Gerhard Henninger, Frankfurt am Main

Sicherheitsbezogene Teile von Steuerungen in mobilen Landmaschinen

Mit der zunehmenden „Elektronisierung" der Landmaschinen und dem Wandel von elektromechanischen hin zu elektronischen Steuerungen (µC) ergibt sich auch die Notwendigkeit, die Normen an sich [2] und für die Agrartechnik anzupassen.

Dazu werden in diesem Beitrag kurz die relevanten, bestehenden Normen beleuchtet und der Normenentwurf, der auf der Grundlage der Arbeiten der Arbeitsgruppe Sicherheit des Technischen Ausschuss Elektronik im VDMA Fachverband Landtechik entstanden ist, erläutert.

Dipl.-Ing. (TU) Gerhard Henninger ist Sekretär des ISO Subkomittees ISO/TC 23/SC 19 Agricultural Electronics im Fachverband Landtechnik des VDMA, Lyoner Straße 18, 60528 Frankfurt am Main; e-mail: *gerhard.henninger@vdma.org*

Schlüsselwörter

Lebenszyklus, Probabilistik, Risikoanalyse, Sicherheitskultur

Keywords

Lifecycle, probabilistic, risk analysis, safety culture

Elektronische Steuerungen und Regelungen in vernetzten Kommunikationssystemen von Landmaschinen [1] steuern in zunehmendem Maße sicherheits-relevante Funktionen wie Fahrantrieb, Lenkung und Bremsen. Da Elektronik eine vergleichsweise junge Disziplin im Fahrzeugbau ist, herrscht Unsicherheit bezüglich der sicheren Verfügbarkeit von Funktionen. Konstruktive Lösungen basieren zum einen auf langjährig bewährten Lösungen und zum anderen existieren seit Jahren Normen und Richtlinien. Dadurch gelten diese Lösungen als sicher, insbesondere durch höhere Auslegung der mechanischen Belastbarkeit.

Die Mutter der Sicherheitsnormen IEC 61508

Die 1998 veröffentlichte Norm IEC 61508 [3] ist gültig für die Maschinen- und Prozess-Industrie und beschäftigt sich mit allen Aspekten der funktionalen Sicherheit während des gesamten Lebenszyklus einer Maschine oder Anlage. Sie hat sich zu einem grundlegenden und übergreifenden Standard für nahezu alle Arten sicherheitstechnischer Fragestellungen für die Bereiche Elektrik und Elektronik entwickelt.

Mit der IEC 61508 gab es einen Strukturwandel in der Normenwelt. Es wurden sowohl die Betrachtung des gesamten Lebenszyklus als auch der probabilistische (Wahrscheinlichkeit) Ansatz zusätzlich zum deterministischen (definierten, eindeutigen) Ansatz eingeführt.

Ein wesentlicher Nachteil dieser nicht harmonisierten Norm (es ist keine Vermutungswirkung zur Maschinenrichtlinie vorhanden) ist deren hohe Komplexität (über 450 Seiten unterteilt in sieben Teile). Daher ist diese Norm für kleine und mittlere Landtechnik-Unternehmen in der Praxis in dieser Form nicht umzusetzen.

EN 954-1 und die Nachfolger

Seit 1996 ist die EN 954-1 [4] eine der meist genutzten Standards, wenn es um Maschinen mit Sicherheitssteuerungen geht.

Mit dem Vormarsch der elektronischen Systeme ergab sich jedoch die Notwendigkeit der Revision dieser Norm. Insbesondere wurde gefordert, dass mit zunehmendem Risiko auch zusätzliche Maßnahmen einhergehen müssen, die das Restrisiko zusätzlich vermindern. Dazu gehört auch, dass in EN 954-1 keine ausreichenden Anforderungen für die Berücksichtigung von Zuverlässigkeitswerten existieren.

Um die Nachfolge von EN 954-1 „konkurrieren" dabei gleich zwei neue Normen: dies ist einmal die ISO 13849-1 [5], die als die direkte Nachfolge von EN 954-1 konzipiert wurde. Zum anderen „konkurriert" die Norm IEC 62061 [6], ein sektorspezifisches Derivat aus IEC 61508 für den Maschinenbau, um die Nachfolge der EN 954-1.

Sowohl mit der einen als auch der anderen Norm hält damit zusätzlich die Wahrscheinlichkeitsrechnung, also das Zuverlässigkeits-Engineering Einzug in die Ausführung sicherheitsbezogener Teile von Maschinensteuerungen. Dagegen basiert der Ansatz von EN 954-1 im Wesentlichen auf der Berücksichtigung von Strukturen (Steuerungskategorien). Insofern ist auch eine Abwärtskompatibilität nicht oder nur unzureichend gegeben.

Die Norm ISO 13849-1 versucht einen Balance-Akt zwischen bewährten Prinzipien der EN 954-1 und neuen Ansätzen der IEC 61508, deterministische und probabilistische Betrachtungen werden also bei der Ausführung von sicherheitsbezogenen Teilen von Maschinensteuerungen kombiniert. Der neue Aspekt des probabilistischen Ansatzes wird auf ein notwendiges und praktikables Maß für den „Durchschnittsanwender" von ISO 13849-1 reduziert. ISO 13849-1 beschäftigt sich ausschließlich mit dem Design von Sicherheits-Steuerungen und definiert keine organisatorischen Anforderungen.

Auch in ISO 13849-1 wird weiterhin ein Risikograph verwendet, jedoch führt die Betrachtung der Risikoparameter nicht mehr zu einer Steuerungskategorie wie in EN 954-1, sondern zu einem Performance Level (PL). Der PL beschreibt die Fähigkeit eines sicherheitsbezogenen Teils einer Maschinensteuerung, eine Sicherheitsfunktion auszu-

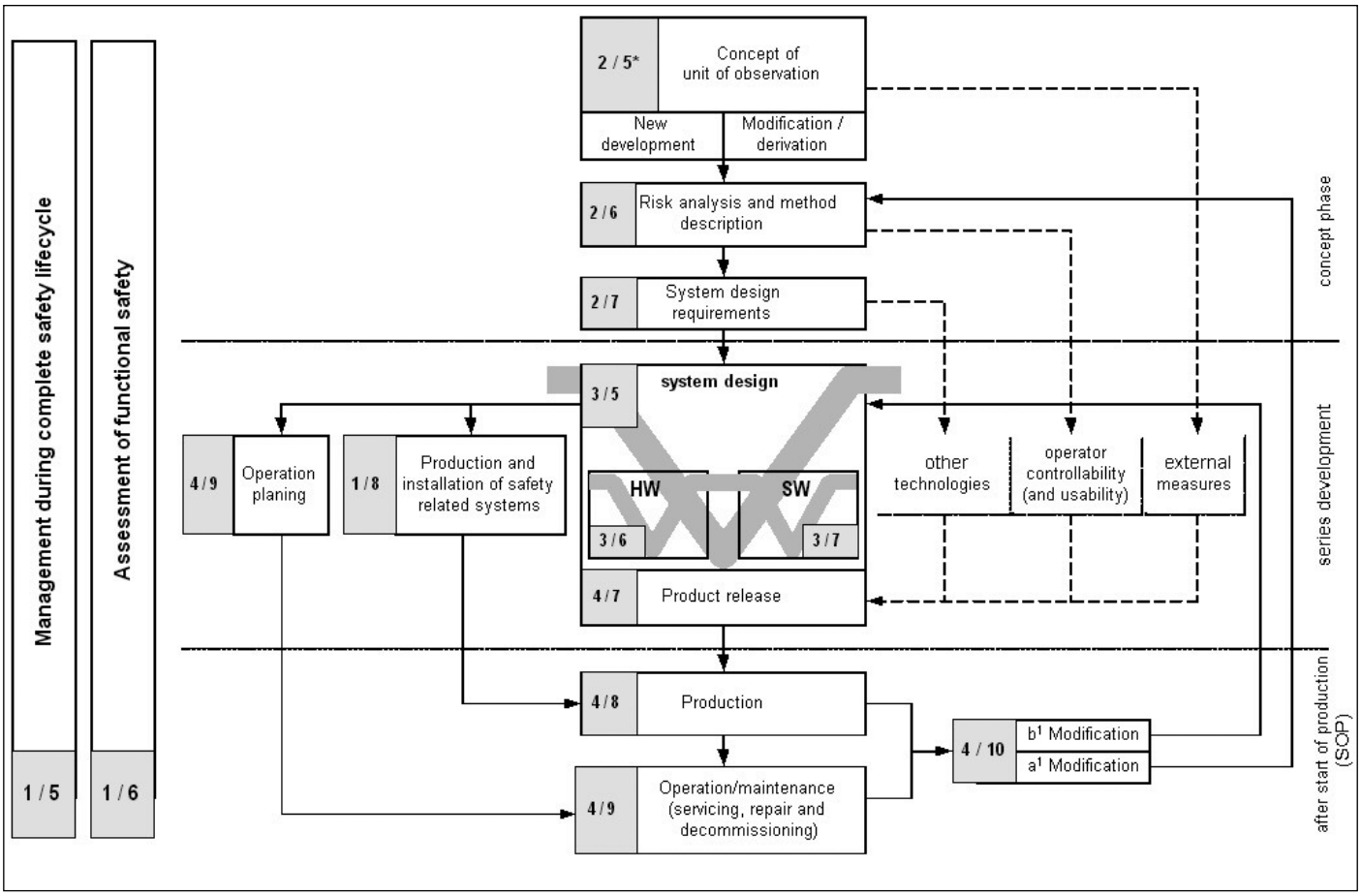

Bild 1: Sicherheits-Lebenszyklus

Fig. 1: Safety lifecycle

führen, um die geforderte Risikominderung zu erreichen. Diese Betrachtungsweise bezieht sowohl quantitative als auch qualitative Aspekte mit ein. Die einzelnen Risikoparameter (Schweregrad der Verletzung, Häufigkeit der Gefährdung sowie Möglichkeiten zur Vermeidung der Gefährdung) sind – verglichen mit EN 954-1 – in ISO 13849-1 unverändert geblieben.

Der Normenansatz für die Landtechnik

Vor dem Hintergrund der sich wandelnden Normenlandschaft und der wachsenden Notwendigkeit stellte sich für die Landtechnik die Frage, wie darauf reagiert werden könnte. Deshalb wurde auf Verbandsebene festgelegt, eine Produktnorm für die Bereiche der Land- und Kommunalmaschinen zu entwickeln. Ausgangspunkt war die EN ISO 13849.

Tab. 1: Norm ISO 25119 Teil 1- 4

Table 1: Standard ISO 25119 Part 1- 4

ISO 25119 Normteile:	
Teil 1:	General principles for design and development
Teil 2:	Concept phase
Teil 3:	Series development, Hardware, Software
Teil 4:	Production, Operation, Modification and supporting processes

Ziel war es, eine Norm zu entwickeln, die insbesondere von der mittelständisch geprägten Industrie einfach umzusetzen ist. Mit einer einfachen Struktur, Beispielen und einen an die bestehenden Prozesse innerhalb der Betriebe sich anlehnenden Aufbau der Norm wurde dies umgesetzt. Die neue ISO/CD 25119 [7] konzentriert sich dabei auf elektrische, elektronische und programmierbare elektronische Systeme. Die klassischen Maschinenbau-Disziplinen wie Mechanik, Hydraulik und Pneumatik werden im Gesamtkonzept nicht berücksichtigt, sind aber bei der Risikobeurteilung der sicherheitsrelevanten Funktionen mit einzubeziehen.

Die ISO/CD 25119 behandelt den gesamten Lebenszyklus der Komponenten und Systeme von der Idee bis zur Verschrottung (*Bild 1*). Es muss im Wesentlichen auf keine andere Sicherheitsnorm zurückgegriffen werden. Eine Ausnahme bilden die EN ISO 12100 Teile 1-2 [8] und ISO 14121 [9], die von der neuen Maschinenrichtlinie 2006/42/EG direkt herangezogen werden.

Die *Tabelle 1* zeigt die Teile der Norm ISO 25119.

Ein wesentlicher Ansatz ist der aus der EN ISO 13849 übernommene und weiter entwickelte Ansatz des „Performance Level“ hin zum AgPLr (required Agricultural Performance Level).

Ausgehend von der Risikoanalyse ergeben sich für den Entwickler mehrere Möglichkeiten den AgPLr zu erreichen. Verschiedene „Categories“ erfüllen zusammen mit dem neu eingeführten „SRL“ (software requirement level), dem „DC“ (diagnostic coverage) genannten Fehler Aufdeckungsgrad sowie dem $MTTF_{dC}$ (Mean Time to dangerous Failure for one channel – mittlere Zeit zum gefährlichen Ausfall für einen Kanal) den geforderten AgPLr. Mit den „Categories“ sind unterschiedliche Hardware-Architekturen gemeint, von einer ganz einfachen Struktur bis hin zur vollständig redundanten Ausführung. Eine einfache Struktur kann zusammen mit einer hohen gefährlichen Ausfallrate der Bauteile eines Kanals und einer guten Überwachung ebenso eine sichere Lösung bringen wie eine komplexere redundante Struktur mit geringeren $MTTF_{dC}$ und einfacher Überwachung. Dieses Vorgehen gibt jedem Entwickler (Unternehmen) die Möglichkeit, auf die spezifischen Belange der Maschine, des Projektes und/oder des Unternehmens einzugehen.

Für $MTTF_{dC}$ werden Datenbanken zum Nachschlagen der MTTF Daten genannt sowie die Umrechnung von Schaltzyklen (Relais, Schalter, ...) in Stunden. Ganz wichtig dabei ist: Es muss nur der Anteil berücksichtigt werden, der zu einem gefährlichen Ausfall führen kann. Beispiel: Relaiskontakt kann kurzgeschlossen (klebt) oder offen sein. Je nach Schaltungsausführung ist nur eine Situation potenziell gefährlich, also 50% der MTTF entsprechen in diesem Fall $MTTF_{dC}$ für den zu untersuchenden Kanal. Damit ergibt sich eine Verdoppelung der Werte in der Berechnung.

Für Hardware und Software wurden eigenständige, in sich geschlossene Abschnitte entwickelt. Dort sind Methoden, Werkzeuge, Vorgehensweisen für jede Entwicklungsphase (Planung, Design, Implementierung bis hin zum Verifizieren und Validieren) detailliert dargestellt. Für die verschiedenen $AgPL_r$ (a bis e) sind die jeweiligen Anforderungen dargestellt. Ein Entwicklungsingenieur kann sich durch das Zusammenfassen von Abschnitten in einem Normteil nur auf diesen konzentrieren und muss sich nicht mit den anderen Teilen beschäftigen („belasten").

Ein für die betriebliche Praxis weitreichender Ansatz von ISO/CD 25119 ist auch die Einbeziehung von notwendigen Management-Aktivitäten (functional safety management, assessment) über den gesamten Lebenszyklus der elektronischen Funktionen/ Komponenten. Die Benennung von verantwortlichen Stellen auf Hersteller- und Lieferanten-Ebene stellt ebenfalls einen gegenüber bisherigen Standards auf dem Gebiet der „Sicherheit elektronischer Systeme" neuen – und anspruchsvollen – Ansatz dar.

Alle unterstützenden Prozesse werden aufgeführt. Es werden Hinweise und Anforderungen an die Zusammenarbeit mit Zulieferanten ebenso beschrieben wie zum Beispiel auch die Vorgehensweise für den Service oder organisatorische Hinweise. Für alles, insbesondere auch für die Dokumentation, wurde auf die bestehenden Abläufe/ Strukturen in den Firmen Rücksicht genommen: Wer nach der ISO/CD 25119 vorgeht, erhält nicht nur eine sichere Elektronik, sondern es ergibt sich automatisch auch eine hohe Produktqualität.

Der Aufbau jeden Abschnitts in der ISO/CD 25119 gibt jeweils allgemeine Hinweise, Ziele und Vorbedingungen (Informativ) an. Im Anschluss folgen die Anforderungen (Normativ). Somit kann ein Entwickler einen Abschnitt wie den anderen bearbeiten.

Wichtig im Gesamtzusammenhang sind die Implementierung einer Sicherheitskultur im Unternehmen und der „rote Faden" (gleiche Lösungen für gleiche Funktionen), der sich durch alle Projekte ziehen sollte.

Die neue Norm ISO CD 25119 mit ihren Teilen 1 bis 4 liegt seit September 2007 als CD (Committee Draft) vor. Der Beginn der DIS Umfrage wird für das zweite Quartal 2008 erwartet.

Aktivitäten in anderen Branchen

Für die Baumaschinen gilt ISO/CD 15998 [10]. Diese Norm eignet sich als Guideline für Elektronik mit EMV- und Umweltanforderungen und der Risikobetrachtung gemäß IEC 61508; bezüglich Sicherheit wurden also keine produktspezifischen Anpassungen vorgenommen.

Für die Kfz-Industrie ist ebenfalls eine produktspezifische Norm für Personen-Kraftfahrzeuge in der Entwicklung und befindet sich zurzeit im Entwurfsstadium (ISO WD 26262 Teil 1-8 Road vehicles – Functional Safety [11]). Der Focus der Norm liegt ebenso wie beim Ansatz in der Land- und Kommunaltechnik auf der Ausführung von sicherheitsbezogenen Teilen von elektronischen Steuerungssystemen für Personen-Kfz bestimmter Klassen (M, N und O). Ein Abgleich zwischen den Normungsaktivitäten von VDMA und FAKRA fand statt.

Fazit

Mit der ISO CD 25119 liegt ein Normenentwurf vor, der es den Unternehmen in der Landtechnik einfacher ermöglicht, sicherheitsrelevante Funktionen für ihre Maschinen zu entwickeln und damit die Anforderungen aus den gesetzlichen Vorschriften und der Produkthaftung erfüllen. Es ist zu erwarten, dass nach Abschluss der Normungsarbeiten Produkte mit Steer-by-wire oder anderen by-wire Lösungen auf dem Markt erscheinen werden. Mit Hilfe der Norm können zum einen sichere Elektronik-Systeme entwickelt werden und zum anderen kann für die zuständigen Stellen der Nachweis der Sicherheit für die Zulassungen im Straßenverkehr einheitlich geregelt werden.

Literatur

Bücher sind mit • gezeichnet

[1] • *Böttinger, S., R. Buschmeier und P. Hieronymus*: Jahrbuch Agrartechnik 2004, Band 16, Kapitel 2.3 Kommunikationssysteme

[2] • *Gehlen, P.*: Funktionale Sicherheit von Maschinen und Anlagen. 1. Auflage, Erlangen, Publucis KommunikationsAgentur GmbH, 2007, ISBN-13: 978-3-89578-281-7

[3] IEC 61508 Functional safety of electrical/electronic/ programmable electronic safety-related systems

[4] EN 954 Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design

[5] ISO 13849 Safety of machinery – Safety-related parts of control systems

[6] IEC 62061 Safety of machinery – Functional safety of electrical, electronic and programmable control systems for machinery

[7] ISO/CD 25119 Teil 1-4, Safety related parts of control systems

[8] ISO 12100 Safety of machinery – Basic concepts, general princiles for design

[9] ISO 14121 Safety of machinery – Principles of risk assessment

[10] ISO 15998 Earth-moving machinery – Machine-control systems using electronic components – Performance criteria and tests

[11] ISO WD 26262 Part 1-8 Road vehicles – Functional Safety

NEUE BÜCHER

Untersuchung zur Reduzierung des gegenseitigen Besaugens von Kälbern in Gruppenhaltung durch Änderungen im Fressbereich und der Tränkeverfahren

Von Gracia Ude. VDI-MEG Schrift 463. Vertrieb: Johann Heinrich von Thünen-Institut, Institut für Agrartechnologie und Biosystemtechnik, Bundesallee 50, 38116 Braunschweig; 2007, 190 S., 44 Abb., 51 Tab.

Bei mutterlosen Aufzuchtverfahren von Kälbern in Gruppen ist während der Tränkperiode häufig gegenseitiges Besaugen zu beobachten, wodurch Erkrankungen und finanzielle Verluste auftreten können.

Daher erfolgte zunächst die Bewertung der baulich-technischen Änderungen am Tränkestand und die Nutzung des möblierten Nachtränkebereichs im Hinblick auf eine Reduzierung des gegenseitigen Besaugens. Die Kontrollgruppe war in einer Zweiflächenbucht auf Tiefstreu aufgestallt, die optimierte Gruppe hatte einen möblierten Nachtränkebereich, strukturierten Auslauf und eine angereicherte Haltungsumgebung. Der Versuch wurde mit 168 weiblichen Kälbern durchgeführt. Die Kälber haben zwölf Wochen Frischmilch über einen Tränkeautomaten erhalten. An drei Terminen wurden je zwei Abende in Folge Direktbeobachtungen nach der Mahlzeit für 20 Minuten durchgeführt. Je nach Altersgruppe haben 11,2 bis 17,2 % der optimierten Gruppe gegenseitiges Besaugen gezeigt mit einer Dauer zwischen 39,0 und 62,0 Sekunden und 58,6 % bis 74 % der Kontrollgruppe mit durchschnittlich 79 bis 122,5 Sekunden. Mit zunehmendem Alter lag die Aufenthaltsdauer im Nachtränkebereich bei 416 Sekunden. Anschließend wurden Standardaufzuchtverfahren und optimierte Verfahren im Hinblick auf den Einfluss eines unterschiedlichen Angebots an Milchmenge und einer unterschiedlichen Technik bei der Milchaufnahme auf den Blutglukosespiegel untersucht. Die zwölf Varianten wurden mit 120 männlichen und weiblichen Kälbern durchgeführt. Die Kälber haben je nach Variante Frischmilch oder MAT erhalten. Die Datenaufnahme erfolgte mit Direktbeobachtungen im Alter von 39 bis 58 Tagen, und Blutprobennahmen zur Erstellung von Glukoseprofilen im Alter von 50 bis 65 Tagen. Die aufgenommene Milchmenge lag bei der Datenerhebung bei allen Varianten, die restriktiv über den Automaten getränkt wurden, bei 3,0 l pro Kalb und Tag. Die Milchmenge bei den Kuh-Kalb-Gruppen betrug 8,0 bis 8,5 l, bei den ad lib Gruppen 7,4 l bis 9,2 l. Die Dauer der Milchaufnahme lag bei restriktiver Fütterung zwischen 3:50 und 5:25 Minuten, bei den Kuh-Kalb-Gruppen zwischen 10:44 und 11:11 Minuten und bei den ad libitum Gruppen zwischen 14:01 und 15:29 Minuten. Im Zeitraum direkt nach Ende der Milchmahlzeit bis 15 Minuten danach war bei elf Varianten ein Zuwachs der Glukosewerte zwischen 0,650 und 2,060 mmol/l zu verzeichnen mit Werten von 5,670 und 9,160 mmol/l. Der höhere Zuwachs trat bei den Varianten MAT, Nachtränke und der ad libitum Frischmilch auf.

Aus den Ergebnissen ergeben sich drei Lösungsansätze in Abhängigkeit von der Betriebsstruktur: Eine Fixierung im Tränkestand (CalfProtect), ein Nachtränkebereich oder eine Ammenkuhhaltung.