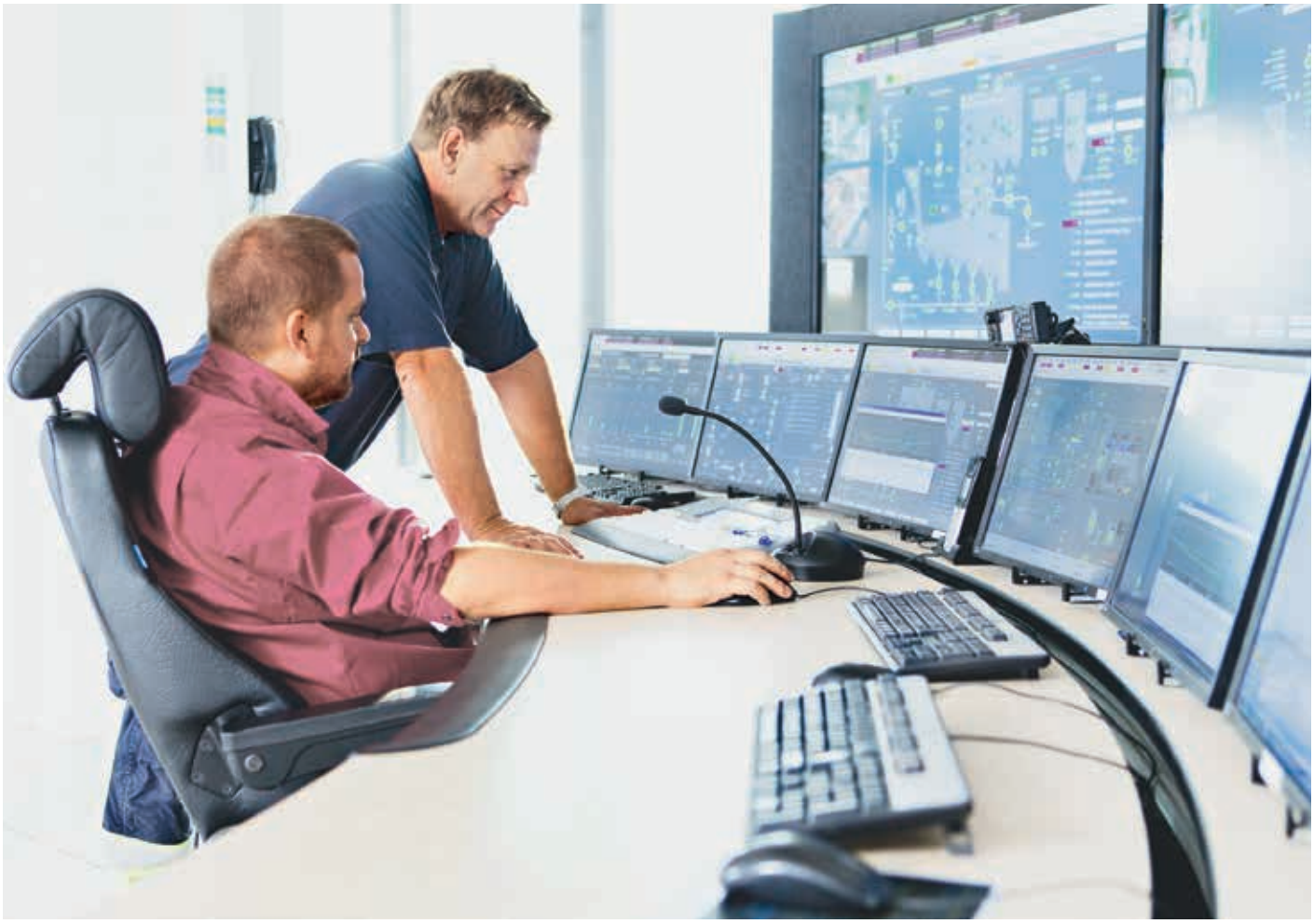


Alarmierende Entdeckungen

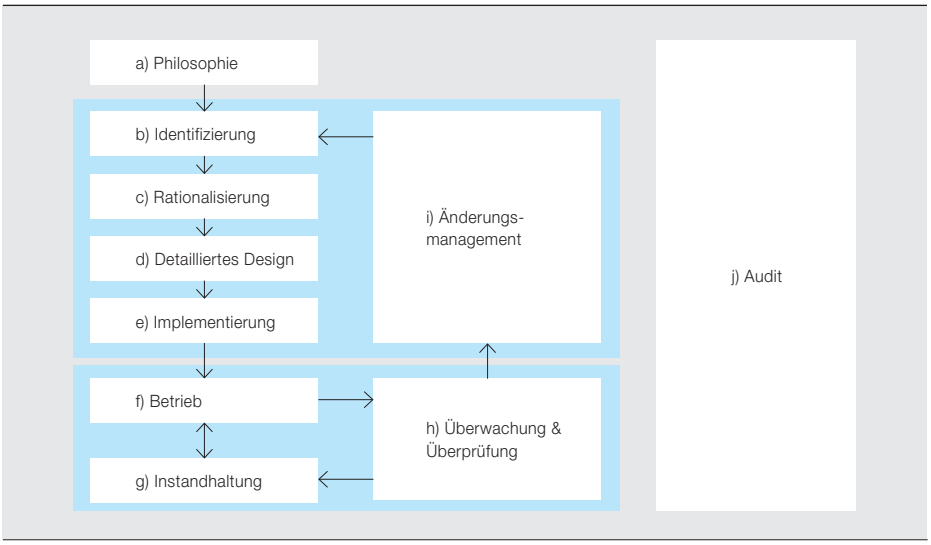
Bessere Bedienereffizienz durch Lebenszyklusunterstützung im Alarmmanagement

MARTIN HOLLENDER, JOAN EVANS, THOMAS-CHRISTIAN SKOVHOLT, ROY TANNER – Der britische Astronaut Tim Peak wurde vor einer Simulationsübung in der Sternenstadt bei Moskau einmal gefragt, was die größte Herausforderung bei einer solchen Simulation sei. Seine Antwort: „Das Schwierigste ist, wenn mehrere Fehler gleichzeitig auftreten“ [1]. Auch in Industrieanlagen mit Prozessleitsystemen gehört die Behandlung von Alarmen, die massenhaft auf das Bedienpersonal einprasseln, nach wie vor zu den größten Herausforderungen. Um diese Alarmfluten unter Kontrolle zu bekommen, muss das gesamte alarmbezogene Designwissen aus der Engineeringphase später in der Betriebsphase, wenn zusätzliches Wissen verfügbar wird, leicht zugänglich sein. Nur so können gehobene Alarmierungstechniken wie Alarmunterdrückung wirklich fachgerecht konfiguriert und optimiert werden. Durch ein gutes Änderungsmanagement und eine entsprechende Lebenszyklusunterstützung kann das Alarmsystem an die sich verändernde Realität in der Anlage angepasst und eine kontinuierliche Verbesserung sichergestellt werden. Alarmmanagementstandards wie IEC 62682 und ISA 18.2 unterstreichen die Bedeutung der Lebenszyklusunterstützung im Alarmmanagement.

1 Der Lebenszyklusgedanke in der funktionalen Sicherheit und im Alarmmanagement

	Funktionale Sicherheit		Alarmmanagement
1996	ANSI/ISA 84.01	2009	ANSI/ISA 18.02
2003	IEC 61511	2014	IEC 62682

2 Lebenszyklus nach IEC 62682



Obwohl die Notwendigkeit eines wirksamen Alarmmanagements mittlerweile allgemein anerkannt ist, zeigen Unfälle wie der Vorfall im Werk von DuPont in Bell, West Virginia, [2] im Jahr 2010, dass es auch bei Unternehmen, die in der Sicherheitstechnik führend sind, Defizite gibt. Seit per Software konfigurierbare Prozessleitsysteme (PLS) in der Industrie gang und gäbe sind, lassen sich zusätzliche Alarme mit minimalem Kostenaufwand für den Endnutzer hinzufügen. Dies hat zu einer sinkenden Alarmsystemqualität in Leitsystemen geführt, weil einfach viel zu viele Alarme konfiguriert wurden. Ein klassisches Beispiel hierfür ist die Explosion in der Raffinerie von Texaco in Milford Haven im Jahr 1994 [3], bei der die beiden Anlagenfahrer in den letzten 11 Minuten vor der Explosion 275 Alarme erhielten. Dies gilt mittlerweile als ein Merkmal für ein überladenes Alarmsystem, das es dem Bedienpersonal unmöglich macht, die Situation richtig einzuschätzen und zu korrigieren. Solche Alarmsysteme sind weder nützlich noch akzeptabel, was schließlich zur Entwicklung systematischer Alarmmanagementansätze geführt hat, die erstmalig in der 1999 veröffentlichten EEMUA-Richtlinie 191 dokumentiert wurden.

Zehn Jahre später wurde das Alarmmanagement in der Norm ISA 18.2 um einen Lebenszyklusansatz ergänzt. Dieser ähnelt dem im Bereich der funktionalen Sicherheit mit der ISA 84 und der IEC 61511 bereits etablierten Ansatz. Einfach ausgedrückt bedeutet dies: Die Gewährleistung eines sicheren Betriebs und eines nützlichen Alarmsystems ist keine Einmalaufgabe, sondern erfordert kontinuierliche Maßnahmen.

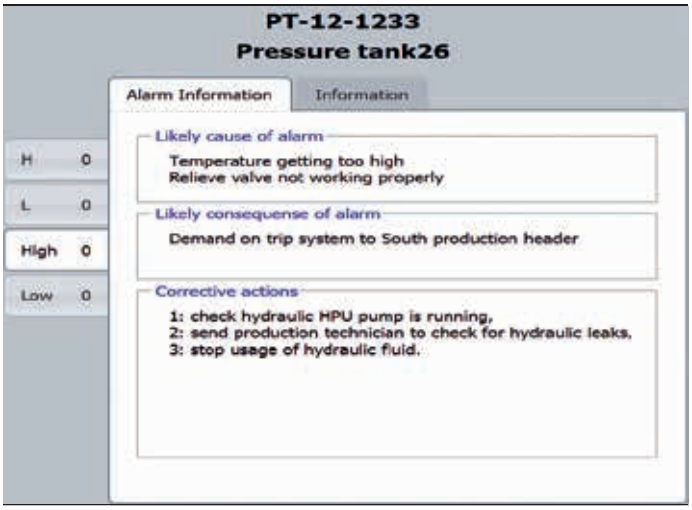
Die neue IEC 62682 (veröffentlicht im Jahr 2014) [4] – die erste internationale Norm für das Alarmmanagement – basiert auf der ISA 18.2 → 1 und betont die Bedeutung eines systematischen Lebenszyklusmanagements. So fordert die IEC 62682 z. B. eine systematische Erfassung und Dokumentation aller für den Entwurf von Alarmen verwendeten Informationen (Sicherheitsstudien, Ausrüstungsspezifikationen usw.). Später, während des Anlagenbetriebs, können die ursprünglichen Designentscheidungen durch weitere Informationen ergänzt oder überprüft werden. Für eine solche Überprüfung müssen sämtliche Informationen, auf denen die ursprüngliche Designentscheidung basiert, verfügbar und vollständig nachvollziehbar sein, um mögliche gefährliche Nebenwirkungen der Änderungen auszuschließen.

Ein klassisches Beispiel für ein überlastetes Alarmsystem ist die Explosion in der Texaco-Raffinerie in Milford Haven, bei der in den letzten 11 Minuten vor der Explosion 275 Alarme aufliefen.

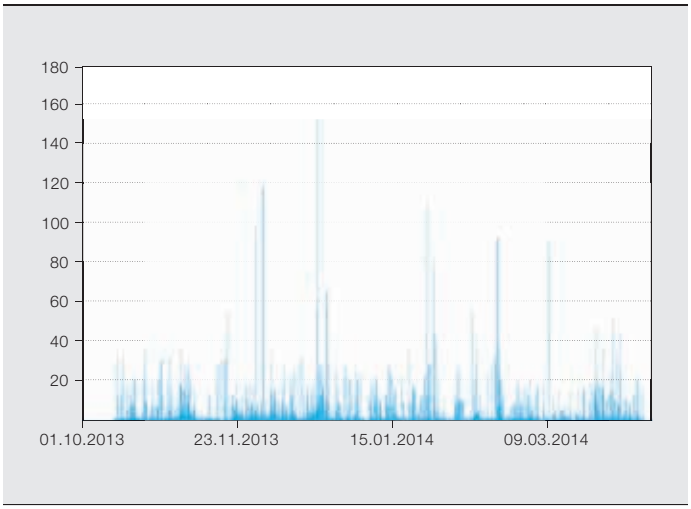
→ 2 fasst den Lebenszyklus gemäß IEC 62682 zusammen und kann als Richtschnur zur Entwicklung und Instandhaltung eines Alarmsystems verwendet werden, das den Anforderungen der IEC 62682 und guter Branchenpraxis entspricht.

Titelbild
Gehobene Alarmierungstechniken bieten wichtige Unterstützung für das Bedienpersonal in modernen Prozessanlagen.

3 Alarm Helper



4 Alarmrate (Alarme in 10 Minuten) über einen Zeitraum von 6 Monaten



Alarmmanagementprinzipien müssen in konkrete Projektaktivitäten übersetzt werden.

Alarmphilosophie

Der erste Schritt im Projektlebenszyklus ist die Alarmphilosophie. Dies ist der Plan, der festlegt, wie Alarme für die betreffende Anlage verwaltet werden sollen. In ihm sind definiert:

- Rollen und Verantwortlichkeiten
- Alarmanforderungen
- Arbeitsabläufe und Verfahren zur Umsetzung der vereinbarten Anforderungen

Die IEC 62682 bietet unter anderem eine nützliche Orientierung für den Inhalt und die Struktur einer geeigneten Alarmphilosophie.

Der Erfahrung von ABB nach liegt die Herausforderung nicht im Verfassen des Dokuments, sondern in dessen Anwendung auf den Projektlebenszyklus. Daher konzentriert sich die Beratungsunterstützung von ABB hierbei schwerpunktmäßig auf die Übersetzung von Alarmmanagementprinzipien in konkrete Projektaktivitäten und -ergebnisse und die Kommunikation der Auswirkungen von Alarmanforderungen an das erweiterte Projektteam.

Dies ist entscheidend, wenn sichergestellt werden soll, dass der Zweck und die Entwurfsabsicht von Alarmen bei Projektüberprüfungen wie Gefahren- und Betriebsfähigkeitsanalysen (HAZOP), Schutzebenenanalysen (LOPA) und Prüfungen der Rohrleitungs- und Instrumentierungspläne (R&I) identifiziert und dokumentiert werden.

Stehen diese Alarmdesigninformationen zur Verfügung, wird im nächsten Projektschritt entschieden, wie und wo alarmbezogene Daten gespeichert und verwaltet werden. Dazu sieht die IEC 62682 das Konzept einer Master-Alarmdatenbank vor, die als „autorisierte Liste rationalisierter Alarme und dazugehöriger Attribute“ definiert ist. Die Umsetzung dieses Konzepts von ABB heißt Alarm Rationalization Tool (ART) und bietet viele wichtige Vorteile:

- Vollständige Datenbankfunktionalität zur Erfassung und schnellen Navigation sämtlicher alarmbezogener Konfigurations- und Designdaten
- Eingabeformulare, bei denen alle Konfigurationseinstellungen für einen Alarm auf einem einzigen Bildschirm angezeigt werden, und die eine effiziente Alarmrationalisierung unterstützen.
- Kontrollierte Kopierfunktionen, die eine Wiederverwendung bestehender Konfigurationen für ähnliche Fälle ermöglichen.

Rationalisierung

Laut IEC 62682 [5] müssen in der Rationalisierungsphase des Alarmlebenszyklus folgende Angaben für jeden Alarm festgelegt werden:

- Empfohlene Bedienerhandlung
- Folgen bei Untätigkeit oder falschen Handlungen
- Mögliche Ursache des Alarms

Stehen diese Informationen während des Betriebs zur Verfügung, führt dies zu konsistenteren Bedienerhandlungen und hilft unerfahrenen Bedienern, eine Wissensgrundlage aufzubauen und Selbstvertrauen zu entwickeln. Dort, wo vorhandene Anlagen modernisiert werden, ist das Bedienpersonal die zuverlässigste Quelle für diese Informationen. Bei neuen Anlagen ist die vollständige Definition der erforderlichen Alarme schwieriger, da man bei der Definition der erforderlichen Alarmkonfiguration stark auf Design- und Anbieterdaten angewiesen ist.

Ein wichtiges Merkmal des ABB ART neben der Erfassung von Alarmanforderungen und Designdaten ist die Möglichkeit zum Export von Bedienerreaktionsdaten an die ABB Online-Funktion Alarm Helper → 3. Alarm Helper stellt diese Informationen auf dem Bedienerarbeitsplatz des Extended Automation System 800xA bereit. Sowohl Alarm Helper als auch ART sind Bestandteil des umfangreichen ABB-Alarmmanagementpakets AlarmInsight. AlarmInsight beinhaltet ein umfassendes Alarmmanagement-Toolset und wurde für die Zusammenarbeit mit System 800xA entwickelt und getestet.

Der unmittelbare Zugriff auf eine solche Online-Hilfefunktion gilt als besonders wichtig für kritische Alarme (IEC-Bezeichnung: „highly managed alarms (intensiv verwaltete Alarme) [6]“) und wird in zunehmendem Maße von Aufsichtsbehörden

5 AlarmInsight-Tool für die Alarmrationalisierung

erwartet. Betriebe, die Alarm Helper bereits verwenden, schätzen ihn als gern genutztes und wirksames Werkzeug zur Bedienerunterstützung.

Kontinuierliche Bemühungen

Im Hinblick auf die Betriebsphase ist das Lebenszyklusmanagement ein zentraler Bestandteil der IEC 62682 und ISA 18.2 und wurde auch in die dritte Ausgabe der EEMUA 191 aufgenommen. Alarmmanagement erfordert kontinuierliche Bemühungen, um eine gleichbleibend hohe Alarmsystemqualität sicherzustellen.

Heutzutage haben viele Anlagen ihre durchschnittliche Alarmrate mit niedrigen Alarmraten im normalen Betrieb gut im Griff. Aber Alarmfluten stellen häufig noch immer eine Herausforderung dar.

→ 4 zeigt die Alarmrate einer petrochemischen Anlage über einen Zeitraum von einem halben Jahr. Obwohl die durchschnittliche Alarmrate bei unter einem Alarm in 10 Minuten liegt und somit gut unter Kontrolle ist, treten zuweilen Fluten von über 100 Alarmen in 10 Minuten und regelmäßig kleinere Fluten von etwa 20 Alarmen in 10 Minuten auf.

Leider treten diese Fluten häufig in den schwierigsten Phasen auf, wenn das Bedienpersonal am meisten Unterstützung benötigt (z. B. beim An- oder Abfahren). Zu den Alarmflutszenarien gehören:

– Alarmfluten, die entstehen, weil Prozessabschnitte heruntergefahren werden (z. B. Alarme aufgrund niedriger Durchflussmengen nach der Abschaltung von Pumpen), sich in unterschiedlichen Betriebszuständen befinden (z. B. Reinigung) oder Messinstrumente kalibriert werden. Diese Alarme können zum Problem werden, wenn sie zusammen mit einem Prozessproblem auftreten und wichtige Alarme in einer Flut von unnötigen Alarmen untergehen.
– Alarmfluten entlang der Ursachenkette nach einer Prozessstörung. Eine einzelne Ursache kann zu einer Vielzahl von Folgealarmen führen. Dabei muss der erste Alarm in der Alarmliste der Hauptursache nicht unbedingt am nächsten liegen – je nach Prozessdynamik und Konfiguration der Schwellenwerte können sekundäre und irreführende Alarme zuerst auftauchen.

> Alarmfluten lassen sich nicht allein durch die Wahl guter Konfigurationswerte für Grenzen, Hysterese- oder Verzögerungstimer verhindern.

Solche Alarmfluten lassen sich nicht allein durch die Wahl guter Konfigurationswerte für Grenzen, Hysterese- oder Verzögerungstimer verhindern. Hier kommen gehobene Alarmierungstechniken wie das Verbergen (IEC 62682: „suppression-by-design“) und Gruppieren von Alarmen ins Spiel. ABB System 800xA bietet eine Reihe von leistungsstarken Tools für die gehobene Alarmierung auf Controller-, Server- und Arbeitsplatzebene einschließlich Gruppierung, Verbergen (dynamisches Unterdrücken) und Zurückstellen (zeitlich begrenztes, bedienergesteuertes Unterdrücken) von Alarmen.

Kalkuliertes Risiko

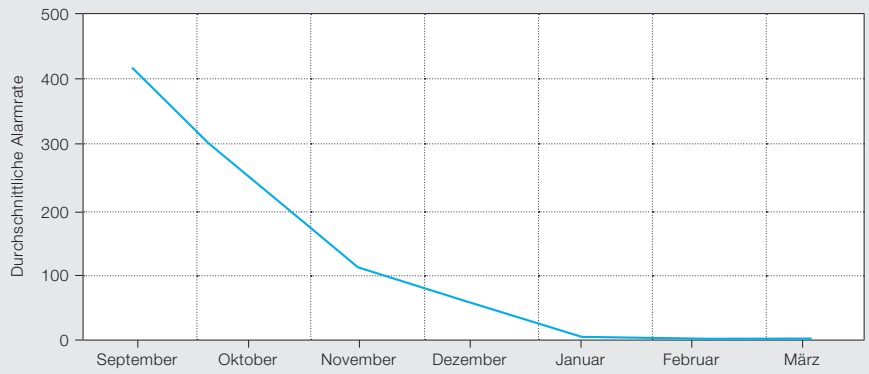
Die Herausforderung bei der Behandlung von Alarmfluten besteht darin, einen Mittelweg zu finden zwischen den möglichen Risiken, die die Unterdrückung eines Alarms in einer bestimmten Situation mit sich bringt, und der Notwendigkeit, Spitzen in der Alarmrate bei außergewöhnlichen Zuständen zu reduzieren. Diese Risiken lassen sich am besten durch eine Kombination aus bewährten, umfassenden Toolsets wie ABB AlarmInsight → 5 und einem robusten Änderungsmanagement mit einem entsprechenden Prüfungs- und Genehmigungsprozess mindern.

In anfänglichen (vorausschauenden) Rationalisierungsprüfungen können bereits Kandidaten für eine grundsätzliche Alarmunterdrückung ermittelt werden – z. B. die Gruppierung von Alarmen, die ausgeblendet werden sollen, wenn ein bestimmtes System außer Betrieb ist. Später kann dies durch die Untersuchung von Alarmfluten während der Betriebsphase verfeinert werden, wobei auf die Funktionen von AlarmInsight zurückgegriffen werden kann:

– Bedienerkommentare zu Alarmreaktionen, die in Alarm Helper gespeichert und dargestellt werden

ABB konnte die durchschnittliche Alarmrate in einer Offshore-Gasanlage senken und die Anlagenabschaltungen von 25 auf sechs im Jahr reduzieren.

6 Reduzierung der Alarmrate in der Offshore-Gasanlage von Rashpetco mit ABB AlarmInsight



– Detaillierte Alarmanalyse mit Expert Tool und Alarm Analysis
– Aktuelle Alarmattribute aus der ART-Datenbank

Dieses kombinierte Toolset erleichtert die Identifizierung möglicher Szenarien zur Alarmunterdrückung durch die Analyse echter Anlagendaten. Dadurch, dass die Notwendigkeit manueller „Ad-hoc"-Analysen entfällt, reduziert sich die Möglichkeit menschlicher Fehler bei der Herleitung von Ursache und Wirkung erheblich. Außerdem können Schlussfolgerungen auf der Grundlage viel umfassenderer Datensätze getroffen werden, die sich über mehrere Jahre erstrecken können. Ist ein bestimmtes Szenario identifiziert, geprüft und bestätigt, kann mithilfe des Toolsets geprüft werden, ob es weitere Fälle gibt, auf die dieselbe Logik angewandt werden kann. Die Produktintegration zwischen System 800xA und AlarmInsight ermöglicht eine kontinuierliche Optimierung, Sicherstellung und Überwachung von Alarmen.

Dieser Ansatz hat seinen Nutzen bereits in einer Reihe von Fällen unter Beweis gestellt, z. B.:
– Erkennung von Folgealarmen nach einem bestimmten Shutdown
– Analyse kritischer Ereignisse mit Hervorhebung von Auslösern, die eine frühe Bedienerreaktion (Eingriff) erfordern und eine Systemabschaltung/Anlagenstörung verhindern könnten.

Die Hauptvorteile werden durch ein Lebenszyklus-Toolset ermöglicht, das die Grundlage für eine kontinuierliche Verbesserung bildet. Zu den Vorteilen gehören:
– Weniger Produktionsabschaltungen
– Geringeres Unfallrisiko, weniger Gefahren für die Umwelt, Einhaltung aller relevanten Vorschriften und Normen
– Verbesserte Bedienereffizienz

→ 6 zeigt, wie es ABB gelungen ist, die durchschnittliche Alarmrate in einer Offshore-Gasanlage der Rashid Petroleum Company (Rashpetco) zu reduzieren. Das Ergebnis war eine Minderung der Anlagenabschaltungen von 25 auf sechs im Jahr. Da jede Abschaltung mit hohen Kosten verbunden ist, bedeutet dies erhebliche Einsparungen für das Unternehmen.

Fazit

Alarmmanagement ist ein Bereich mit wachsender Bedeutung sowohl für Aufsichtsbehörden als auch die Öffentlichkeit, die den Nachweis eines lebenszyklusorientierten Ansatzes und kontinuierlicher Verbesserung zur Gewährleistung eines sicheren Anlagenbetriebs fordern. Mit der IEC 62682 stehen bewährte Verfahrensweisen des Alarmmanagements nun auch als internationale Norm zur Verfügung. Hierzu bietet ABB einen umfassenden Werkzeugkasten, mit dem nachweislich Einsparungen erzielt und ein auch von den Aufsichtsbehörden als vorbildlich angesehenes Alarmmanagement erreicht werden kann.

Martin Hollender
ABB Corporate Research
Ladenburg, Deutschland
martin.hollender@de.abb.com

Joan Evans
ABB Process Automation, Oil, Gas & Chemicals
Billingham, Großbritannien
joan.evans@gb.abb.com

Thomas-Christian Skovholt
ABB Process Automation, Oil, Gas & Chemicals
Oslo, Norwegen
thomas-christian.skovholt@no.abb.com

Roy Tanner
ABB Process Automation, Control Technologies
Wickliffe, OH, USA
roy.tanner@us.abb.com

Literaturhinweise

[1] D. Shukman (11. November 2015): „Tim Peake: British astronaut's training nears end". Verfügbar unter http://www.bbc.com/news/science-environment-34788169
[2] S. Smith: „Did DuPont Prioritize Cost Over Safety at Belle, W.Va., Facilities? Chemical Safety Board Investigation Indicates It Did". EHS Today, Juli 2011
[3] „The explosion and fires at the Texaco Refinery, Milford Haven, 24 July 1994". Health and Safety Executive. Norwich, 1997
[4] „Alarmmanagement in der Prozessindustrie". DIN-EN 62682 (VDE 0820-382), 2015
[5] „Geforderter und empfohlener Inhalt der Alarmphilosophie". DIN-EN 62682 (VDE 0820-382), Abschnitt 6.2.1, Tabelle 3
[6] „Intensiv verwaltete Alarme" (engl. Highly Managed Alarms). DIN-EN 62682 (VDE 0820-382), Abschnitt 6.2.9