Marcus Martinus und Rüdiger Freimann, Garching

Prozesssicherheit Landmaschinenelektronik

In dem von der Deutschen Forschungsgemeinschaft unterstützten Projekt „Prozesssicherheit Landmaschinenelektronik“ sollen elektronisch geregelte Arbeitsprozesse und Automatiken bei Traktor/Gerätekombinationen und selbstfahrenden Landmaschinen hinsichtlich ihrer funktionalen Sicherheit untersucht werden. Ziel ist es, ein Konzept aus Entwicklungsschritten, Methoden und Werkzeugen zu erarbeiten, welches die sicherheitsgerechte Entwicklung der mechatronischen Systeme ermöglicht. Die Methoden der System- und Risikoanalyse sowie ein durchgängiges Entwicklungsmodell für elektronische Steuerungen stehen dabei im Mittelpunkt.

Dipl.-Ing. Marcus Martinus und Dipl.-Ing. Rüdiger Freimann sind wissenschaftliche Assistenten am Lehrstuhl für Landmaschinen (Leitung: Prof. Dr.-Ing. Dr. h.c. K.Th. Renius) der Technischen Universität München, Boltzmannstr. 15, 85748 Garching; e-mail: *martinus@ltm.mw.tum.de; freimann@ltm.mw.tum.de*
Die Projektarbeit wurde finanziell von der Deutschen Forschungsgemeinschaft unterstützt.
Referierter Beitrag der LANDTECHNIK, die Langfassung finden Sie unter LANDTECHNIK-NET.com.

Schlüsselwörter

Funktionale Sicherheit, Prozesssicherheit, Gerät steuert Traktor, Elektronik, FMEA

Keywords

Functional safety, process safety, implement guided tractor control, electronics, FMEA

Literatur

Literaturhinweise sind unter LT 02321 über Internet http://www.landwirtschaftsverlag.com/ landtech/local/fliteratur.htm abrufbar.

Arbeitsprozesse von Traktor/Geräte-Kombinationen und selbstfahrenden Arbeitsmaschinen erreichen einen immer höher werdenden Automatisierungsgrad. Um die Betriebssicherheit der Systeme zu gewährleisten, stellen Programmautomatiken auch neue Anforderungen an den Entwicklungsprozess der Elektronik.

Ein Ansatz des DFG-Projektes „Prozesssicherheit Landmaschinenelektronik“ ist es deshalb, auf Basis bestehender allgemeiner Normen, etwa [1], Methoden für sichere automatisierte Arbeitsprozesse bei Landmaschinen zu entwickeln.

Ein prozesssicheres System hat die Aufgabe, das Auftreten eines sicherheitsrelevanten Fehlers zu vermeiden oder zumindest zu erkennen und dann den Arbeitsprozess in den sicheren Zustand zu überführen oder diesen nicht zu verlassen. In der Sicherheitstechnik wird diese Eigenschaft mit „Fail Safe“-Verhalten beschrieben [2]. Der sichere Zustand ist hier als Zustand eines technischen Systems definiert, bei dem aufgrund der getroffenen Schutzmaßnahmen das Sicherheitsrisiko *vertretbar* gering ist. Bei der Konzeption einer Schutzfunktion muss deshalb konkret festgelegt werden, wie dieser sichere Zustand aussieht.

Entwicklungskonzept für automatisierte Arbeitsprozesse

In der Anfangsphase des Projekts „Prozesssicherheit Landmaschinenelektronik“ wurde ein Konzept zur Untersuchung der Prozesssicherheit vorgeschlagen [3, 4], welches mittlerweile mit den relevanten Normen abgeglichen und zu einem sicherheitsgerechten Entwicklungskonzept für automatisierte Prozesse der Feldarbeit erweitert wurde.

Bei der Entwicklung eines sicheren Systems müssen alle sicherheitskritischen Steuerungen identifiziert und so konzipiert werden, dass sie durch MSR-Schutzeinrichtungen (Messen/Steuern/Regeln) überwacht und abgesichert werden können. Mit der zunehmenden Anzahl an Schutzeinrichtungen steigt allerdings auch der Gesamtaufwand. Mit der Anzahl möglicher „Falschmeldungen“ der Sicherheitstechnik sinkt die Systemverfügbarkeit. Ein sinnvoller Kompromiss aus Betriebssicherheit und Verfügbarkeit ist deshalb notwendig. Das neue Konzept ist dadurch gekennzeichnet, dass am Anfang in einer System-Synthese die Struktur des Arbeitsprozesses bestimmt wird. Aus der Anforderungsliste für das Gesamtsystem ergibt sich dabei die Unterteilung in Teilsysteme mit untergeordneten Funktionen. Aus den sicherheitsrelevanten Funktionen der Teilsysteme lassen sich danach erste Ergebnisse für notwendige MSR-Schutzeinrichtungen mit in ein Lastenheft übernehmen.

System- und Risikoanalyse

Ziel der System- und Risikoanalyse ist es, durch systematisches Vorgehen eine qualitative Risikoabschätzung für das Gesamtsystem und jede einzelne angedachte MSR-Schutzfunktion zu ermöglichen. Mit der Einschätzung des Risikos kann entschieden werden, welche Maßnahmen zu ergreifen sind, um der geforderten Sicherheit gerecht zu werden. In DIN V 19250 [5] und 19251 [6] wird ein systematischer Weg zur Bestimmung von Anforderungsklassen mit Hilfe eines Risikographen beschrieben. Sicherheitsanforderung kann zum Beispiel eine Fehlermöglichkeits- und -einflussanalyse (FMEA) nach [7] sein. Die Vorgehensweise bei der FMEA landwirtschaftlicher Feldarbeiten wurde ausführlich in [3, 4] beschrieben.

Systemabsicherung nach dem V-Modell

Die Entwicklung von Steuergeräten nach einem methodischen Konzept erleichtert die Vorgehensweise, etwa nach dem etablierten sogenannten V-Modell [8]. In *Bild 1* wird ein Vorschlag für ein angepasstes V-Modell gemacht. Die Vorgehensweise führt auf dem linken Ast von der Spezifikation auf Systemebene über Funktions- und Modulebene zur eigentlichen Implementierung und am rechten Ast wieder zurück zur geprüften Gesamtrealisierung. Die einzelnen Ebenen sind durch iterative Systemtests, Integrationstests und Modultests miteinander vernetzt. In Bild 1 sind außerdem die jeweiligen Einsatzmöglichkeiten verschiedener Methoden (MIL, FMEA, RCP, HIL, ...) gezeigt, mit denen eine geschlossene Werkzeug-Kette von der Spezifikation bis zur Validation erreicht werden kann [9].

Die System-Integration mit Verifikation und Validation schließt das Entwicklungs-

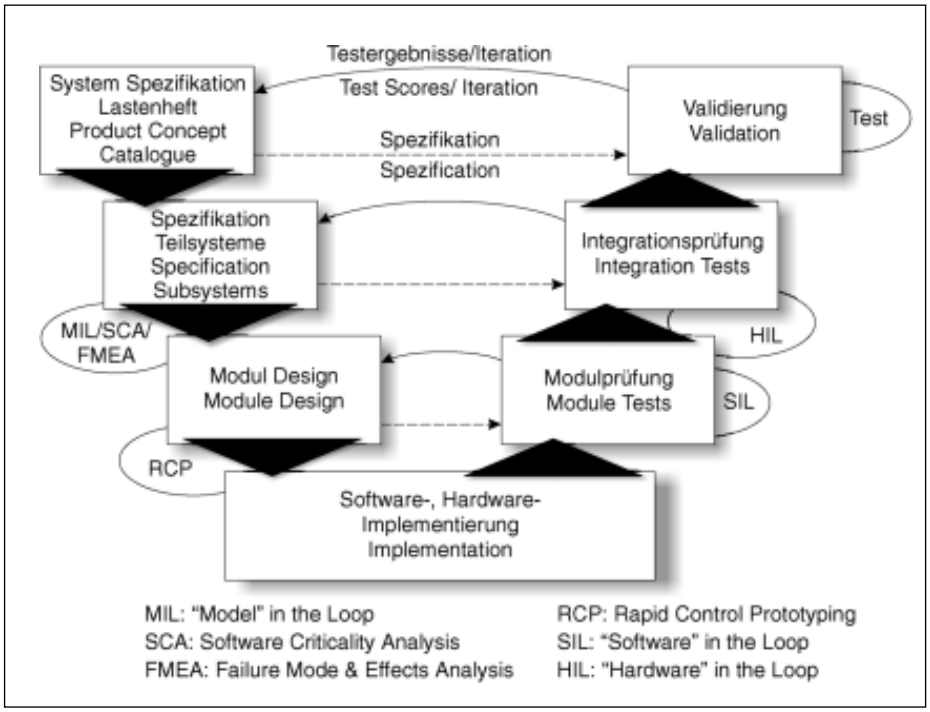

Bild 1: Angepasstes V-Modell zur Steuergeräteentwicklung

Fig. 1: Adjusted V-Model for development of electronic control units (ECUs)

konzept ab. Die Durchführung von Komponententests, Prüfstandsversuchen und Feldtests soll hier die Sicherheit, aber auch die Verfügbarkeit des Systems nachweisen. Die konzipierten MSR-Schutzeinrichtungen müssen auf Fehler richtig reagieren. Tests unter möglichst extremen Umweltbedingungen [10] und hinsichtlich Elektromagnetischer Verträglichkeit (EMV) [11, 12, 13] schließen die Validierung ab.

Beispielhafte Umsetzung einer Gespannautomation

Um ein möglichst aussagefähiges System zur Analyse der Prozesssicherheit zu finden, sollten in dem elektronischen Zusammenspiel mehrere Schnittstellen zwischen Fahrer, Traktor und Gerät angesprochen werden. Als besonders geeignet für die Untersuchung der Prozesssicherheit wurde eine Bestellkombination bestehend aus Traktor und Frontpacker, Kreiselegge und aufsattelbarer pneumatischer Drillmaschine ausgewählt. Geräte und Traktor sollten dabei mit einem CAN-BUS nach ISO 11783 [14] zur freien Datenkommunikation ausgerüstet sein.

Als Applikation wurde eine neuartige vollständige Automation des Vorgewendemanagements in das System integriert [15, 16]. In diesem Konzept wird der gesamte Arbeitsablauf beim Ein- und Aussetzen des Gespanns mit einem einzigen Knopfdruck durchgeführt. Der Knopfdruck bestimmt den virtuellen Ein- oder Aussetzpunkt des Gespanns. Die programmgesteuerten Anbaugeräte kontrollieren daraufhin ihre Schnittstellen zum Traktor (Hubwerke, Zapfwellen, Zusatzhydraulik [17, 18]) und die Traktorfahrgeschwindigkeit genau so, dass jedes einzelne an dem vorgegebenen Punkt mit seiner Arbeitsfunktion beginnt oder endet.

Während der Reihenfahrt wird über die zentrale Auftragsbearbeitung zusätzlich die Aussaatmenge, die maximale Fahrgeschwindigkeit und, als Versuch zur Steuerung des Arbeitsergebnisses der Kreiselegge, das maximal zulässige Drehmoment an der Heckzapfwelle vorgegeben. Diese Vorgabe wird, ebenso wie die des Vorgewendemanagements, nicht an den Traktor, sondern an die Anbaugeräte gegeben. Sowohl Drillmaschine als auch Kreiselegge können dann entsprechend ihrem Regelziel beispielsweise die Fahrgeschwindigkeit des Traktors beeinflussen.

Sicherheitstechnische Untersuchung „Gerät steuert Traktor"

Überlegungen in der Systemsynthese zeigten, dass der Zugriff der einzelnen Geräte auf die Traktorressourcen Hubwerke, Zapfwelle und hydraulische Zusatzventile exklusiv für die betrachtete Schnittstelle erfolgen muss. Die Zuordnung von Schnittstelle und Gerät muss hier eindeutig sein und kann beispielweise über Interaktion mit dem Traktorfahrer erfolgen. Kritischer in der Priorisierung des momentanen Reglerzugriffs ist die Geschwindigkeitsregelung des Gespanns. Hier sind bei der Anforderung der Sollgeschwindigkeit konkurrierende Gerätekommandos an den Traktor möglich.

Diejenige MSR-Schutzeinrichtung, die für die richtige Priorisierung konkurrierender Geschwindigkeitswünsche verantwortlich ist, wurde in einer Risikoanalyse untersucht. Für die Absicherung des Gesamtsystems wurde eine System-FMEA mit dem Werkzeug IQ-FMEA der Firma APIS durchgeführt, welches die strukturierte Vorgehensweise nach VDA 4.2 [7] enthält. Damit konnten weitere potenzielle Fehlerfälle nach Ursache und Auswirkung identifiziert und Abhilfemaßnahmen aus der System-FMEA iterativ in die Programmierung des Traktorrechners aufgenommen werden.

Als Ergebnis ist die in *Bild 2* dargestellte Hierarchie der Sollwertgeber im Gespann zu berücksichtigen. Die Geschwindigkeitsregelung beim Ein- und Aussetzvorgang sowie beim Reihefahren birgt dort das größte Risikopotenzial, wo auch Regler gleicher Ebene gleichzeitig Vorgaben an den Traktor machen können. Hier gilt im ersten Ansatz die Priorisierung des kleinsten Wertes.

Ausblick

Die Gespannautomation wurde zunächst in der Simulation und darauf folgend mit simulierten Gerätevorgaben an den Traktor realisiert. Als nächster Schritt sollen diese auf dem ISO Geräte-BUS durch reale Kommandos der Anbaugeräte ersetzt und damit die Funktion „Gerät steuert Traktor" vollständig implementiert werden. Mit Feldversuchen sollen dann die herausgefundenen Sicherheitsmaßnahmen überprüft und der Vorschlag für einen „Entwicklungsleitfaden für sicherheitsgerichtete elektronische Steuerungen in Landmaschinen" weiter verbessert werden.

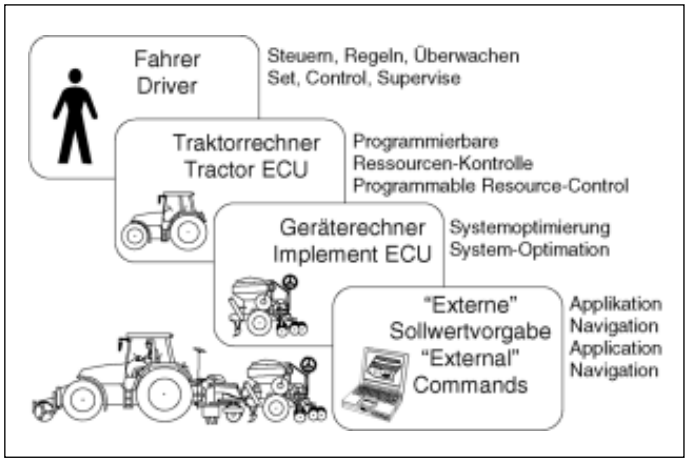

Bild 2: Sollwert-Hierarchie im Traktor/Geräte-Gespann

Fig. 2: Control-target-hierarchy of the tractor implement combination