3. Workshop Automatisierungstechnische Verfahren für die Medizin vom 17.-18. September 2001 in Bochum

„Sicherheitsaspekte bei der Realisierung von Bahnsteuerungen für medizinische Geräte“

T. Bürger, U. Laible
Institut f. Steuerungstechnik der Werkzeugmaschinen und Fertigungseinrichtungen, Univ. Stuttgart, Stuttgart, Deutschland
E-Mail: thomas.buerger@isw.uni-stuttgart.de, ulrich.laible@isw.uni-stuttgart.de

W. Bachmann, D. Scheifele
Industrielle Steuerungstechnik GmbH, Stuttgart, Deutschland

Band: Beiträge zum 3. Workshop Automatisierungstechnische Methoden und Verfahren für die Medizin
Editors: Jürgen Werner, Martin Hexamer
ISBN: 3-00-008240-9
Pages: 42-43

Sicherheitsaspekte bei der Realisierung von Bahnsteuerungen für medizinische Geräte

T. Bürger[1], U. Laible[1], W. Bachmann[2], D. Scheifele[2]

[1]Institut f. Steuerungstechnik der Werkzeugmaschinen und Fertigungseinrichtungen, Univ. Stuttgart
[2]Industrielle Steuerungstechnik GmbH, Stuttgart

[1]{thomas.buerger,ulrich.laible}@isw.uni-stuttgart.de
[2]{wolfram.bachmann, dieter.scheifele}@isg-stuttgart.de

EINLEITUNG

Immer öfter werden für chirurgische Eingriffe Robotersysteme eingesetzt, bei denen Instrumente und Werkzeuge durch eine oder mehrere angetriebene Achsen im Manipulatorbetrieb oder automatisch gesteuert werden. Eine Fehlfunktion der antriebsnahen Bahnsteuerung (Robotersteuerung) kann unmittelbar zur Gefährdung von Patienten führen, da diese Steuerung neben Computertomograph, Planungssystem, Navigationssystem und Benutzerschnittstelle eine Komponente mit hoher Sicherheitsanforderung ist.

Während für speicherprogrammierbare Steuerungen (SPS) schon länger Konzepte und auch Produkte bekannt sind, die eine sehr hohe Sicherheit und Verfügbarkeit gewährleisten [1], ist dies für Robotersteuerungen und für die gesamte numerische Steuerungstechnik erst ein relativ neues Anwendungsfeld. Es existieren zwar auch bezüglich der Sicherheit von numerischen Steuerungen Normen und Vorschriften [2], diese beziehen sich jedoch größtenteils auf Maschinen und Anlagen und sind nur bedingt auf Anwendungen in der Medizintechnik übertragbar. Ein mehrkanaliger, vollständig redundanter Aufbau, wie von Sicherheits-SPS bekannt, ist für numerische Steuerungen wesentlich komplexer und bisher kaum realisiert [3].

Dieser Beitrag berichtet über das Konzept einer zweikanaligen, fehlersicheren Robotersteuerung, die im Rahmen eines Industrieprojektes mit der Fa. Universal Robot Systems GmbH (URS) [4] für einen in der Chirurgie eingesetzten Medizinroboter entwickelt wurde. Dies umfasst die wesentlichen sicherheitsrelevanten Merkmale und Entwicklungsschritte bis hin zur abschließenden Zertifizierung durch den TÜV.

ANWENDUNGSGEBIET UND GERÄTEAUFBAU

Das von der Fa. URS entwickelte Robotersystem soll sowohl bei Operationen mit interaktiv gesteuerter Instrumentenführung (z.B. Neurochirurgie, minimalinvasive Chirurgie) als auch bei voll- und teilautomatischen Eingriffen (z.B. Hüft- und Knieendoprothetik, Wirbelsäulenchirurgie, Unterstützung bei der Implantation von Hörhilfen) eingesetzt werden.

Die hybride Kinematik des Roboters besteht aus einem Hexapod mit serieller Linearachse sowie drei redundanten Messachsen in Form eines Tripods. Die während dem operativen Eingriff bewegte Kinematik ist an ein mobiles Trägersystem montiert, das zur präoperativen Vorpositionierung des Systems relativ zum Patienten verwendet wird. Die in diesem Trägersystem integrierten Antriebe werden nicht über die Robotersteuerung angesteuert.

ANFORDERUNGEN AN DIE SICHERHEIT

Generell kann ein System fehlersicher (failsafe) und/oder fehlertolerant (fault tolerant) sein [1]. Ein fehlersicheres System besitzt einen sicheren Zustand, der im Fehlerfall erreicht werden muss. Im sicheren Zustand steht nicht mehr der gesamte Funktionsumfang zur Verfügung. Ein fehlertolerantes System muss dagegen mehrere Fehler ohne Einschränkung der Funktion und der Sicherheit tolerieren können. In der Praxis trifft man meistens auf Mischformen, d.h. Systeme, die zu einem gewissen Grad fehlertolerant sind, bei bestimmten Fehlern aber in einen sicheren Zustand wechseln, sofern das System einen sicheren Zustand besitzt.

Die oben genannten chirurgischen Anwendungen erfordern primär ein fehlersicheres Robotersystem. Im Fehlerfall muss das System sofort alle Bewegungen stoppen (sicherer Zustand: Stopp aller Achsen). Anschließend kann die Operation manuell weitergeführt werden.

Als Voraussetzung für den Einsatz an Patienten ist eine sicherheitstechnische Abnahme des gesamten Robotersystems durch eine benannte Stelle (z.B. TÜV) erforderlich, die zu einer CE-Zertifizierung gemäß den Medical Device Directives führt [5]. Mögliche Risiken und Auswirkungen bei Versagen einzelner Hard- und Softwarekomponenenten der Steuerung müssen vor Beginn und während der Entwicklung durch eine FMEA (Failure Mode and Effect Analysis) untersucht und abgeschätzt werden.

In der FMEA wird die gesamte Kette von den Eingabegeräten bis zu den elektromechanischen Antriebskomponenten betrachtet. Die FMEA begleitet die Entwicklung des Sicherheitskonzeptes in einem iterativen Prozess. Werden Fehlerfälle entdeckt, die mit dem aktuellen Sicherheitskonzept nicht erkannt werden können, muss das Konzept entsprechend optimiert und die FMEA für das geänderte Sicherheitskonzept erneut durchgeführt werden.

REALISIERTES SICHERHEITSKONZEPT

Um ein fehlersicheres System realisieren zu können müssen Fehler vom System zunächst erkannt werden (Fehlererkennung). Anschließend muss eine der schwere des Fehlers entsprechende Fehlerreaktion durchgeführt werden, die das System in einen sicheren Zustand überführt.

Fehler können systematischer Art (Softwarefehler, Spezifikationsfehler) sein oder zufällig auftreten (Hardwareausfall, elektromagnetische Beeinflussung). Durch geeignete Testverfahren kann die Anzahl möglicher systematischer Fehler sehr stark reduziert werden. Zufällige Fehler können dagegen nur durch Überwachungsfunktionen erkannt werden, die auch im laufenden Betrieb aktiv sind.

Zufällige CPU- oder Speicherfehler können theoretisch dazu führen, dass die Robotersteuerung falsche Achssollwerte generiert. Um diese Fehler zu erkennen sieht das realisierte Konzept einen zweikanaligen Aufbau der Steuerungshardware und -software (2 CPUs, redundante I/O Karten) vor. Alle sicherheitsrelevanten Messgrößen werden redundant eingelesen, die Sollwerte werden redundant berechnet. Die Steuerung vergleicht im Echtzeittakt die berechneten Sollwerte beider Kanäle und gibt diese nur bei Gleichheit aus. Um vergleichbare Werte zu erhalten, müssen Steuerungs- und Überwachungskanal an mehreren Stellen synchronisiert werden. Dabei darf jedoch der Steuerungskanal in seinem Programmablauf zeitlich nicht durch den Überwachungskanal beeinflusst werden.

Ein weiterer wichtiger Bestandteil des Sicherheitskonzepts ist das redundante Meßsystem, welches die Istposition der Plattform unabhängig von dem Meßsystem der Antriebsachsen erfasst. Da sich die Kinematik für das Meßsystem (Tripod) von der für die angetriebenen Achsen (Hexapod) unterscheidet, können auch Fehler in der kinematischen Transformation oder ein fehlerhaftes Referenzieren der Achsen entdeckt werden.

Fehler im Antrieb oder im Lageregelkreis werden durch eine dynamische Schleppabstandsüberwachung erkannt. Der zulässige Schleppabstand wird dabei ständig an die aktuelle Geschwindigkeit und Beschleunigung der Achse angepasst. Im Stillstand ist nahezu kein Schleppabstand zulässig.

Alle sicherheitskritischen Fehler führen sofort zu einer Leistungsabschaltung der Antriebe, wobei die Leistung sowohl vom Steuerungskanal als auch vom Überwachungskanal unabhängig abgeschaltet werden kann. Beim Einschalten des Steuerungssystems werden umfangreiche Selbsttests durchgeführt. Diese laufen automatisch (Speichertests, Test des Not-Aus-Kreis, usw.) oder interaktiv ab (Joystick-Test).

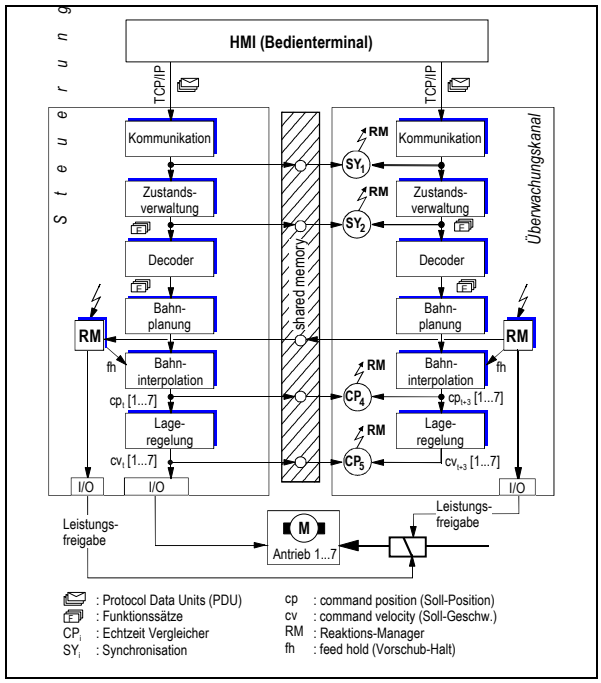

Abbildung 3: Redundanter Überwachungskanal der Robotersteuerung.

ZUSAMMENFASSUNG

Die in diesem Beitrag beschriebenen Entwicklungsschritte führten im Ergebnis zu dem Konzept und der Realisierung einer ausfallsicheren Robotersteuerung, welche den Sicherheitsanforderungen der Medical Device Directives entspricht. Das zugrundeliegende Sicherheitskonzept kann ebenso wie die Steuerungssoftware als Ganzes oder in Teilen ohne große Änderung auch für andere Anwendungsfälle (z.B. für Werkzeugmaschinen und Industrieroboter) eingesetzt werden, die eine im hohen Maße ausfallsichere Bahnsteuerung benötigen.

LITERATURHINWEISE

[1] Halang, W. A.; Konakovsky, R.: Sicherheitsgerichtete Echtzeitsysteme. München, Wien: Oldenbourg 1999.

[2] DIN EN 954-1: Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil1: Allgemeine Gestaltungsleitsätze. Berlin: Beuth-Verlag 1997.

[3] Weck, M.; Kohring, A.: Sicherheitsaspekte bei der Ansteuerung von Industrieroboterachsen. Hrsg.: Bundesanstalt für Arbeitsschutz. Dortmund: Verlag für neue Wissenschaft 1990.

[4] Fa. Universal Robot Systems GmbH (URS): http://www.medicalrobots.com/

[5] DIN EN 60601-1: Medizinische elektrische Geräte - Teil 1: Allgemeine Festlegungen für die Sicherheit. Berlin: Beuth-Verlag 1996.