Bachelorthesis im FG Sicherheitstechnik/Arbeitssicherheit

Übungskonzept zur Risikobeurteilung von sicherheitsbezogenen Maschinensteuerungen

Das **Ziel** der Arbeit ist die Erstellung eines Lehr- und Übungskonzeptes, mit welchem den Studierenden das Verfahren der Risikobeurteilung von Maschinensteuerungen in geeigneter Form vermittelt wird. Das Erlernen und Üben „handwerklicher" Fertigkeiten der Risikobeurteilung soll um die Vermittlung der entsprechenden fachspezifischen Hintergründe ergänzt werden.
Das Thema „Steuerungsbezogene Schutzmaßnahmen" deckt einen wichtigen und vergleichsweise umfassenden Aspekt der Maschinensicherheit ab. Dabei hängt die Sicherheit des Maschinenbedieners insbesondere von der Zuverlässigkeit der Steuerung ab. Schon allein sprachlich beeindruckende Begriffe wie „Erwartungswert der Zeit bis zum gefahrbringenden Ausfall" stellen sich dem Nicht-Experten in den Weg. Und die Entscheidung, ob mit Redundanzen alles gut wird, trifft der Zuverlässigkeitslaie auch eher aus dem Bauch heraus.
Die DIN EN ISO 13849 „Sicherheit von Maschinensteuerungen", an welcher sich das neue normative Bewertungskonzept orientiert, schlägt dem Anwender hier ein vereinfachtes Verfahren vor. Die vier Grundrechenarten genügen, um die Sicherheit von Maschinensteuerungen zu bestimmen. Es werden die klassischen Ansätze des Determinismus mit probabilistischen Verfahren kombiniert.

Zunächst ist die **Sicherheitsfunktion**, eine sicherheitsgerichtete Reaktion der Maschinensteuerung auf ein Gefährdungsereignis, zu definieren. Anhand der Sicherheitsfunktion werden die sicherheitsbezogenen Steuerungsteile ermittelt.
Als Anforderung an die Steuerung dient der **erforderliche Performance Level PL**$_r$. Er wird in fünf Stufen a (geringe Anforderungen) bis e (hohe Anforderungen) ausgewiesen. Zu seiner Ermittlung dient ein Risikograph, bei dessen Anwendung lediglich diese Fragen in jeweils zwei Stufen (Entscheidungen) zu beantworten sind:

- Besteht die Gefahr leichter oder schwerer Verletzungen?
- Sind die Benutzer häufig oder selten gegenüber der Gefahr exponiert?
- Besteht die Möglichkeit, die Gefahr zu vermeiden?

Am PL$_r$ muss sich zum Abschluss der Risikobeurteilung die Güte der Steuerung messen lassen.
Als Maß für die Fähigkeit der Steuerung, die Sicherheitsfunktion auszuführen, dient der **erreichte Performance Level PL.** Auch er wird in den Stufen a bis e angegeben und beruht auf der Ausfallwahrscheinlichkeit der Steuerung. Der PL ergibt sich aus den vier Parametern:

- Mittlere Zeit bis zum gefahrbringenden Ausfall (MTTF$_d$)
- Kategorie
- Diagnosedeckungsgrad (DC$_{avg}$)
- Schutz gegen Fehler infolge gemeinsamer Ursache (CCF)

Diese Parameter werden jedoch nicht als starre Grenzwerte berücksichtigt. Vielmehr werden diese durch Bänder mit einem höheren oder niedrigeren Beitrag zur Gesamtsicherheit dargestellt. Hierdurch können, in gewissen Grenzen, Defizite in einem Bereich durch bessere Leistungen in einem anderen kompensiert werden.
Maßgeblichen Einfluss auf die Ausfallwahrscheinlichkeit der Steuerung hat die Zuverlässigkeit der Bauteile. Sie geht in Form der in drei Stufen unterteilten „Zeit bis zum gefahrbringenden Ausfall" (MTTF$_d$) in das Gesamtergebnis ein. Hierbei handelt es sich um einen statistischen Erwartungswert, keinesfalls um eine garantierte Lebensdauer. Die theoretische Zuverlässigkeit eines Systems ließe sich durch die Verwendung von Komponenten mit einer sehr hohen MTTF$_d$ beliebig erhöhen. Da aber auch diese, auf dem Papier sehr sicheren Steuerungen, gefahrbringend ausfallen können, dürfen Zeiten über 100 Jahre nicht angenommen werden (Kappungsgrenze). Somit ist es erforderlich die Steuerung durch ihre Struktur gegen Ausfälle zu ertüchtigen. Die für die Praxis relevanten Strukturen „einkanalig", „einkanalig mit Überwachung" und „zweikanalig" werden durch die Kategorien B und 1 bis 4 berücksichtigt.
Der Sicherheitsgewinn durch Redundanz ist jedoch marginal, wenn Ausfälle nicht erkannt werden können. Daher wird auch der Diagnosedeckungsgrad DC$_{avg}$ in drei Stufen hinzugezogen. Er gibt den Anteil der erkannten Ausfälle an der Gesamtzahl der Ausfälle an.
Nun besteht die Gefahr, dass die aufwändig getroffenen Maßnahmen zur Zuverlässigkeit dadurch unterlaufen werden, dass Ereignisse eintreten, die auf alle Kanäle der Steuerung zugleich wirken, wie z.B. Temperaturschwankungen. Diese Fehler infolge gemeinsamer Ursache (CCF) werden mittels eines Checklistenverfahrens in den Stufen „erfüllt" und „nicht erfüllt" bewertet. Sind die vier Parameter ermittelt, lassen sich aus einem Diagramm oder einer Tabelle der erreichte PL und die Ausfallwahrscheinlichkeit der Steuerung ablesen.

Um diese Inhalte, und weitere, nicht quantitative Aspekte, der Steuerungssicherheit in die universitäre Lehre einbringen zu können, müssen sie entsprechend aufbereitet werden. Der Rahmen hierfür ist durch die, seit Jahren bewährte, Lehrmethodik des Fachgebiets Arbeitssicherheit abgesteckt. Zur Strukturierung der Inhalte wird ein Ablaufschema verwendet, das die relevanten Schritte der Risikobeurteilung aufgreift. Ein solches Vorgehen hat sich in der ingenieurwissenschaftlichen Ausbildung und Arbeitsweise bewährt.

Die Umsetzung des Lehr- und Übungskonzeptes ist von zwei ambivalenten Faktoren geprägt. Einerseits sind bei den angehenden Sicherheitsingenieuren kaum Kenntnisse der Steuerungstechnik vorhanden. Andererseits ist auch das vereinfachte Verfahren der Norm aufgrund verschiedener Abhängigkeiten der Inhalte voneinander auf Anhieb nicht leicht zu erfassen. Das Anliegen der Norm wird daher ständig durch Beispiele verdeutlicht, Bezüge sollen das Verständnis verbessern.

Diverse Entwicklungen im Umfeld der Norm zeigen die hohe Aktualität des Themas. So sind Erweiterungen im Bereich der $MTTF_d$ vorgesehen, um auch mit sehr komplexen Steuerungen eine sehr hohe Ausfallsicherheit erreichen zu können.

Da sichere Produkte eine Grundlage der sicheren Arbeitsausführung auf betrieblicher Ebene sind, ist die Produktsicherheit eine wesentliche Ergänzung der Lehrinhalte der Arbeitssicherheit.

Die fachliche Betreuung der Bachelorthesis erfolgte durch Prof. Anke Kahl und M. Sc. Florian Pillar, Fachgebiet Arbeitssicherheit an der Bergischen Universität Wuppertal.

Kontakt

Sie als Leser sind herzlich eingeladen, Ihr Fachwissen einzubringen, Fragen zu stellen oder zu diskutieren per Mail an: gerhold@uni-wuppertal.de

Malte Gerhold