Marcus Martinus und Rüdiger Freimann, Garching

Prozesssicherheit automatisierter Abläufe bei Traktoren und Arbeitsmaschinen

Im Rahmen dieser von der Landtechnik Vereinigung (LAV) angeregten Arbeit werden Grundlagen geschaffen, um automatische Arbeitsabläufe (bis hin zur autonomen Navigation) hinsichtlich ihres Gefährdungspotentials für Mensch und Umwelt beurteilen und damit sicher gestalten zu können. Mit Hilfe von FMEA (Fehlermöglichkeits- und -einflussanalyse) und Simulation von Arbeitsvorgängen am PC werden Lösungsansätze erarbeitet, welche bereits in einem frühen Stadium der Entwicklung anwendbar sind.

Technische Entwicklungen lassen Arbeitsvorgänge in der Landwirtschaft durch Automatisierung immer effektiver werden [1]. Ziel ist es dabei, die Wirtschaftlichkeit von Arbeitsmaschinen zu erhöhen und den Fahrer mehr und mehr von seinen Regelaufgaben zu entlasten. Da der Fahrer dadurch aber auch immer weniger Eingriffsmöglichkeiten in den Prozessablauf hat, muss verstärkt auf die Betriebssicherheit der automatisierten Vorgänge geachtet werden. Am Lehrstuhl für Landmaschinen der TU München wurde in einem durch die Stiftung Landtechnik geförderten Projekt zur „Prozesssicherheit im Betrieb von Traktoren und selbstfahrenden Landmaschinen" [2] ein neues Konzept entwickelt.

Konzept zur Untersuchung der Prozesssicherheit

Man beginnt am besten mit der Untersuchung einer möglichst großen Anzahl repräsentativer Maschinen und Einsatzfälle. Hierfür wurde ein Konzept aus Prozesssynthese, Prozessanalyse, Simulation des Systems am Rechner und realem Versuch (*Bild 1*) aufgebaut. Die einzelnen Arbeitsschritte sind durch mögliche Rückkopplungen miteinander verbunden.

Nach Auswahl des zu untersuchenden Arbeitsvorgangs ist es nötig, die erfassbaren Signale sowie sicherheitsrelevante Schnittstellen des Systems zu bestimmen und damit die Grundlage für die Prozessanalyse und darauf folgende FMEA [3, 4, 5] zu schaffen.

Prozess-FMEA in der Landtechnik

Die FMEA legt tabellarisch die potentiellen Fehlerfälle dar und zeigt auf, welche Folgen aus den verschiedenen Fehlern resultieren können und welche Ursachen den Fehlern vorausgingen. Die einzelnen Fehlerfälle werden anhand der Kriterien Auftretenswahrscheinlichkeit A, sicherheitstechnische Bedeutung B und Entdeckenswahrscheinlichkeit vor Eintreten der Fehlerfolgen E jeweils von 1 (gut) bis 10 (schlecht) bewertet (*Tab. 1*). Das Produkt der drei Bewertungen ergibt die Risiko-Prioritäts-Zahl (RPZ) des Fehlers. Mit ihr wird entschieden, ob ein sicherheitsrelevanter Fehler vorliegt und Abhilfemaßnahmen getroffen werden müssen. Die Bewertungskriterien A, B und E wurden an die Randbedingungen beim Arbeiten mit landwirtschaftlichen Maschinen und Geräten angepasst. Bei der Auftretenswahr-

Fortsetzung Seite 227

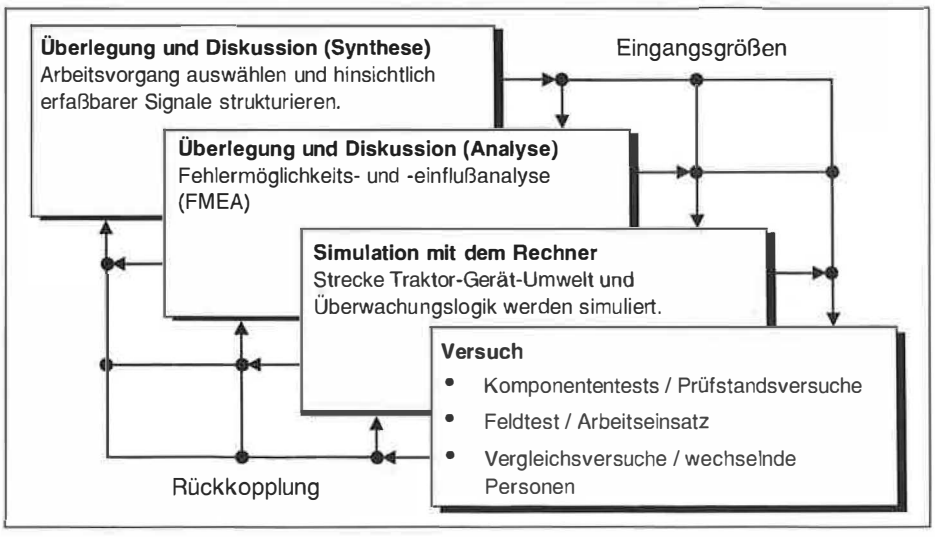

Bild 1: Konzept zur Untersuchung der Prozesssicherheit

Fig. 1: Concept tfor examining process safety

Dipl.-Ing. Marcus Martinus und Dipl.-Ing. Rüdiger Freimann sind Wissenschaftliche Mitarbeiter am Lehrstuhl für Landmaschinen, Technische Universität München, 85748 Garching (Leitung: Prof. Dr.-Ing. Dr. h.c. K.Th. Renius); e-mail: martinus@ltm.mw.tum.de, freimann@ltm.mw.tum.de

Schlüsselwörter

Prozesssicherheit, FMEA, Simulation, Landmaschinen

Keywords

Process safety, FMEA, simulation, agricultural machinery

Literaturhinweise sind vom Verlag unter LT 99406 erhältlich oder über Internet http://www.landwirtschaftsverlag.com/landtech/local/fliteratur.htm abrufbar.

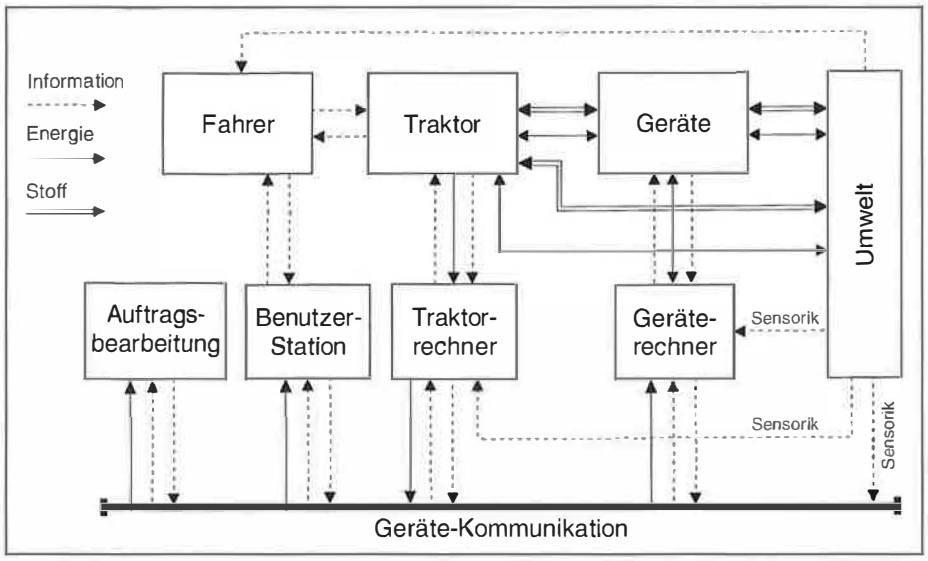

Bild 2: Signalflussplan der Simulation Fahrer/Traktor/Gerät mit ISO 11783 oder LBS

Fig. 2: Signal flow chart of simulating driver/tractor/implement, using ISO 11783 or LBS

scheinlichkeit wurde die Fehlerhäufigkeit auf die Anzahl der zu erwartenden Arbeitseinsätze während eines Maschinenlebens bezogen. Die Bewertung der Bedeutung des Fehlers wurde vorrangig nach sicherheitstechnischen Gesichtspunkten ausgelegt und nicht, wie bei der Konstruktions-FMEA, nach konstruktiven oder produktionstechnischen Grundsätzen. Bei der Entdeckenswahrscheinlichkeit richtet man sich nach dem Wahrnehmungsvermögen des Fahrers und eingesetzter unterstützender Automatiken.

Grundsätzlich ist ein Fehler näher zu betrachten, wenn seine RPZ den Wert 125 übersteigt. Zusätzlich ist der sicherheitsrelevante Fehler dadurch gekennzeichnet, dass er eine Schädigung von Mensch und Maschine nach sich ziehen würde, also seine Bedeutung B größer oder gleich 7 ist. Eine Ausnahme zur 125-Grenze ist der Fehler mit einer RPZ von 100, der durch eine akute Personengefährdung (Bedeutung B = 10) und ebenfalls einer Bewertung von 10 eines der beiden anderen Kriterien A oder E entsteht. Auch dieser ist dann sicherheitsrelevant einzustufen, da er entweder nicht zu entdecken ist oder ständig auftritt. Wurden für einen Fehlerfall bestimmte Abhilfemaßnahmen getroffen, so kann er in einem weiteren Analysedurchgang neu bewertet werden.

Simulation des Systems Traktor/Gerät/Mensch/Umwelt

Der nächste Schritt in der Untersuchung der Prozesssicherheit ist die Simulation des Systems Traktor/Gerät/Mensch/Umwelt am PC. Mit Hilfe des Programmpaketes MATLAB/SIMULINK können Systemabläufe in ihrem Zusammenwirken bis ins Detail nachgebildet und Fehler durch Manipulation am System provoziert werden. Dies ermöglicht sowohl die Überprüfung der in der FMEA beschriebenen Fehlerauswirkungen als auch die Rückführung neuer Erkenntnisse in die sicherheitstechnische Bewertung. Zusätzlich kann die erarbeitete Simulation als Basis dienen, um in einer simulierten Datenübertragung zwischen Traktor und Gerät(en) Kommunikationsstrukturen und programmierte Sicherheitsabfragen zu überprüfen.

Der Aufbau der Simulation gestaltet sich entsprechend der Darstellung in *Bild 2*. Hier sind die verschiedenen Systemkomponenten in einem Signalflussplan mit „Information", „Energie" oder „Stoff" verbunden und rückgekoppelt. Die Kommunikation der Einzelrechner, die die jeweiligen Systemkomponenten im Netzwerk repräsentieren, erfolgt über LBS [6] oder ISO 11783 [7].

Über eine Softwareschnittstelle kann unabhängig programmierter Quellcode in die Simulation eingebunden werden. Damit ist es möglich, Programmstrukturen realer Steuergeräte zu integrieren und die korrekte Abarbeitung von Sicherheitsstrategien in einem sogenannten SIL (Software-in-the-Loop)-Test [8, 9] zu verifizieren.

Neben den SIL-Tests kann auch reale Hardware, etwa ein Steuergerät, in die Simulation integriert werden (Hardware-in-the-Loop). Hierfür ist die Erweiterung der verwendeten Simulationssoftware mit einer Echtzeit-Schnittstelle möglich. Die Einbindung der Hardware in die Simulationen ist ein wichtiger Schritt für die gefahrlose Erprobung sicherheitskritischer Anwendungen oder Automationen vor der Implementierung in das reale Fahrzeug.

Abschließende Systemüberprüfung im Feldversuch

Obwohl der beschriebene Weg der Simulation schon sehr gute Aussagen über sicherheitsrelevante Zustände und Größen liefern kann, ist ein abschließender Feldversuch mit dem kompletten Fahrzeug nicht vollständig zu ersetzen. Der Aufwand mit Prototypen wird aber erheblich reduziert, da sowohl Software als auch Steuerungshardware weitgehend vorab erprobt sind.

Erst unter Ausnutzung aller Hilfsmittel: Synthese, Analyse, Simulation und Versuch und deren Rückkopplung untereinander kann die Prozesssicherheit von einzelnen Arbeitsvorgängen vollständig nachgewiesen und dokumentiert werden.

Tab. 1: Beurteilungskriterien der FMEA / *Table 1: Assesssment criteria of the FMEA*

Auftretenswahrscheinlichkeit A: Wahrscheinlichkeit für das Auftreten einer Fehlfunktion im Zeitraum von 10 000 Arbeitseinsätzen im zehnjährigen Gesamtlebenszyklus	**Bedeutung B : Bedeutung für Bedienpersonen, unbeteiligten Personen, Maschine und Umwelt**	**Entdeckenswahrscheinlichkeit E: Wahrscheinlichkeit der Entdeckung des Fehlers und Vermeidung der Fehlerauswirkungen vor Schadenseintritt**
Unwahrscheinlichkeit Fehlerrate 0 Bewertung 1 (Nie)	Unbedeutender Fehler Unbemerkt Bewertung 1	Hoch 99,99% Bewertung 1
Sehr gering Fehlerrate 1/10 000 Bewertung 2-3 (Einmal im Leben)	Geringfügiger Fehler Belästigung Bewertung 2-3	Mäßig Automatische Bewertung 2-5 Prüfung
Gering Fehlerrate 1/1000 Bewertung 4-6 (Einmal im Jahr)	Mittelschwerer Fehler technischer Bewertung 4-6 Ausfall	Gering Sichtprüfung Bewertung 6-8
Mäßig Fehlerrate 1/100 Bewertung 7-8 (Mehrmals im Jahr)	Schwerer Fehler Schädigung Bewertung 7-8 von Mensch und Maschine	Sehr gering 80-90% Bewertung 9
Hoch Fehlerrate >1/2 Bewertung 9-10 (Fast bei jedem Einsatz)	Äußerst schwerer Fehler akute Gefahr Bewertung 9-10 für Personen	Unwahrscheinlich < 80% Bewertung 10