Ein ganzheitliches Konzept für die Sicherheitsautomatisierung

Wie Technologie, weltweite Normen und offene Systeme zur Steigerung der Produktivität und Gesamtanlageneffektivität beitragen

Von: Dan Hornbeck

Jeder Hersteller hat das Ziel, für seine Mitarbeiter einen sichereren Arbeitsplatz zu schaffen. Darüber hinaus muss jedoch die Produktivität der Einrichtung bewahrt werden, während Produktionsanlagen und die Umgebung geschützt werden sollen. Außerdem ist ein Hersteller, abhängig von der Firmenkultur und vom Standort der einzelnen Einrichtungen, für verschiedene soziale Belange und gesetzliche Kriterien verantwortlich.

Was macht ein Sicherheitsprogramm erfolgreich? Zunächst ist es vor allem die Unterstützung durch das Unternehmen. Diese Unterstützung muss beim Engagement des oberen Managements beginnen und sich bis zu jedem einzelnen Mitarbeiter fortsetzen – dabei müssen alle nach dem Grundsatz „Sicherheit hat Vorrang" handeln.

Sobald die unternehmensweite Unterstützung gewährleistet ist, umfasst ein effizientes Sicherheitsprogramm verschiedene wichtige Faktoren. Diese reichen vom richtigen Einsatz von Schutzbrillen und Gehörschutz bis hin zur Übernahme moderner Fertigungsstrategien und zur Implementierung eines gut konzeptionierten und integrierten Sicherheitsautomatisierungssystems. In diesem White Paper wird vor allem Letzteres beschrieben.

Die historische Betrachtungsweise

In vielen bestehenden Fertigungsanwendungen werden heute überholte Technologien und veraltetes Know-how eingesetzt. Einige dieser Anwendungen wurden ohne Berücksichtigung des Sicherheitsaspekts entwickelt – es wird ausschließlich darauf vertraut, dass Bediener und Instandhaltungstechniker selbst auf die Gefahren achten. Andere Technologien wurden nachträglich implementiert – als Reaktion auf einen Unfall oder nach dem Inkrafttreten neuer Industrienormen. Sie verwenden für die Sicherheit eine Art „Black Box"-Konzept, wobei die Sicherheitslösung vom Automatisierungssystem vollständig isoliert war. Doch auch die Einschränkungen der Sicherheitstechnologie tragen zu diesem reaktiven und separaten Konzept bei. Dabei müssen Maschinen oft zu einem vollständigen Stillstand kommen und sich in einem „sicheren Zustand" befinden, wenn Reparatur- und Instandhaltungshaltungsarbeiten durchgeführt werden müssen oder auch nur ein Bedienerzugriff erforderlich ist. Da diese Stillstandszeit aufgrund eines Sicherheitsereignisses zu einer verringerten Produktivität beiträgt, haben bislang Bediener und Instandhaltungsmitarbeiter das Sicherheitssystem oft umgangen und dabei ihre eigene Sicherheit aufs Spiel gesetzt. Es wurden auch andere Systeme unter Berücksichtigung des Sicherheitsaspekts entwickelt, die jedoch nicht ordnungsgemäß implementiert wurden und die erforderliche Produktivität der Anlage beeinträchtigten – die dabei eingegangenen „Kompromisse" führten dazu, dass beide Seiten nicht vollständig optimiert wurden.

Solche Risiken müssen dank fortschrittlicher, vorgeschriebener weltweiter Normen, maßgeblicher technologischer Innovationen und Risikomanagement nicht länger eingegangen werden und sind auch nicht mehr akzeptabel. Sofern sie mit einem ganzheitlichen Konzept ordnungsgemäß implementiert wurden, lassen moderne Sicherheitssysteme das Beste aus beiden Welten zu – eine sicherere Umgebung für Mitarbeiter, eine geringere Beeinträchtigung der Umwelt, bessere Prozesse und optimierte Produktivität.

Der Einfluss von Normen

Zwar haben sich Sicherheitsnormen im Verlauf der Fertigungsgeschichte immer weiterentwickelt, doch vor allem die jüngste Überarbeitungswelle sorgt für eine Verbesserung der Art und Weise, wie Sicherheitssysteme entwickelt werden. Diese Normen werden im Allgemeinen als funktionale Sicherheitsnormen bezeichnet.

Bislang waren Sicherheitsnormen stets von vorschreibender Natur und boten Anleitungen dazu, wie Steuerungssysteme zu strukturieren sind, um sicherzustellen, dass die Sicherheitsanforderungen erfüllt werden. Diese Normen setzen auf Redundanz, Vielfalt und Diagnoseprinzipien. Sie definierten Ebenen für die „Strukturen" eines Sicherheitssystems, um gewährleisten zu können, dass die Sicherheitsfunktion ausgeführt wird. Doch es fehlte ein äußerst wichtiges Element – Zeit.

Das neue Konzept der funktionalen Sicherheit für weltweite Normen umfasst ein Zeitelement – auch bekannt als Wahrscheinlichkeit eines gefahrbringenden Ausfalls (Probability of Dangerous Failure) und ihrer Umkehr, der mittleren Zeit bis zu einem gefährlichen Ausfall (Mean Time to Dangerous Failure) – und baut auf dem bestehenden Konzept für Sicherheitsstrukturen auf. Mit diesem Zeitelement wird das Sicherheitssystem um einen Zuverlässigkeitsfaktor ergänzt, d. h. es kann davon ausgegangen werden, dass das Sicherheitssystem heute und auch in Zukunft ordnungsgemäß funktioniert.

Zwei wichtige Normen – EN ISO13849-1:2006 und IEC 62061:2005 – wenden das Zeitelement auf Sicherheitssysteme für den Maschinensektor an. EN ISO 13849-1:2006 basiert auf den „Kategorien" der Sicherheitsstruktur, während IEC 62061 auf der Grundlage der Struktur bzw. der so genannten „Hardware-Fehler-Toleranz" basiert. Das Ganze wird um ein drittes Element, die Diagnose (im Grunde genommen nichts Neues) ergänzt, um dem Entwickler des Sicherheitssystems mehr Flexibilität beim Erreichen der sicherheitstechnischen Anforderungen zu ermöglichen. Zusammengenommen ergeben diese drei Elemente einen zeitabhängigen Integritätslevel in einem Sicherheitssystem. IEC 62061 verwendet hier den Begriff „Sicherheits-Integritätslevel" (SIL). Auf Maschinensysteme können nur drei SILs angewandt werden: SIL1, SIL2 und SIL3. EN ISO 13849-1:2006 verwendet den Begriff „Performance-Level" (PL) und anschließend Buchstaben des Alphabets für PLa bis Ple.

Anbieter von Sicherheitskomponenten sind eher für die funktionale Sicherheit verantwortlich. Jeder Komponente im Sicherheitssystem muss eine Wahrscheinlichkeit eines gefahrbringenden Ausfalls oder die mittlere Zeit bis zu einem gefährlichen Ausfall zugeordnet sein. Momentan steht dieser Informationstyp oft nicht zur Verfügung. In der Tat werden derzeit viele Produktentwicklungsnormen modifiziert, um die Kriterien für einen gefahrbringenden Ausfall, Testanforderungen und Statistik-Tools zum Bestimmen der Zeit bis zu einem gefahrbringenden Ausfall zu definieren. Sobald dies abgeschlossen ist, muss in monatelangen Tests der erreichte Level bestätigt werden.

Die Maschinensicherheit wird also ständig weiterentwickelt. Diese Änderung sorgt für mehr Flexibilität bei der Entwicklung sicherer Konstruktionen. Es wird einige Zeit dauern, bis diese Änderung allgemein angenommen werden, doch es gibt beständige Fortschritte. Anbieter von Sicherheitskomponenten setzen nun alles daran, dass diese Anforderungen erfüllt werden. Und Maschinenanbieter müssen sich der funktionalen Sicherheit bewusst werden und herausfinden, wie sie deren Vorteile nutzen können.

Erweitern der technologischen Grenzen

Ein grundlegender Wandel in zwei wichtigen und zusammengehörigen Bereichen hat dieses neue funktionale Sicherheitskonzept erst möglich gemacht. Zum einen wurden wichtige Entwicklungen bei den Sicherheits- und Steuerungstechnologien erzielt – vor allem die Einführung neuer mikroprozessorgestützter Technologien anstelle von elektromechanischen oder fest verdrahteten Steuerungen. Zum anderen wurden weltweite Sicherheitsnormen entwickelt, die die Integration dieser neuen elektronischen Technologien in industrielle Sicherheitssysteme ermöglichen.

Die Fehlerbehebung bei auf herkömmliche Weise fest verdrahteten Sicherheitssystemen kann äußerst schwierig sein, weil sie keinerlei Hinweis darauf geben, wo ein Fehler aufgetreten ist. Beispielsweise sorgt in einem Szenario mit mehreren in Reihe angeschlossenen und in einem Sicherheitsrelais fest verdrahteten Not-Halt-Schaltern ein „offener Schaltkreis" zwischen zwei der Not-Halt-Schalter dafür, dass das Relais die Steuerung informiert und ein sicherer Zustand hergestellt wird. Die Instandhaltungsmitarbeiter müssen anschließend den Grund für den offenen Schaltkreis suchen – möglicherweise wurde ein Not-Halt aktiviert oder der Schaltkreis ist aus einem anderen Grund ausgefallen. Ohne geeignete Diagnose kann dieser Prozess sehr viel Zeit in Anspruch nehmen, was zu einem Produktionsausfall führen kann.

Doch Not-Halt-Ereignisse sind nicht nur schwer zu diagnostizieren, sondern verursachen noch mehr Unannehmlichkeiten. Normalerweise treten sie auf, wenn eine Maschine mit maximaler Kapazität läuft. Dies kann möglicherweise zu Problemen bei der Maschinenausrichtung, zu Materialausschuss, längeren Neustartzeiten und mit der Zeit möglicherweise sogar zu Schäden an der Anlage führen. Diese Faktoren tragen zu längeren Ausfallzeiten und höheren Kosten bei, da eventuell Reinigungs-, Entsorgungs-, Rückstell- oder Verschrottungsarbeiten anfallen und Anlagen wieder in die Ausgangsposition gebracht oder erneut initialisiert werden müssen.

Betrachten Sie auf der anderen Seite ein Szenario, in dem Not-Halt-Schalter mit einem Sicherheits-E/A-Block verdrahtet sind, der über ein sicherheitsfähiges Netzwerk – z. B. DeviceNet oder EtherNet/IP – am integrierten, programmierbaren Standard-/Sicherheits-Automatisierungssystem angeschlossen ist. In diesem Fall werden die Diagnosedaten der Steuerung und der Bedienerschnittstelle (HMI) in einem sofort zugänglichen Format bereitgestellt und die Steuerung oder ein Bediener/Instandhaltungsmitarbeiter kann die entsprechenden Maßnahmen ergreifen, um den Fehler zu beheben. Diese Diagnosedaten könnten darüber informieren, dass der Bediener der dritten Schicht für bestimmte Aufgaben den Not-Halt-Schalter betätigt, anstatt die festgelegten Schritte auszuführen, um ein System in einen sicheren Zustand zu bringen. Möglicherweise geben sie auch Aufschluss darüber, dass ein ernsthaftes Problem der Elektrik vorliegt, das behoben werden muss. In beiden Fällen wird die Ursache des Ereignisses schnell erkannt, sodass das Instandhaltungsteam das Problem beheben und die Produktion schneller wieder aufgenommen werden kann.

Die zweite wichtige Entwicklung in Sachen Sicherheitstechnologie wurde durch dieselbe Marktdynamik gefördert, die auch dazu führte, dass Unternehmen andere Steuerungsabläufe integriert haben (Ablauf-, Achs-, Antriebs- und Prozesssteuerungen). Das Ergebnis ist eine neue Generation von Schutz- und Sicherheitssteuerungsplattformen, bei denen Sicherheitstechnologie bereits in Standard-Automatisierungsprodukte wie programmierbare Automatisierungssteuerungen, programmierbare Sicherheitsrelais sowie frequenzgestellte und Servoantriebe integriert ist. Darüber hinaus sind auch Sicherheitskommunikationsnetzwerke mit hoher Integrität installiert, die Nachrichtenredundanz, Gegenkontrollen und exaktes Timing umfassen. Dadurch könnten Sicherheits- und Standardnachrichten sowie Sicherheits- und Standardgeräte auf gemeinsamen Medien vorhanden sein.

Bisher wurde Sicherheit von der Standardsteuerung getrennt, ganz gleich, ob die Sicherheit mit individuellen Komponenten wie Sicherheitsrelais oder Sicherheitsschützen implementiert wurde oder ob eine dedizierte Sicherheitssteuerung zum Einsatz kam, was unterschiedliche Hardware und Software erforderte. Viele Hersteller schätzen dieses Konzept noch heute, da die einzigen Mitarbeiter, die die Sicherheitshardware und -software einer Anlage kennen, dedizierte Sicherheitsmitarbeiter sind. Anders ausgedrückt: wenn die Mitarbeiter nicht mit der Sicherheitshardware oder Sicherheitssoftware vertraut sind, besteht ein geringeres Risiko einer Sicherheitsbeeinträchtigung – ein fundiertes Konzept, das jedoch im Allgemeinen zusätzliche Kosten nach sich zieht.

Im Gegensatz dazu bietet die Möglichkeit, die Sicherungssteuerung innerhalb einer Architektur zu implementieren, die die vier primären Steuerungsaufgaben ausführen kann, wichtige Vorteile. Für Einsteiger sind die Hardwarekosten minimal, da Systemkomponenten von den Standard- und Sicherheitskomponenten der Anwendung verwendet werden können. Software- und Supportkosten werden ebenfalls reduziert, da dieselbe Software verwendet werden kann und die Mitarbeiter lediglich Kenntnisse zu einer Netzwerkarchitektur erwerben und erweitern müssen. Außerdem können Benutzer abhängig von den Anforderungen der Anwender die erforderliche Hardware implementieren und verteilen, um die Anwendungsanforderungen zu erfüllen. Dabei spielt es keine Rolle, ob es um eine einzelne Maschine oder um eine ganze Anlage geht.

Sicherheitsautomatisierungssysteme können jetzt vollständig in das Standard-Fabrikautomatisierungssystem integriert werden – so entsteht eine einzelne Plattform, die definierte Sicherheitsfunktionen ausführt, die Anforderungen von Sicherheitsnormen erfüllt und die Anlage effizient bedient. In diesem Szenario sind beide Facetten des Automatisierungssystems so konzipiert, dass alle Lebenszyklusaufgaben der Maschine untergebracht werden können. Hierzu zählen Konstruktion, Inbetriebnahme, Bedienung und Instandhaltung. Außerdem können durch dieses ganzheitliche Konzept, basierend auf detaillierten Risikobeurteilungen in den frühen Phasen eines Projekts, Möglichkeiten zur Beseitigung von Gefahren bereits bei der Konstruktion entstehen. Zudem wird die Verkürzung der Instandhaltungsverfahren unterstützt.

Beispielsweise haben Hersteller bisher ihre Mitarbeiter mit der Unterbrechung der gesamten Stromversorgung zur Maschine beauftragt, um Zugang zur Maschine zu erhalten und Instandhaltungsarbeiten ausführen zu können – ein Verfahren, das als „Ausschalten und Sichern" (Lock-out/Tag-out) bekannt ist. Da dieses Verfahren häufig zeitaufwändig war und die allgemeine Verfügbarkeit der Maschine für die Produktion beeinträchtigte, wurde es oft von den Instandhaltungsmitarbeitern des Werks umgangen.

Dank der geänderten Sicherheitsnormen und der Einführung neuer, weiterentwickelter Sicherheitssteuerungen können Hersteller Sicherheitszonen in die Anwendung integrieren, die sich für die unterschiedlichsten Betriebs- und Instandhaltungsszenarien unabhängig verwalten lassen. Diese Konstruktionsflexibilität sorgt dafür, dass die Mitarbeiter des Werks nach Ausführung der erforderlichen Instandhaltungsarbeiten den Betriebszustand der Maschine schneller wiederherstellen können, wodurch die Produktivität verbessert wird. Darüber hinaus sind die Bediener weniger geneigt, das Sicherheitssystem zu umgehen, was die Sicherheit der Anlage erhöht.

Wie diese Beispiele zeigen, ermöglichen gut konstruierte Sicherheitssysteme Produktionsverbesserungen, mit denen sich ihre Implementierung rechtfertigen lässt. Außerdem kann die Industrie mit dem Aufkommen von Normen zur funktionalen Sicherheit, die die Integration von Technologieentwicklungen vorsehen, neue Tools nutzen wie z. B. integrierte Sicherheitssysteme zur Verbesserung der Leistung. Ein ganzheitliches Konzept, das auf Risikobeurteilungen und auf modernster Technologie basiert, kann sicherstellen, dass die Aufgaben für die Instandhaltung und Bedienung der Maschine untrennbar damit verbunden sind, wie Sicherheit gesteuert wird. Das Sicherheitssystem ist nicht länger eine individuelle Einheit – vielmehr handelt es sich um eine kritische Komponente der gesamten Fabrikautomatisierung und des Produktionssystems.

Diese Verbindungen werden zusätzlich durch die Fortschritte bei den Vernetzungs- und Kommunikationstechnologien unterstützt.

Überbrücken der Kommunikationslücken

Die Integration von Sicherheitssteuerungssystemen in ein Standardsteuerungssystem ist ein Anzeichen dafür, dass Sicherheitslösungen in Zukunft flexibel und effizient sein werden. Ein weiteres Anzeichen ist die Kommunikationsintegration unter Verwendung offener Protokolle.

Die nahtlose Kommunikation war in der Vergangenheit nahezu unmöglich, weil kein einziges Netzwerk dazu in der Lage war, Sicherheits- und Standardsteuerungssysteme zu integrieren, während gleichzeitig die nahtlose Übertragung von Daten in mehrere physische Netzwerke im Fertigungsbereich erlaubt war. Dies hat sich mit CIP Safety, einem Netzwerkstandard geändert, der den Anschluss sicherheitsrelevanter Geräte an dasselbe Kommunikationsnetzwerk als Standardsteuerungsgeräte zulässt. CIP Safety basiert auf dem CIP-Standard (Common Industrial Protocol), einem offenen Anwendungsprotokoll für industrielle Vernetzung, das unabhängig vom physischen Netzwerk ist.

CIP Safety sorgt für eine erheblich bessere Integration von Standard- und Sicherheitssteuerungsfunktionen und erhöht die Transparenz der Sicherheit im gesamten System. Dank der Kombination aus schnell reagierenden, zentralen Sicherheitszellen und dem Routing von Sicherheitsdaten zwischen den Zellen entstehen Sicherheitsanwendungen mit schnelleren Reaktionszeiten. Die zusätzliche Flexibilität unterstützt zudem die Beschleunigung von Systemkonfiguration, Tests und Inbetriebnahme.

Eine weitere Integrationsstufe, die häufig übersehen wird, ist die Verwendung von Sicherheitsdaten in einem werksweiten Informationssystem. Da Sicherheitsdaten stets verfügbar sind, kann das Informationssystem eng mit der sicheren Automatisierungsstrategie verbunden sein. Dies führt dazu, dass Informationen, wie z. B. Diagnosedaten, Begründungen für und Häufigkeit der Sicherheitsereignisse, statistische Daten für die Verbesserung der schlanken Fertigung, Produktionsdaten, Sicherheitszugriff und vieles mehr, zur Verfügung stehen.

Ein Grund, warum Sicherheitsnetzwerke bisher im Steuerungsbereich stets isoliert wurden ist, dass die Sicherheitsgeräte und -steuerungen auf die unterschiedlichen Geschwindigkeiten ihres Standardgegenstücks reagieren mussten. Bisher war die Verwendung eines einzelnen Netzwerks zur Unterbringung von Sicherheits- und Standardsystemen eher problematisch, weil ein Netzwerk mit zunehmender Größe auch langsamer wurde. Mit CIP Safety kann die Netzwerkaktualisierungsgeschwindigkeit jedes Netzknotens jedoch unterschiedlich konfiguriert werden. So kann jedes Gerät mit der Geschwindigkeit arbeiten, die für seine Sicherheitsfunktion optimal ist, was auch eine effiziente Zuordnung der Netzwerkbandbreite unterstützt.

Bridging und Routing ist ein wichtiges Leistungsmerkmal von CIP Safety, da es die nahtlose Kommunikation von Sicherheits- und Standarddaten in mehreren und möglicherweise unterschiedlichen physischen Netzwerken ermöglicht. Dieses Leistungsmerkmal macht ein Nachrichtenpfad-Routing ebenso überflüssig wie eine Datenübersetzung und ermöglicht den offenen Fluss der Daten zwischen Netzwerken und Geräten mit minimalem Aufwand für den Systemingenieur. Diese nahtlose Kommunikation ermöglicht Herstellern die Ausführung von Überwachungs- und Datenerfassungsaufgaben auf ihren Standard- und Sicherheitssystemen von einem genehmigten Standort in einer Einrichtung aus.

Die Schutzmaßnahmen innerhalb von CIP Safety unterstützen Kommunikation mit hoher Integrität, wenn Sicherheits- und Standardkommunikation gemeinsam verwendet werden. Dies ermöglicht den Einsatz von Sicherheitssensoren zusammen mit frequenzgesteuerten Antrieben, Standardsensoren, Sicherheitssteuerungen mit speicherprogrammierbaren Standardsteuerungen und Näherungsschaltern. Anwender können die unterschiedlichsten Sicherheits- und Standardgeräte im gleichen Netzwerk verwenden, während die Integrität des Sicherheitsregelkreises erhalten bleibt.

Der größte Vorteil von CIP Safety sind wahrscheinlich die bedienerfreundlichen Funktionen und die Zuverlässigkeit, wie z. B. Bridging und Routing ohne Programmierungsanforderungen. Dies hat effizientere Schulungen, schnellere Inbetriebnahmen und verbesserte Diagnosefähigkeiten zur Folge. CIP Safety-Funktionen in DeviceNet- und EtherNet/IP-Netzwerken verfügen über eine TÜV-Zulassung mit den heute verfügbaren Produkten auf beiden Netzwerken von unterschiedlichen Anbietern. CIP Safety unter EtherNet/IP ermöglicht die Integration von Sicherheitsnetzwerken in dieselbe Ethernet-Architektur, die von Standard-Steuergeräten, dem Internet und vom übrigen Unternehmen verwendet wird.

Auch die Aussichten für die Zukunft sind bestens, da immer mehr Automatisierungsanbieter CIP Safety-kompatible Produkte entwickeln, die eine Integration in Sicherheits- und Standardsteuerungen, -geräte und -netzwerke unterstützen.

Effizientes Risikomanagement

Ein weiterer Lichtblick und kritischer Aspekt eines ganzheitlichen Sicherheitskonzepts ist die vermehrte Unterstützung proaktiver Risikoanalysen von Seiten der Hersteller. Das allgemeine Ziel eines Sicherheitssystems ist es, die Sicherheit von Personen, Prozessen und Maschinen zu erhöhen, ohne die Produktivität zu verringern. Maschinenhersteller, die Risikobeurteilungen vornehmen, können all die oben genannten Vorteile schneller erreichen und tragen so zu einer Verringerung von Risiken und der damit verbundenen Kosten bei.

Die Definition formaler Risikobeurteilungsprozesse, die Risikoidentifikation, Risikoquantifizierung und Risikominderung umfassen, wurde in zahlreiche internationale und regionale Normen aufgenommen wie z. B. IEC 61508, ISO 13849 und ANSI/B155.1. Risikobeurteilungsprozesse, die innerhalb dieser Normen definiert sind, erfordern typischerweise ein Konzept für den gesamten Lebenszyklus, um zu verdeutlichen, wie ein effizienter Prozess implementiert werden muss, um maschinenbezogene Risiken erkennen und das Risikoausmaß hinsichtlich Schwere, Aussetzungshäufigkeit und Vermeidungswahrscheinlichkeit quantifizieren zu können. Das Ergebnis ist ein quantifiziertes Risiko, das mithilfe von Schutzmaßnahmen verringert werden muss.

Durch Risikobeurteilungen steht den Herstellern ein Prozess zur Verfügung, mit dem sie 1) bestimmte Gefahren an einer Maschine erkennen können, 2) das Risiko quantifizieren können, das durch diese Gefahren für die Mitarbeiter besteht, und 3) Methoden beurteilen können, mit denen sich das Risiko vermindern lässt. Außerdem wird bei dem Prozess die am besten geeignete Architektur für den Sicherheitsschaltkreis festgelegt, die erforderlich ist, um das Anfangsrisiko zu mindern, das vom Beurteilungsteam bestimmt wurde.

Sobald die Risiken vollständig definiert und verstanden wurden, müssen sie entweder eliminiert oder bis zum maximal tolerierbaren Ausmaß gemindert werden. Die Maßnahmen für die Risikominderung sorgen für eine physische Verbesserung der Maschine und so für eine Verringerung möglicher Verletzungen von Personen oder Umwelt- und Sachschäden. Die Risikominderung kann mithilfe unterschiedlicher Maßnahmen vorgenommen werden. Eine effiziente Methode ist die Verwendung von Sicherheitseinrichtungen wie Lichtgitter, Sicherheitsrelais und Seilzugschalter, um das Risiko für die Mitarbeiter zu verringern.

Ein formaler Prozess zur Risikobeurteilung bietet auch den Vorteil, dass alle erkannten Risiken, die Schutzmaßnahmen und -vorrichtungen zu deren Minderung und das Restrisiko nach der Implementierung dieser Maßnahmen dokumentiert werden. Durch den Nachweis angemessener Sorgfalt und guter Engineering-Verfahren bei der Bereitstellung einer sicheren Arbeitsumgebung kann ein Unternehmen möglicherweise im Falle eines Unfalls das Risiko von Rechtsstreitigkeiten senken.

Nach der Implementierung und Dokumentation des Prozesses sind geeignete Schulungen und Überwachungsmaßnahmen erforderlich. Es muss unbedingt sichergestellt werden, dass Bediener die Sicherheitsmaßnahmen verstanden haben und z. B. angemessene persönliche Schutzausrüstung verwenden. Bediener müssen so geschult werden, dass sie die Maschinen effizient bedienen und ihre Arbeit sicher ausführen können. Hierzu zählt auch die eindeutige Definition ihrer Aufgaben und der Prozesse im Vergleich zu den Aufgaben, die durch speziell geschulte Instandhaltungsmitarbeiter ausgeführt werden müssen.

Ein umfassendes Maschinensicherheitsprogramm kann den Betrieb im Fertigungsbereich und die Produktivität im Allgemeinen verbessern. Um den vielschichtigen Lebenszyklus der Maschinensicherheit zu vereinfachen, müssen Risikoanalyse, Risikominderung und Schulung/Überwachung miteinander verbunden werden, um die Effizienz des Maschinensicherheitsprogramms beurteilen zu können. Es ist wichtig, dass alle Mitarbeiter im Fertigungsbereich von den Sicherheitsmaßnahmen und den verfügbaren Schulungen profitieren, um ihre Sicherheit zu gewährleisten.

Nutzen Sie die Vorteile eines ganzheitlichen Sicherheitskonzepts

Fortschrittliche Hersteller müssen sich heute mehr denn je auf Lösungen für die Sicherheitsautomatisierung konzentrieren, damit ihre Mitarbeiter sicher sind, ihre Maschinen produktiv arbeiten und ihre Gewinne stabil bleiben. Dank des ganzheitlichen Konzepts der Sicherheitsautomatisierung – bei dem großer Wert auf weltweite Normen, innovative Technologien, geschulte Mitarbeiter und fortlaufende Risikobeurteilungen gelegt wird, die alle zusammenarbeiten – haben Hersteller nun eine Vorlage für bewährte Methoden, um ein hohes Maß an Sicherheit zu implementieren und zu erreichen.

www.rockwellautomation.com

Hauptverwaltung für Antriebs-, Steuerungs- und Informationslösungen

Amerika: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204 USA, Tel: +1 414 382 2000, Fax: +1 414 382 4444
Europa/Naher Osten/Afrika: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgien, Tel: +32 2 663 0600, Fax: +32 2 663 0640
Asien/Australien/Pazifikraum: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, China, Tel: +852 2887 4788, Fax: +852 2508 1846

Deutschland: Rockwell Automation GmbH, Parsevalstraße 11, 40468 Düsseldorf, Tel: +49 (0)211 41553 0, Fax: +49 (0)211 41553 121
Schweiz: Rockwell Automation AG, Industriestrasse 20, CH-5001 Aarau, Tel: +41(62) 889 77 77, Fax: +41(62) 889 77 11, Customer Service – Tel: 0848 000 277
Österreich: Rockwell Automation, Kotzinastraße 9, A-4030 Linz, Tel: +43 (0)732 38 909 0, Fax: +43 (0)732 38 909 61

Publikation SAFETY-WP005-DE-P – Juli 2008