

Sichere Maschinen dank neuer Denkweise

Artikelserie Automation: Sicherheit (7)

Der Begriff Sicherheit ist einem steten Wandel unterworfen. Was gestern von unserer Gesellschaft akzeptiert wurde, gilt heute vielleicht schon als zu gefährlich. Dies hat die Europäische Union (EU) mit der Maschinenrichtlinie 98/37/EG (MRL) erkannt und dem Hersteller Schutzziele vorgegeben. Damit hat die EU den Weg geebnet, dass die Entwickler wegkommen vom reinen Denken in Normen und Vorschriften.

«Welche Sicherheitsvorschriften und Normen müssen wir berücksichtigen?» fragte sich der Hersteller bei der Entwicklung einer neuen Maschine oder eines Sicherheitsbauteils. Dies entspricht

Hans Ruckli, Mario Luzzatto

der alten Denkweise. Mit der Maschinenrichtlinie 89/392/EWG wurde eine neue Denkweise lanciert. Darin wird nicht die Lösung, sondern das Ziel vorgegeben.

Vorteil der alten Arbeitsweise war die Vorgabe von rezeptartigen Lösungen. Diese wurden vielfach ohne zu hinterfragen übernommen. Ein Nachteil war, dass sich die Lösungen oft nicht so einfach ins Steuerungskonzept integrieren liessen. Auch bei fehlenden Vorschriften und Normen war die Umsetzung des Sicherheitskonzeptes unklar. Oft wählte der Hersteller entweder eine traditionelle, ungeeignete Sicherheitslösung, oder noch schlimmer, er unternahm nichts, da er ja nirgendwo eine Lösung fand. Dies führte je nach Betriebsart der Maschine zu einer Behinderung der Bedienung, was sowohl für den Hersteller wie auch für den Bediener unbefriedigend war.

Sicherheit ist das Ziel

Damit ein Hersteller im Markt bestehen kann, muss er innovative Produkte schnell und kostengünstig anbieten können, muss aber ebenfalls den zunehmenden

Sicherheitsanforderungen unserer zivilisierten Welt gerecht werden. Die Maschinenrichtlinie 98/37/EG (MRL) beinhaltet deshalb eine Sicherheitsphilosophie, bei der die grundlegenden Sicherheitsanforderungen in Form von Schutzzielen formuliert werden. Mit dieser liberalisierten Sicherheitsdenkweise werden dem Hersteller weder durch Normen noch durch eine staatliche Stelle Sicherheitslösungen aufgezwungen. Dies bringt den Vorteil, dass der Hersteller innovative, neue und moderne Lösungen für die bestmögliche Sicherheit umsetzen kann.

Natürlich sind Normen und Sicherheitsvorschriften weiterhin hilfreich und können angewandt werden, aber sie besitzen keinen Gesetzescharakter mehr. So heisst es in der MRL: «Die Übereinstimmung mit harmonisierten Normen lässt die Übereinstimmung mit grundlegenden Anforderungen vermuten» und «Normen müssen unverbindliche Bestimmungen bleiben.»

Mehr Verantwortung für den Hersteller

Die Schweiz hat sich schon vor Abschluss der bilateralen Verhandlungen dazu entschlossen, die Maschinenrichtlinie 98/37/EG (vormals 89/392/EWG) freiwillig zu übernehmen und damit die Voraussetzungen für den freien Warenverkehr mit den EU-Staaten zu bewirken. Die MRL wurde am 1. Juli 1995 vollumfänglich in das Bundesgesetz über die Si-



Bild 1 Werkzeugmaschine der Firma Mikron Agno, zertifiziert durch NSBIV AG

cherheit von technischen Einrichtungen und Geräten (STEG) integriert. Nach einer Übergangsfrist von 1,5 Jahren wurde somit auch in der Schweiz die neue Denkweise umgesetzt.

Die neue Sicherheitsdenkweise brachte dem Hersteller mehr Freiheit, führte jedoch zur Erhöhung der Eigenverantwortung. Der Hersteller muss für jede Maschine oder jedes Sicherheitsbauteil

Artikelserie zur Automation

Das *Bulletin SEV/VSE* veröffentlichte dieses Jahr eine Serie zur Automation. Die Artikel können von der Electrosuisse-Homepage heruntergeladen werden: www.electrosuisse/bulletin.

- Einführung (Nr. 1/05)
- Steuerung (Nr. 3/05)
- Kommunikation (Nr. 7/05)
- Sensoren, Bildverarbeitung (Nr. 11/05)
- Antriebe, Regelungstechnik (Nr. 15/05)
- Software, Bedienen, Beobachten (Nr. 19/05)
- Sicherheit

Kernaussagen der Maschinenrichtlinie 98/37/EG:

Der Hersteller muss ein Konformitätsbewertungsverfahren entsprechend Kapitel II/Art. 8 der MRL durchführen. Grundlage eines solchen Verfahrens ist immer die Gefahrenanalyse mit einer Risikobewertung. Der Hersteller muss dann die Maschine unter Berücksichtigung dieser Analyse entwerfen und bauen.

Die Maschine muss in allen Betriebsarten ohne Gefährdung bestimmungsgemäss verwendet werden können und der vorhersehbare Missbrauch muss berücksichtigt werden. Unter den Betriebsarten versteht man den Normalbetrieb sowie alle Sonderbetriebsarten. Dies sind z. B. Montage, Transport, Einrichten, Störungsbehebung und Instandhaltung, bis und mit Entsorgung.

Bei der Wahl der angemessenen Lösungen muss der Hersteller folgende Reihenfolge einhalten:

1. *Priorität:* Beseitigung der Gefahr durch Integration des Sicherheitskonzepts bei der Entwicklung und Herstellung.
2. *Priorität:* Trennung von Gefahr und Person mittels Schutzmassnahmen.
3. *Priorität:* Organisatorische Massnahmen und/oder Unterrichtung des Benutzers über Restgefahren (Ausbildung, Persönliche Schutzausrüstung PSA).

Die gewählten Lösungen sind bezüglich bestehenden Restrisiken auf Akzeptanz zu hinterfragen. Die Risikoakzeptanz richtet sich nach den Wertmassstäben der Gesellschaft und kann sich verändern. Der Hersteller muss eine technische Dokumentation ausarbeiten, die über alle grundlegenden Aspekte der Sicherheit und Gesundheitsvorsorge Auskunft gibt. Der Hersteller bestätigt mit der Unterzeichnung der Konformitäts- oder Herstellererklärung und der Anbringung der CE-Kennzeichnung an seiner Maschine oder seinem Sicherheitsteil, dass er die Vorgaben der MRL und eventuell weitere zutreffende EG-Richtlinien eingehalten hat.

ein Konformitätsbewertungsverfahren nach MRL durchführen. Dies beinhaltet die Erstellung einer technischen Dokumentation, die Ausstellung einer Konformitäts- oder Herstellererklärung und in der EU die Anbringung der CE-Kennzeichnung. Die technische Dokumentation beinhaltet neben der zentralen Gefahren- und Risikoanalyse alle nötigen Unterlagen, um bei einer Kontrolle den Beweis zu erbringen, dass die gebaute Maschine, resp. das Sicherheitsbauteil, dem Stand der Technik vom Baujahr

sowie den grundlegenden Sicherheitsanforderungen der MRL genügt. Die Betriebsanleitung stellt dabei ein Teil der technischen Dokumentation dar.

Mit der rechtsgültigen Unterschrift der Konformitäts- oder Herstellererklärung bestätigt der Unterzeichner die Einhaltung der MRL und somit der gesetzlichen Auflagen. Der Hersteller kann seine Maschine oder sein Sicherheitsbauteil in Eigenverantwortung bauen und in den Verkehr bringen. Zur Unterstützung kann er eine europäisch akkreditierte Zertifizie-

rungsstelle beziehen und ist sogar in einzelnen speziellen Fällen dazu verpflichtet (entsprechend MRL Anhang IV).

Eindeutige Gewaltentrennung

Mit diesem Verfahren kristallisiert sich somit ein weiterer Vorteil heraus: Die klare Gewaltentrennung zwischen dem Staat als Vollzugsorgan und dem Hersteller. Die Kontrollstellen müssen als Folge dieser Liberalisierung keine Mängel mehr nachweisen, denn jetzt ist der Hersteller in Beweisnot (Unterzeichner der Konformitäts- oder Herstellererklärung).

Was passiert, wenn die technische Dokumentation fehlt?

Auf einen interessanten Punkt weist die MRL im Anhang V bezüglich Nicht-Aushändigen der technischen Dokumentation hin: «*Werden die Unterlagen auf gebührend begründetes Verlangen der zuständigen nationalen Behörden nicht vorgelegt, so kann dies ein ausreichender Grund dafür sein, die Übereinstimmung mit den Bestimmungen der Richtlinie zu bezweifeln.*»

Das heisst, wenn die technische Dokumentation fehlt, wird die korrekte Umsetzung der MRL bezweifelt. Im Ereignisfall besteht die Möglichkeit, dass die Leistungen durch die Versicherung reduziert und einzelne Personen verurteilt werden.

NSBIV

Das Firmenkürzel NSBIV steht für «Nationales Sicherheitsbüro Industrie und Verkehr». Das Unternehmen wurde 1997 als Non-Profit-Organisation gegründet und beschäftigt heute sechs Sicherheitsingenieure und Arbeitshygieniker, die über einschlägige Erfahrung in der Arbeitssicherheit und der Zertifizierung von Maschinen und Anlagen verfügen. Als Zertifizierungsstelle, SIBE Schweiz, überprüft die NSBIV technische Einrichtungen und Geräte, Komponenten, Maschinen und Anlagen sowie PSA auf Konformität gemäss Maschinenrichtlinie 98/37/EG und PSA-Richtlinie 98/686/EG. Sie berätet und unterstützt Einzelbetriebe und Branchen bezüglich Arbeitssicherheit und Gesundheitsschutz (ASA)²⁾. Bei Schadenfällen und Unfällen kann die NSBIV für die Erstellung von Expertisen oder technische Gutachten beigezogen werden. (www.sibe.ch)

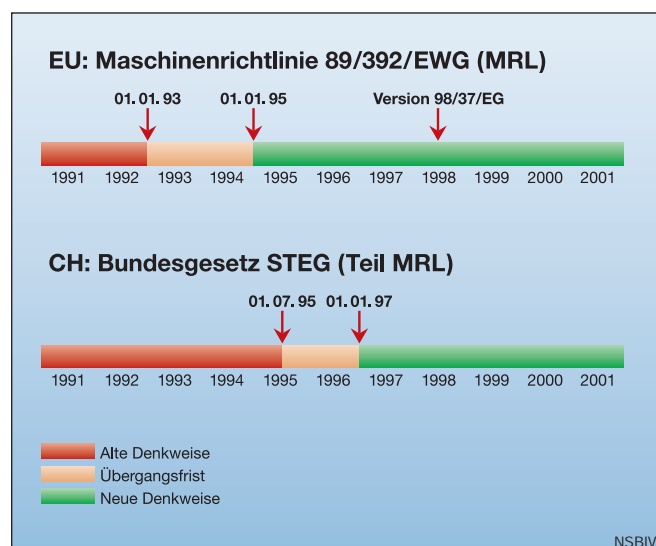


Bild 2 Die Entwicklung der neuen Denkweise in Europa und in der Schweiz

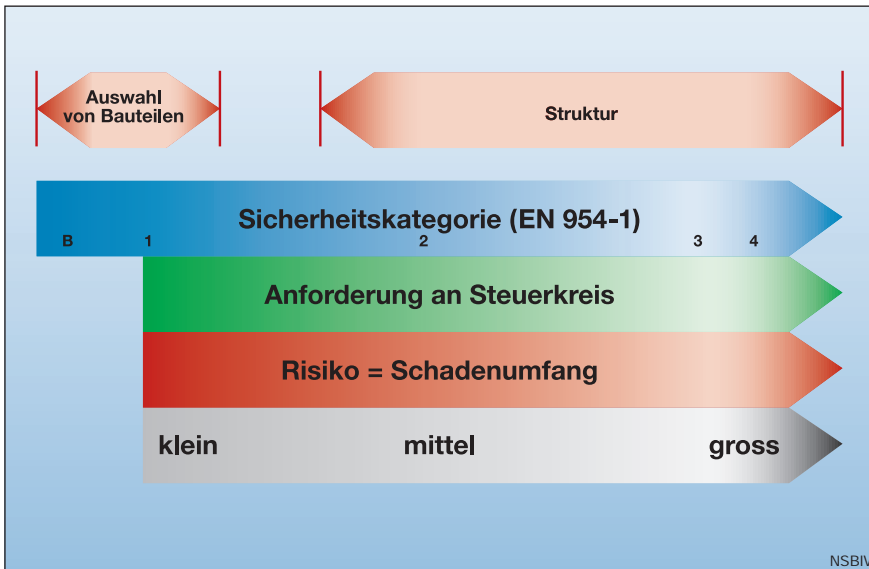


Bild 3 Sicherheits-Kategorien nach EN 954-1

Gefährliche Situationen voraussehen

Die MRL fordert, dass Steuerungen so konzipiert und gebaut sind, dass sie sicher und zuverlässig funktionieren und somit keine gefährlichen Situationen entstehen. Insbesondere müssen sie den zu erwartenden Betriebsbeanspruchungen und Fremdeinflüssen standhalten, Fehler in der Logik dürfen zu keiner gefährlichen Situation führen.

Um diesen Forderungen der MRL gerecht zu werden, kommen die Grundsätze der harmonisierten Norm EN 954-1 zur Anwendung. Diese Norm enthält Ausführungen zu sicherheitsbezogenen Teilen von Steuerungen. Dabei wird die Sicherheit entweder durch die Auswahl der Bauteile oder durch die Struktur gewährleistet. Bewährte Bauteile werden auf Grund ausgewählter Prüfverfahren, festgehalten in diversen Normen, auf ihre Einsatztauglichkeit im Sicherheitsbereich ausgewählt. Bei der Struktur von Sicherheitssteuerungen wird das Verhalten im Fehlerfall betrachtet. Dies kann zum Beispiel durch die Anwendung von redundanten und diversitären Systemen realisiert werden, die sich kontinuierlich überwachen.

Bei grossen Risiken, also einem hohen Schadenumfang, sind die Anforderungen an die Steuerkreise höher, dies in Anlehnung an die MRL. Je höher der Schadenumfang, desto höher die Sicherheitskategorie.

Nicht nur sicher, auch zuverlässig

Für die Zuverlässigkeit wird bei der EN 954-1 auf bewährte Bauteile zurück-

gegriffen. Möglicherweise wurde bei der Erstellung der EN 954-1 davon ausgegangen, dass es auch ohne Vorschriften im Interesse des Herstellers liegt, eine prozesssichere Steuerung zu bauen. Denn ein Hersteller kann im Markt nur dann bestehen, wenn er nicht nur sichere, sondern auch zuverlässige Maschinen baut. So gibt es Anwendungen, bei denen ein Ausfall der Steuerung weit reichende Konsequenzen hat: Der Startabbruch der Raumfähre Discovery am 13. Juli 2005 zeigt, dass ein unzuverlässiges System zu immensen Kosten und zu einem massiven Imageschaden führen kann. Ein einzelner defekter Sensor am Treibstofftank hatte den Start um mehrere Tage verzögert. Das System mag sicher sein. Aber handelt es sich hier um eine prozesssichere und zuverlässige Steuerung?



Bild 4 Raumfähre Discovery beim Start am 26. Juli 2005

Ein defekter Sensor verzögerte den Start der Raumfähre um zwei Wochen. Ein sicheres System ist nicht unbedingt zuverlässig.

Warum wird die EN 954-1 überarbeitet?

Die Gewährleistung der Sicherheit von elektrischen und elektronischen Bauteilen und Steuerungen wird in der Norm IEC EN 61508-1...-7 durch die Betrachtung des gesamten Lebenszyklus erreicht. Bei diesen Betrachtungen stellt die Zuverlässigkeit das zentrale Element dar. Dabei wird entsprechend einem möglichen Schadenumfang der so genannte

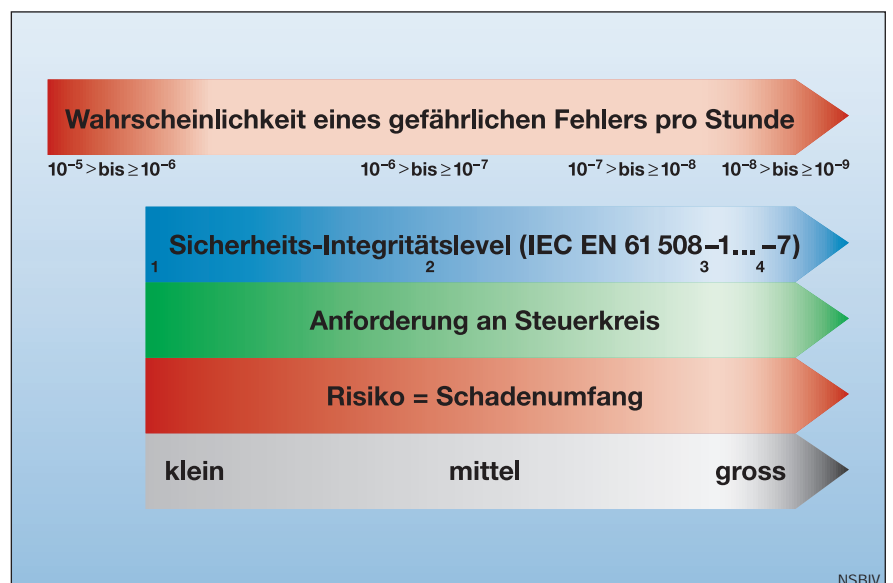


Bild 5 Sicherheits-Integritätslevel nach IEC EN 61508-1...-7

Sicherheits-Integritätslevel SIL (SIL= Safety Integrity Level) festgelegt. Auch hier gilt, je grösser der Schadenumfang umso grösser der SIL.

Diese Norm findet zum Beispiel bei der Entwicklung von elektronischen Steuerungen oder Sicherheits-SPS¹⁾ Anwendung. Auf Grund der komplexen mathematischen Modelle zur Bestimmung der Wahrscheinlichkeit eines gefährlichen Fehlers sowie weiteren Faktoren, die zur Berechnung der SIL berücksichtigt werden müssen, ist der Aufwand hoch. Deswegen kommt diese Beweisführung in der Maschinenindustrie selten zur Anwendung. In der Norm prEN ISO 13849-1 wird nun versucht, neben dem strukturellen Ansatz der EN 954-1 auch den Wahrscheinlichkeitsansatz der IEC EN 61508-1 ...-7 vereinfacht mit einzubeziehen. Dazu wird neu ein fünfstufiger Performance Level (PL) *a* bis *e* eingeführt. Bei der Umsetzung werden unter anderem die Zuverlässigkeit einzelner Bauteile und Komponenten sowie die Wahl gezielter Strukturen auf Basis der bestehenden EN 954-1 berücksichtigt. Weitere Faktoren sind der Fehler-Detektionsmechanismus (Diagnosedeckungsgrad) oder Ausfälle infolge gemeinsamer Ursache. Jeder dieser Faktoren kann die Erreichung des PL positiv wie auch negativ beeinflussen.

Macht prEN ISO 13849-1 die Maschinen sicherer?

Grundsätzlich ist eine zuverlässige Maschinensteuerung auch sicherer. Es stellt sich jedoch die Frage: Muss die Zuverlässigkeit von Sicherheitssteuerungen geregelt werden? Nein! Im Markt bestehen nur anwenderfreundliche und zuverlässige Systeme, in die die Sicherheit integriert ist. Leider existiert beim heutigen

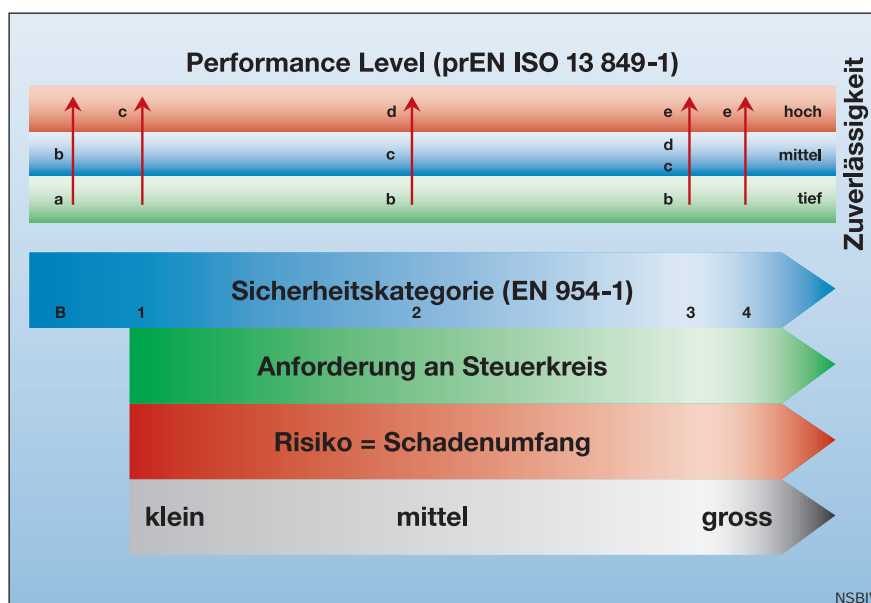


Bild 6 Performance Level nach prEN ISO 13849-1

Stand der prEN ISO 13849-1 die Gefahr, dass sichere Strukturen durch Zuverlässigkeitsberechnungen umgangen werden.

Als europäische akkreditierte Zertifizierungsstelle wird die SIBE Schweiz den neuen Ansatz der prEN ISO 13849-1 so umsetzen, dass der heute erreichte Stand der Technik, abgeleitet aus der EN 954-1, zusätzlich mit dem Aspekt der Zuverlässigkeit verbunden, nicht aber durch diesen abgelöst wird. Dadurch können moderne, sichere Systeme entwickelt werden, die sämtlichen Aspekten der Arbeits- und Prozesssicherheit genügen.

Angaben zu den Autoren

Hans Ruckli, dipl. El.-Ing. HTL, Betriebs- & Sicherheitsingenieur, ist seit 2001 bei der NSBIV AG für die Zertifizierung von Maschinen und Sicherheitsbau-

teile, ASA-Beratung²⁾ und Expertisen zuständig. Zwischen 1990 und 2001 war er bei Rockwell Automation als Projektmanager und Abteilungsleiter Systems Engineering tätig.

NSBIV AG, 6002 Luzern, hans.ruckli@sibe.ch

Mario Luzzatto, dipl. El.-Ing. ETH, Sicherheitsingenieur, ist Mitgründer der NSBIV AG und hat mehrjährige Erfahrung in der Zertifizierung von Sicherheitssteuerungen und Maschinen, ASA-Beratung²⁾ und Expertisen. Ferner unterstützt er Firmen im In- und Ausland bei der Erarbeitung von modernen Sicherheitskonzepten.

NSBIV AG, 6002 Luzern, mario.luzzatto@sibe.ch

¹ SPS: Speicherprogrammierbare Steuerung

² ASA: Arbeitsärzte und andere Spezialisten der Arbeitssicherheit