



Bild: Strutzke

Dr. Michael Huelke, Leiter des Referats Neue Technologien, Mensch und Technik im Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung: „Erst eine Validierung der Sicherheitsfunktionen macht eine Maschine sicher.“

Immer wenn Mensch und Maschine ohne Schutzzaun eng zusammenarbeiten, ist eine Sicherheitssteuerung zwingend erforderlich.



Sicher programmieren statt verdrahten

Eine programmierbare Steuerung zum Schutz von Mensch und Maschine? Das war vor Jahren noch undenkbar. Heute sind sicherheitsgerichtete Steuerungssysteme Stand der Technik. Auch die Grenze zwischen Standard- und Sicherheitstechnik schwimmt zunehmend. Wann lohnt sich der Einsatz von programmierbaren Sicherheitssteuerungen?

ALEXANDER STRUTZKE

Die Integration von Sicherheitstechnik in Maschinen und Anlagen hat in den letzten Jahrzehnten dazu geführt, dass die Zahl der Unfälle deutlich zurückgegangen ist. Trotzdem gibt es immer noch Unfälle, meist sind diese auf technische Mängel oder organisatorische Probleme zurückzuführen. Außer der ethischen Komponente, alles zu tun, um einen Unfall zu vermeiden, sprechen auch die Ausfallkosten dafür, bereits bei der Planung einer Maschine oder Anlage über Sicherheitstechnik nachzudenken. Dr. Peter Wratil, Geschäftsführer der Innotec GmbH, Rosengarten, bestätigt: „Die Kosten einer Maschine, die aufgrund eines Unfalls steht, können Sie gar nicht

kalkulieren.“ Allerdings sind die Betreiber von Maschinen und Anlagen auch an höchstmöglicher Produktivität interessiert. Jochen Ost, Produktmanager Safety Controls bei der Bosch Rexroth Electric Drives and Controls GmbH, bekräftigt: „Sicherheitstechnik muss zum Prozess passen und darf nicht die Produktivität reduzieren.“ Wratil argumentiert: „Sie erreichen hohe Produktivität nur, wenn Sie den Menschen in die Maschine integrieren. Das bedeutet, Sie müssen eine Sicherheitstechnik haben, die zu 100% garantiert, dass dem Menschen nichts passiert.“ Nach Wratils Aussage sind wir am Standort Deutschland deshalb so produktiv, weil wir Sicherheitstechnik verstehen und nutzen. „Wir sind in der Lage, einen Menschen in den Gefahrenbereich einer Maschine zu schicken, ohne dass ihm etwas passiert, so dass er dort Fehler beheben kann, bevor sie signifikant die Produktivität beeinträchtigen.“

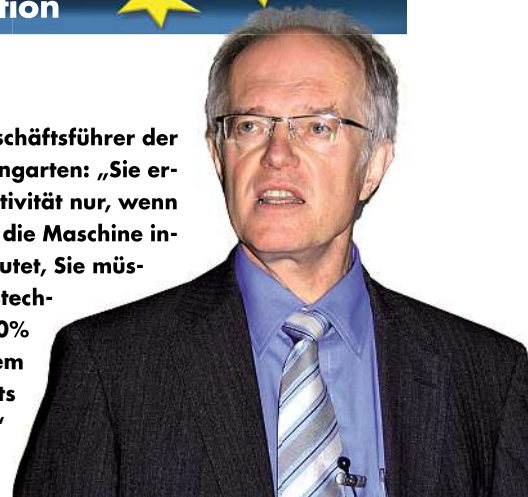
Verdrahtung ist kompliziert und unflexibel

Sicherheitstechnik wird oft als notwendiges Übel angesehen und den Schaltschrank-Konstrukteuren zugeschoben, erläutert Helmut Börjes, bei der Wago Kontakttechnik GmbH & Co. KG zuständig für Komponenten und Systeme mit funktionaler Sicherheit. Mit der wach-



Ulrich Hochrein, verantwortlich für das Team Sicherheitstechnische Dienstleistungen bei der Edag GmbH & Co. KG:
„Software ist abstrakt. Und je abstrakter ein Thema ist, umso leichter können sich Fehler einschleichen.“

Bild: Strutzke



Dr. Peter Wratil, Geschäftsführer der Innotec GmbH, Rosengarten: „Sie erreichen hohe Produktivität nur, wenn Sie den Menschen in die Maschine integrieren. Das bedeutet, Sie müssen eine Sicherheitstechnik haben, die zu 100% garantiert, dass dem Menschen nichts passiert.“

Bild: Strutzke

senden Erfahrung und erprobten technischen und methodischen Konzepten wird die Sicherheitstechnik heute aber immer mehr integraler Bestandteil der Automation. Einen Vorteil der programmierbaren Sicherheitstechnik beschreibt Wratil: „Verdrahtung ist manchmal so kompliziert, dass sie selbst Elektriker vor Probleme stellt, insbesondere wenn die Schaltung verändert oder erweitert werden muss.“ Verdrahtung ist außerdem unflexibel. Eine Software ist, wenn man sie verstanden hat, wesentlich leichter zu modifizieren. „Außerdem“, so Wratil, „ist Software frei von zufälligen Fehlern.“ Eine Software fällt nicht aus, weil eine Komponente oder ein Modul verschlissen ist.

„Software hat nur systematische Fehler, die durch den Programmierer eingebaut werden.“ Diese Fehleranfälligkeit unterstreicht auch Ulrich Hochrein, verantwortlich für das Team Sicherheitstechnische Dienstleistungen bei der Edag GmbH & Co. KG: „Software ist abstrakt. Und je abstrakter ein Thema ist, umso leichter können sich Fehler einschleichen.“

Sicherheitstechnik muss getestet werden

Deshalb ist es wichtig, dass die Programmierer gut ausgebildet sind und nicht unter Stress stehen. Hochrein erläutert: „Verbindliche Ar-



beitsweisen helfen, Fehler zu vermeiden.“ Zudem ist eine gute Dokumentation sehr wichtig. Außerdem gilt, wie Wrtil ausführt, für die programmierbare Sicherheitstechnik genauso wie für die konventionelle über Verdrahtung: „Man muss die Sicherheitstechnik testen.“ Dr. Michael Huelke, Leiter des Referats Neue Technologien, Mensch und Technik im Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, bestätigt: „Erst eine Validierung der Sicherheitsfunktionen macht eine Maschine sicher.“

Einen anderen wichtigen Vorteil der programmierbaren Sicherheitstechnik beschreibt Jürgen Malin, Leiter Sicheres Steuerungskonzept bei der Bachmann Electronic GmbH: „Mit programmierbarer Sicherheitstechnik haben Sie auch bei verteilten Anlagen die Möglichkeit, durch Fernwartung die Fehlersuche zu vereinfachen und Softwaremodule auszutauschen.“ Eine Software besteht meist nur aus wenigen Kilobyte und kann auch über Internet oder Telefon auf eine Anlage übertragen werden. Dabei dürfen natürlich Security-Aspekte nicht außer Acht gelassen werden, denn sonst wird auch die Sicherheit von Mensch und Maschine nicht gewährleistet.

Manipulierbarkeit der Sicherheitstechnik eingeschränkt

Nicht zuletzt kann ein einmal erstelltes Softwaremodul häufig mit geringen Anpassungen auf andere Maschinen übertragen werden. Das gilt natürlich auch für den Schaltplan einer Verdrahtung. Dabei zeigt jedoch die Erfahrung, dass häufig abweichend vom Schaltplan spontane Änderungen vorgenommen werden, die schlimmstenfalls nicht mal dokumentiert sind. Eine Rolle spielt dabei auch die Manipulierbarkeit der Sicherheitstechnik. Der beste Sensor hilft nicht, wenn er per Draht überbrückt wird. Theoretisch kann man einen Sensor auch bei der programmierbaren Sicherheitstechnik überbrücken, jedoch ist das bei modernen Sensoren wesentlich schwieriger und die Software macht eine Manipulierung, wenn überhaupt, nur einem kleinen Kreis von Personen möglich. ■