Sicherheitsmanagement in der Prozessindustrie

Teil 2: Der Ansatz von ABB

Robert Martinez, Per Christian Juel, Per Fjelldalen

Die sichere Durchführung industrieller Prozesse erfordert einen strukturierten Ansatz, der auf alle betrieblichen Aspekte und Ebenen angewandt wird und darauf ausgelegt ist, das aus dem Prozess resultierende Gesamtrisiko zu minimieren.

ABB blickt auf eine lange Tradition als Lieferant von Sicherheitssystemen für industrielle Prozesse zurück. Die hierbei gewonnene Erfahrung kommt dem Unternehmen bei der Implementierung neuer Sicherheitsstandards wie der IEC 61508 und der IEC 61511 und deren Integration in das unternehmenseigene Prozessleitsystem System 800xA zugute.

Seit mehr als 25 Jahren entwickelt ABB Sicherheitssysteme für die Prozessindustrie und gehört zu den erfahrensten Anbietern von programmierbaren Sicherheitssystemen.
Dank der hierbei gewonnenen Erfahrungen ist ABB in der Lage, ihre Kunden in der Prozessindustrie bei der Bewältigung der technischen, organisatorischen und finanziellen Herausforderungen, die mit strengen Sicherheitsmanagementvorschriften verbundenen sind, zu unterstützen. Ein weiterer bedeutender Vorteil von ABB ist das Prozessleitsystem System 800xA[1)], das eine umfangreiche Palette an sofort verfügbaren Services zur Umsetzung eines eng integrierten Managements nach IEC 61511[2)] ermöglicht. Dazu gehören Auditierung, Authentifizierung, Zugriffsmanagement, Dokumentenmanagement, Anlagen- und Betriebsmittelüberwachung und die Integration eines computergestützten Wartungsmanagementsystems (CMMS). Diese und andere Softwaredienste bieten Funktionalitäten, die dabei helfen, eine nachweisliche Erfüllung der Anforderungen über die Betriebsphasen des Sicherheitslebenszyklus hinweg zu gewährleisten.
ABB Corporate Research in Norwegen hat untersucht, inwieweit die System 800xA-Plattform die IEC 61511 bereits erfüllt, um festzustellen, in welchen Bereichen die Norm noch stärker unterstützt werden kann. Die Studie ergab eine Möglichkeit zur Abdeckung des vollständigen Lebenszyklus durch Funktionalitäten zur Unterstützung der folgenden Planungs- und Engineering-Phasen:

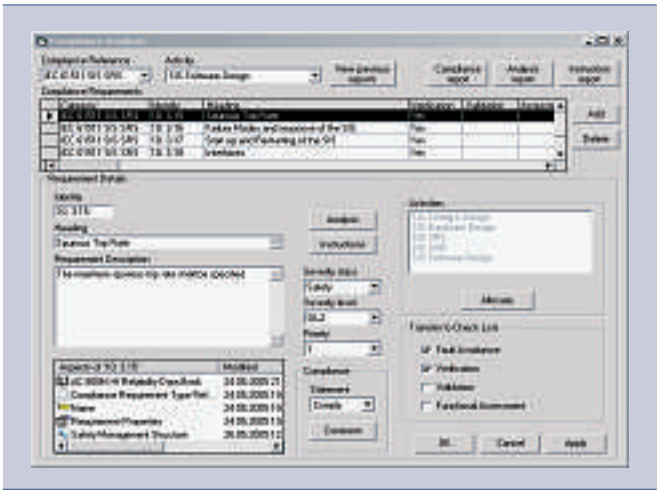
- Sicherheitstechnisches Projektmanagement
- Gefährdungs- und Risikoabschätzung
- Auslegung der Sicherheitsfunktionen hinsichtlich Integrität und Zuverlässigkeit
- Sicherheitsbezogene Programmierung von Ursache-Wirkungs-Matrizen

ABB Corporate Research hat zusammen mit der Abteilung für Sicherheit von ABB Process Automation die Vorteile eines «Safety Workplace»-Pakets für das System 800xA untersucht, das die bestehenden und geplanten Funktionalitäten zu einer nahtlosen Lösung kombiniert, die sowohl Benutzer mit Engineering- als auch Betriebsführungsaufgaben unterstützt.
Auch die beratende Rolle von Sicherheitsexperten wurde nicht außer Acht gelassen. Die vorgeschlagene Reihe von Sicherheitstools *(Safety Tool Chain)* wurde als tragbares System mit einem Minimum an Abhängigkeiten und einem offenen Design konzipiert, um den Import von Daten aus verschiedenen Quellen zu erleichtern. Diese Merkmale sind besonders wichtig für die beratenden Sicherheitsingenieure von ABB beim Kunden vor Ort und bei Kundenschulungen. 2004 wurden Prototypen für das sicherheitstechnische Projektmanagement und die Programmierung von Ursache-Wirkungs-Matrizen fertig gestellt.

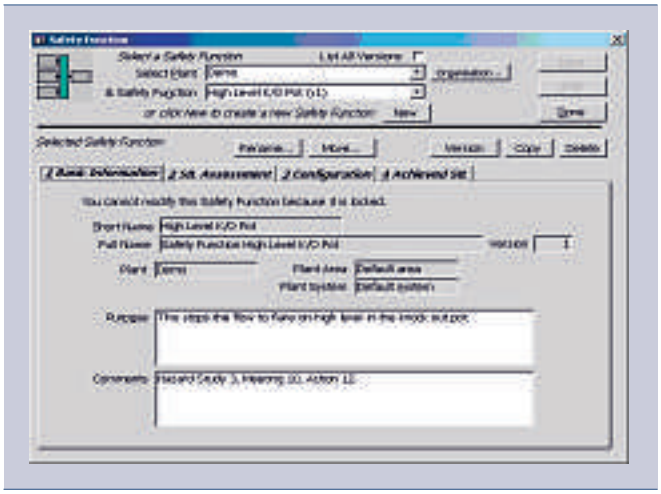
Unterstützung für sicherheitstechnisches Projektmanagement

Der Geschäftsbereich ABB Process Auto-

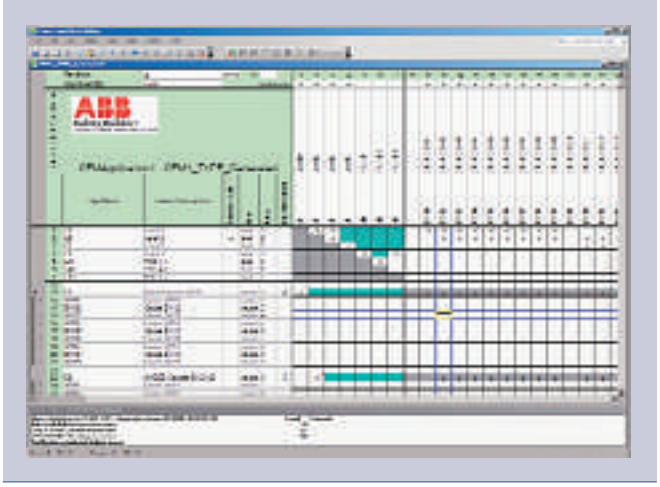
1 Bildschirmausdruck des Compliance Managers



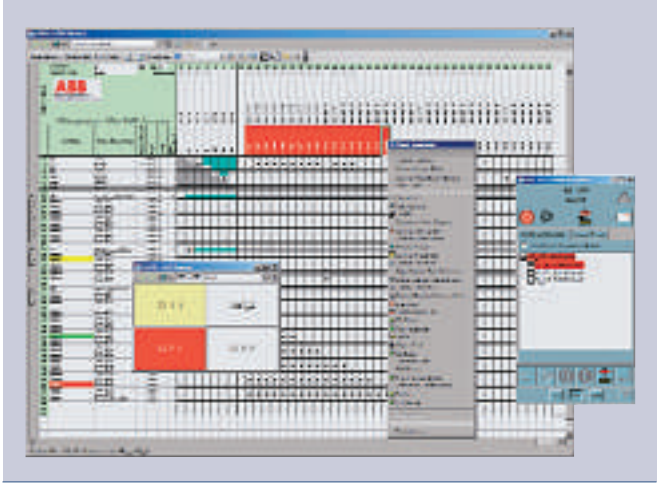
2 Bildschirmausdruck des ABB TRAC (Trip Requirement and Availability Calculator) zur SIL-Berechnung



3 Bildschirmausdruck des System 800xA Safety Builder Editors



4 Bildschirmausdruck des System 800xA Safety Builder Viewer-Tools

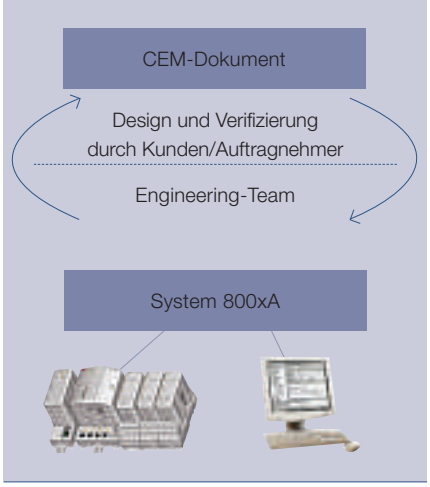


mation hat in seiner Produktentwicklung ein formelles und TÜV-geprüftes Sicherheitsmanagementsystem implementiert. Diese Zulassung war eine notwendige Voraussetzung für die erfolgreiche Entwicklung des neuen AC 800M HI Sicherheitscontrollers. Der für diese Zulassung erforderliche Wissenspfad lieferte wertvolle Eingaben für den Prototyp eines Tools, das nun für den Rollout an Projektteams und Kunden bereit ist: der «Compliance Manager».
Compliance Manager unterstützt den Benutzer bei der Bildung von Sicherheitsteams, der Beschreibung von Kompetenzen der Teammitglieder und der Zuweisung von Zuständigkeiten mit Hilfe einer Verantwortlichkeitsmatrix (RACI). Über den eingebauten Compliance Editor können alle möglichen Anforderungssammlungen eingegeben werden. Die Norm IEC 61511 wird vorher geladen, sodass der Benutzer sofort mit der produktiven Arbeit beginnen kann 1. Zu den Funktionen zählt eine Lückenanalyse gegen die Anforderungen mit anschließender automatischer Erstellung von Prüflisten und Spezifikationsunterlagen. Ebenfalls in das Tool integriert ist eine ABB-Interpretation der IEC 61511 und ihrer Anwendbarkeit auf die unternehmenseigenen Systeme. Dank dieser Funktion sind die Ingenieure von ABB in der Lage, schnell und einheitlich auf kundenspezifische Sicherheitsanforderungen und Spezifikationen zu reagieren.

Design und Programmierung des Sicherheitssystems

Im Anschluss an die Konfiguration der Sicherheitsfunktion (SIF)[2] wird die Zuverlässigkeit sämtlicher Komponenten in die Berechnung einer Sicherheitsintegritätsstufe (SIL) eingegeben, um zu prüfen, ob die angestrebte Risikominderung erreicht wird. Diese Berechnung ist keinesfalls banal, vor allem wenn die Auswirkungen von Redundanz- und so genannten Common-Cause-Fehlern (Fehler bzw. Ausfälle gemeinsamer Ursache) berücksichtigt werden. Passenderweise hatte eine Gruppe von Sicherheitsingenieuren bei ABB Engineering Services in England zu einem früheren Zeitpunkt ein unabhängiges Tool zur SIL-Berechnung mit der Bezeichnung TRAC (Trip Requirement and Availability Calculator) entwickelt 2. Das ABB-Team in Norwegen erarbeitete eine Roadmap zur Integration des Berechnungstools mit dem System 800xA und den anderen im Sicherheitspaket enthaltenen Tools.
Die SIL-Berechnungen sind nicht nur sehr nützlich zur Validierung des SIF-Designs, sondern können auch wertvolle Daten wie Zeitintervalle liefern, nach denen der Kunde die SIF-Komponenten auf ihre Funktion hin testen muss. Andere nützliche Angaben aus dieser Phase sind die Verfügbarkeit und Gesamtausfallzeit, der mittlere Ausfallabstand (MTBF) und die mittlere Ausfalldauer (MTTR).
In dieser Phase des Lebenszyklus ist die gesamte SIF-Hardware konfiguriert, doch die Sicherheits-Anwendungssoftware muss noch implementiert werden. Vor der größten Herausforderung in dieser Phase stehen die Programmierer von großen Notfall- und Prozess-Abschaltsystemen (Emergency/Process Shutdown, ESD/PSD). Diese SIS-Systeme erstrecken sich über alle Prozessbereiche und greifen auf eine Vielzahl von Prozessvariablen oder «Tags» zu. Abschaltprozeduren sind normalerweise hierarchisch in mehreren Ebenen aufgebaut, wobei die höheren «Notfallebenen» niedrigere «Prozessebenen» auslösen.
Aufgrund dieser speziellen Anforderungen hat sich die Programmierung mit Hilfe von Ursache-Wirkungs-Matrizen (Cause and Effect Matrix, CEM) zum Defacto-Standard bei der Konzeption von ESD/PSD-Sicherheitssystemen oder Systemen mit Verriegelungslogik entwickelt. Die CEM in ihrer einfachsten Form ist eine Matrix mit bezeichneten «Tags». Die Symbole der Matrix geben an, welche Wirkung (Spalten) eintritt, wenn die entsprechende Ursache (Zeilen) ausgelöst wird 3.
Zur Unterstützung der CEM-basierten Programmierung für Automatisierungsplattformen gemäß IEC 61131 hat ABB das «System 800xA Safety Builder»-Toolkit entwickelt. Das Editor-Tool unterstützt den Anwender bei der optischen und intuitiven Spezifizierung einer komplexen Notfall- und Prozess-Abschaltlogik mit Hilfe eines Matrixgitters. Aus dieser Matrix heraus wird dann automatisch hochwertiger, SIL-zertifizierter Code für den neuen AC 800M HI Controller erzeugt. Anschließend kann das «Viewer Tool» zur Erstellung eines vollständig integrierten Bedieneranzeige- und Navigationselements für das System 800xA aufgerufen werden 4. Das Navigationselement zeigt den Sammelalarm bzw. den Sperrstatus des gesamten Sicherheitssystems aufgeteilt in «Blätter» für die einzelnen Prozessbereiche. Auf diese Weise gelangt der Bediener mit einem Klick zu dem mit dem Alarm verknüpften Blatt und kann auf einen Blick erkennen, welche Geräte und Ebenen abgeschaltet wurden.
Die Tools des System 800xA Safety Builder bauen auf dem Safety Builder für Safeguard auf und zeichnen sich durch zahlreiche neue Funktionen und eine größere Flexibilität aus. Darüber hinaus führt der System 800xA Safety Builder das leistungsstarke Konzept des «Single-Source-Engineering» ein, bei dem Entwurf, Programmierung und Darstellung alle auf demselben Dokument basieren. Durch diesen Designansatz kann das zugrundeliegende CEM-Dokument auch von Auftragnehmern genutzt werden, die nicht über System 800xA verfügen. Das Design wird einfach in der Matrix spezifiziert und das Dokument anschließend zur Generierung des System 800xA-Codes und der Anzeige zurückgeschickt 5. Auf diese Weise wird eine flexible und dezentrale Entwicklung erleichtert.
Übertragungsfehler werden durch die automatische Generierung der Steuerlogik und der Bedieneranzeige aus derselben Designmatrix heraus ausgeschlossen. Damit reduziert sich nicht nur der anfängliche Engineering-Aufwand um den Faktor 10, auch Modifikationen lassen sich leichter implementieren, testen und verfolgen.

5 Flexible Programmierung von Ursache-Wirkungs-Beziehungen



Robert Martinez
Per Christian Juel
ABB Corporate R&D
Billingstad, Norwegen
robert.martinez@no.abb.com
per.c.juel@no.abb.com

Per Fjelldalen
ABB Process Automation
Oslo, Norwegen
per.fjelldalen@no.abb.com

Fußnoten

1) Taft, Mark W.: «Industrial^{IT} System 800xA – Erweiterte Automatisierungslösungen für eine kontinuierliche Produktivitätssteigerung», ABB Technik 1/2004, S. 32–37.

2) Siehe auch Seite 47–50 in diesem Heft.