Marcus Martinus, Garching

Sicherheitsgerichtetes Entwicklungskonzept für mechatronische Systeme bei Landmaschinen

Im Rahmen des DFG-Projektes „Prozesssicherheit Landmaschinenelektronik“ werden am Lehrstuhl für Landmaschinen der Technischen Universität München automatisierte Arbeitsvorgänge bei Traktor/Gerätekombinationen und selbstfahrenden Arbeitsmaschinen hinsichtlich ihrer Prozesssicherheit untersucht und ausgelegt. Dazu wurde ein sicherheitsgerichtetes Entwicklungskonzept aus Entwicklungsschritten, Methoden und Werkzeugen erarbeitet, welches das schrittweise Vorgehen von der System-Synthese bis zur Validierung (Funktionsbeweis) von mechatronischen Systemen beschreibt.

Dipl.-Ing. Marcus Martinus ist wissenschaftlicher Assistent 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*

Schlüsselwörter

Landmaschine, Prozesssicherheit, Entwicklungsmethodik, Elektronik, FMEA, V-Modell, Simulation

Keywords

Agricultural machinery, process safety, development methods, electronics, FMEA, V-model, simulation

Die Arbeitsprozesse von Traktor/Gerätekombinationen und selbstfahrenden Arbeitsmaschinen erreichen einen immer höher werdenden Grad der Elektronifizierung [1]. Um die Betriebssicherheit der Systeme bei angemessenem Aufwand auch weiterhin zu gewährleisten, ergeben sich neue Anforderungen an die Entwicklungsprozesse der mechatronischen Systeme.

Als Anwendungsbeispiel für automatisierte geräteseitige Traktorsteuerungen [2] wurde eine Gespann-Kombination aus Traktor mit Ringpacker im Frontanbau, Kreiselegge und aufsattelbarer pneumatischer Drillmaschine im Heckanbau mit Elektronik ausgerüstet.

Vorgehen und Auswahl von Methoden

Bei der Entwicklung der drei Geräterechner und des Traktorrechners, welche die Funktion „Gerät steuert Traktor“ bereitstellen, hat sich ein schrittweises Vorgehens-Modell (V-Modell) aus Entwicklungsschritten und Methoden von der System-Spezifikation bis zur System-Validierung bewährt [3]. Begünstigt durch die Erfahrungen des Anwendungsbeispiels wurde ein auf Landmaschinenelektronik verallgemeinertes V-Modell entwickelt, welches die Auswahl der einzelnen Methoden erleichtert und die Zwischenergebnisse aus Spezifikation und Test der einzelnen Detaillierungsebenen einander zuordnet (*Bild 1*).

Die Ergebnisse des Testzweiges und die Anforderungen des Spezifikationszweiges des V-Modells werden interpretiert und als Wissensbasis (Entscheidungsdokumentation) dokumentiert. Neue in Tests erworbene Erkenntnisse können eine Änderung der Spezifikation in der jeweiligen Detaillierungsebene des Systems notwendig machen. Nachfolgend werden die einzelnen Schritte des V-Modells und ausgewählte Beispiele für geeignete Entwicklungsmethoden kurz beschrieben.

Abbildung der Systemstruktur

Die allgemeinen Systemfunktionen werden im ersten Schritt mittels Strukturanalyse aus den Anforderungen entwickelt und in Funktionsgruppen und -modulen angeordnet. Die Methode der Black-Box-Darstellung mit Energie-, Stoff- und Informationsflüssen erleichtert dabei die Definition der Schnittstellen.

Um eine möglichst umfassende Durchgängigkeit von modellbasierten Methoden (CASE-Tools) während des gesamten Entwicklungsprozesses zu erhalten, können Requirement Management Werkzeuge (etwa DOORS) verwendet werden, die Funktionsanforderungen aus dem Lastenheft dokumentieren und die direkte Verbindung zu Funktionsmodellen (etwa MATLAB) herstellen [4]. Die Modelle werden später weiterverwendet und im Idealfall durch aus der Simulation automatisch generierten Code auf der Zielhardware implementiert (Vorteil einer durchgängigen Tool-Kette).

Die Methoden Risikoanalyse [3] und System-FMEA (Fehlermöglichkeits- und -einflussanalyse) [5] lassen erste Rückschlüsse auf das Gefährdungspotenzial und daraus resultierende Anforderungen zu.

Spezifikation der Subsysteme und Module

Im nächsten Schritt werden die Funktionen auf Funktionsgruppen einzelner Subsysteme und Module verteilt und dadurch die Anforderungen an Hardware und Software festgelegt.

Den Schwerpunkt bilden theoretische Untersuchungsmethoden der System-FMEA und Risikoanalyse. Potenzielle Fehlerfälle werden aufgezeigt und hinsichtlich Risiko klassifiziert. Risikoanalyse und System-FMEA können sich dabei ideal ergänzen und gehen in der Anwendung Hand in Hand. Erste Ansätze für MSR-Sicherheitsfunktionen (Messen, Steuern, Regeln) können daraus abgeleitet werden.

Entwickelte Algorithmen und Reglermodelle lassen sich gefahrlos am Rechner an der simulierten Strecke „Model in the Loop“ testen und durch Rapid Control Prototyping über eine spezielle Echtzeit-Hardware im Fahrzeug online auslegen.

Hardware-, Software-Implementierung

Bei den Entwicklungsschritten der Komponentenebene kommen die Vorteile einer ge-

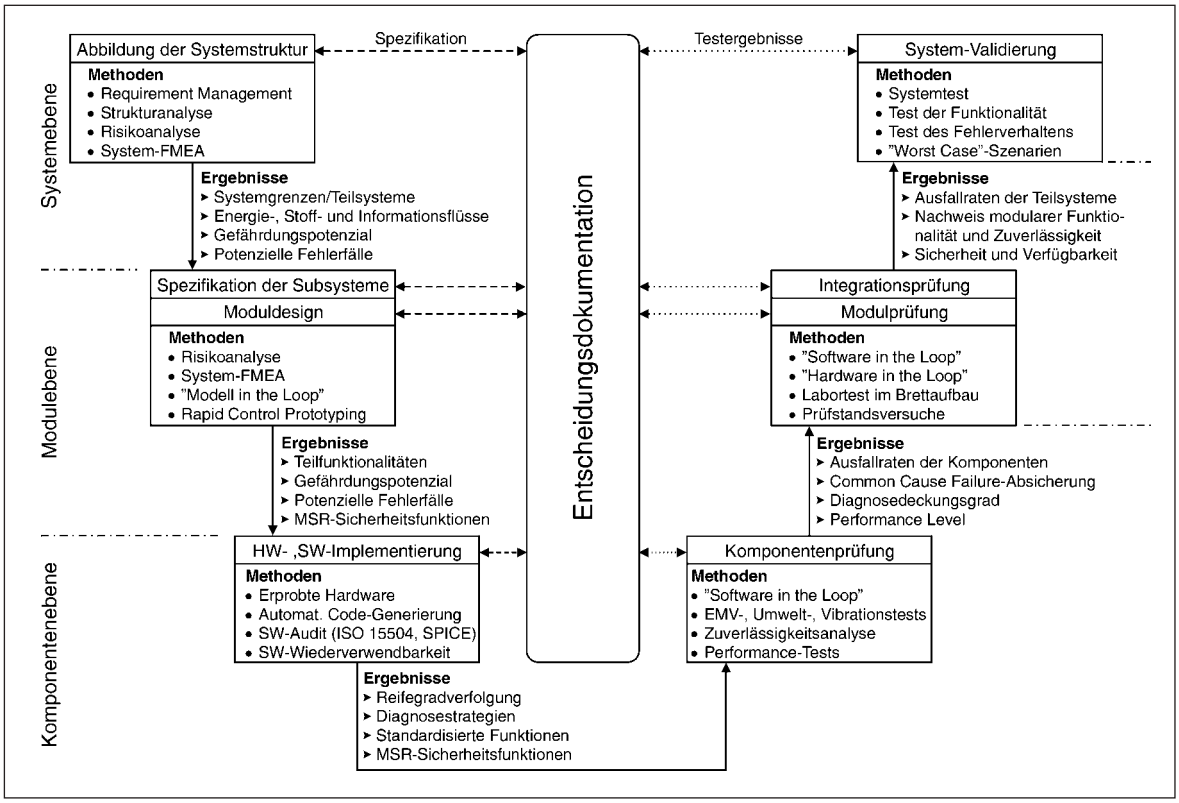

Bild 1: V-Modell zur Entwicklung sicherer mechatronischer Systeme mit Auswahl von Methoden

Fig. 1: V-Model for development of safe mechatronic systems with selection of methods

schlossenen Kette aus modellbasierten Methoden [6] zum Tragen. Die automatische Code-Generierung übersetzt die entwickelten und bereits getesteten Funktionsmodelle in Seriencode und verkürzt dabei die Entwicklungszeit.

Durch konventionelle Methoden, wie Wiederverwendung erprobter Software- und Hardware-Komponenten, wird der Aufwand verkleinert und der Reifegrad der Systeme verbessert. Für die Entwicklung von sicherem und qualitativ einwandfreiem C-Code stehen Software-Standards in Form von Programmier-Richtlinien (MISRA-Regeln [7]) zur Verfügung. Die Norm ISO/IEC 15504 [8] (SPICE) liefert den Maßstab für die Bewertung von SW-Entwicklungsprozessen (SW-Audit) und vertieft die für die Software-Entwicklung wesentlichen Prozessbereiche [7].

Komponentenprüfung

Auf der Testseite werden durch modellbasierte oder konventionelle Methoden die Komponenten auf Funktionalität und Ausfallsicherheit erprobt.

Die Hardware kann durch Komponententests, wie EMV-Prüfung (elektromagnetische Verträglichkeit) oder Umweltstressversuche überprüft werden. Bei der Software gilt der „Software in the Loop"-Test als effektive Methode, programmierten Code unter sicheren Bedingungen in der Simulation der Strecke (Fahrzeug, Sensor/Aktor-Einheit) am PC zu testen.

Intergrations- und Modulprüfung

Im nächsten Entwicklungsschritt nimmt der Detaillierungsgrad der zu testenden Systeme weiter ab. In der Modulprüfung und später in der Integrationsprüfung werden Sicherheit und Verfügbarkeit der Sub-Systeme überprüft. So können beispielsweise fertig programmierte und konfektionierte elektronische Steuerrechner konventionell im Brettaufbau durch simulierte Ein- oder Ausgänge auf Funktion geprüft werden.

Alternativ wird im modellbasierten „Hardware in the Loop"-Test ein Steuerrechner über eine Echzeit-Entwicklungsumgebung in die am PC simulierte Regelstrecke eingebunden und so unter Berücksichtigung realistischer Anwendungssituationen getestet.

System-Validierung

Im letzten Schritt des Entwicklungskonzepts soll die Funktionalität des Gesamtsystems sowie das richtige Verhalten im Fehlerfall nachgewiesen werden.

Versuche unter realen Einsatzbedingungen bis hin zum ungünstigsten Fall, in dem sicherheitskritische Systemfehler provoziert werden, sind hier zu nennen. Grundsätzlich müssen die Systeme so ausgelegt sein, dass der sichere Zustand zu jedem Zeitpunkt gewahrt bleibt [3].

Fazit

Das vorgestellte Entwicklungskonzept dient als Leitfaden für die Entwicklung von mechatronischen Systemen bei Landmaschinen. Zur Entwicklung komplexer systemübergreifender Elektroniken („Gerät steuert Traktor") empfiehlt es sich, überschaubare Teilsysteme zuerst getrennt von einander zu betrachten und später im Gesamtsystem sukzessive zusammenzuführen. Während eines kompletten Entwicklungsprozesses ergibt sich so im Realfall ein Vorgehen nach verschachtelten V-Modellen für Teilsysteme im Rahmen eines übergeordneten V-Modells für das gesamte Maschinensystem.

Auf Grund von Parallelen in Systemaufbau, verwendeten Technologien und Arbeitsumfeld ist das Entwicklungskonzept unter Anpassung einiger Methoden allgemein auf die Anwendung bei mobilen Arbeitsmaschinen erweiterbar.

Literatur

[1] *Lang, Th.*: Mechatronik in Landmaschinen. Jahrbuch Agrartechnik. Landwirtschaftsverlag, Münster, 15 (2003), S.71-75, 275-276

[2] *Renius, K.Th.*: Entwicklungstendenzen bei Traktor-Geräte-Kombinationen. Vortrag und Diskussion im Arbeitskreis Technik, VDMA Fachverband Landtechnik, Frankfurt/M., 15. 2. 2001

[3] *Martinus, M. und R. Freimann*: Prozesssicherheit Landmaschinenelektronik – Gerät steuert Traktor. LANDTECHNIK 57 (2002), H.3, S. 142-143; Agrartechnische Forschung 8 (2002) H.3, S. 61-69

[4] *Kokes, M. und A. von Querfurth*: Methodik zur Spezifikation von Elektronik im Fahrzeug. VDI-Tagung „Elektronik im Kraftfahrzeug 2001" Baden-Baden 27./28. 9. 2001. VDI-Berichte 1646, VDI- Verlag, Düsseldorf, 2001, S. 169-179

[5] *Martinus, M.*: System-FMEA als Methode bei der Entwicklung von Landmaschinenelektronik. VDI-MEG-Tagung „Landtechnik 2002", Halle, 10./11. 10. 2002. VDI-Berichte 1716, VDI-Verlag, Düsseldorf, 2002, S. 357-362

[6] *Wohnhaas, A. und H.-J. Habrock*: Szenarien und Schritte bei der Einführung modellbasierter Methoden in der Kfz-Elektronikentwicklung. VDI-Tagung „Elektronik im Kraftfahrzeug 2000" Baden-Baden , 5./6. 10. 2000. In: VDI-Berichte 1547, VDI-Verlag, Düsseldorf, 2000, S. 327-345

[7] *Thomsen, T.*: Integration automotiver Standards in die Seriencodegenerierung. VDI-Tagung „AUTOREG 2002 – Steuerung und Regelung von Fahrzeugen und Motoren", Mannheim, 15./16. 4. 2002. VDI-Berichte 1672, VDI-Verlag, Düsseldorf, 2002, S. 205-221

[8] –: Informationstechnik – Bewertung von Software-Prozessen. Norm ISO/IEC TR 15504. Beuth Verlag, Berlin, 1998