Marcus Martinus and Rüdiger Freimann, Garching

Process safety in farm machinery electronics

In the German Research Society supported project „Process safety in farm machinery electronics" the functional safety of electronically controlled work procedures and automatic concepts with tractor/implement combinations and self-propelled farm machinery was investigated with the aim of creating a concept utilising development steps, methods and tools enabling safety-oriented development of mechatronic systems. The main focus was thereby on methods for system and risk analysis as well as a comprehensive development model for electronic control.

Dipl-Ing. Marcus Martinus and Dipl-Ing. Rüdiger Freimann are scientific assistants at the Chair for Farm Machinery (director: Prof. Dr-Ing. Dr. h.c. K.Th. Renius), TU Munich, Boltzrmannstr. 15, 85148 Garching; e-mail: *martinus@tm.mw.tum.de; freimann@tm.mw.tum.de*. The project work was supported by the German Research Society.

A refereed paper for LANDTECHNIK, the full-length version of which can be accessed under LANDTECHNIK-NET.com

Keywords

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

Literature

Literature details under LT 02321 at http://www.landwirtschaftsverlag.com/landtech/lo cal/tliteratur.htm abrufbar.

Work procedures with tractor/implement combinations and self-propelled machinery feature ever-increasing automation. To ensure system safety program automatics are also making new demands on the development process of the electronics.

An aim of the DFG project „Process safety in farm machinery electronics" is therefore the development of methods for safer automatic procedures in farm machinery on the basis of existing general standards e.g. [1].

A safe procedural system should stop safety-relevant errors occurring or at least identify such a development and react by guiding procedure back into a safe situation or preventing procedure from leaving this condition in the first place („fail-safe") [2]. The secure condition is defined here as the condition of a technical system where, through the protective actions taken, safety risk is acceptably low. Thus, in the conception of a protection function, the actual description of this safety condition must be firmly established.

Development concept for automated work processes

In the initial phase of the project „process safety in farm machinery electronics" a concept for investigation of process safety was suggested [3, 4] and this in the meantime has been compared with relevant standards and extended to a safety-oriented development concept for automated fieldwork procedures.

In the development of a safe system all safety-critical controls must be identified and so conceived that they are able to be monitored and secured through MSR protection systems (measuring/steering/regulating). However, total expense rises in line with the increasing number of protection systems. With the number of possible „false alarms" in the security technology the practicality of the system decreases. A more practical compromise of working safety and operational reliability is therefore necessary. The new concept is characterised through the structure of the work procedure being determined initially through system synthesis. From the total system requirement list is thus produced sub-divisions with subordinate functions. From the safety-relevant functions within the part-system first results for necessary MSR protection systems can be subsequently taken over with a specification document.

System and risk analysis

The aim of this is to enable qualitative risk assessment for the total system and each individually-recognised MSR safety function through systematic procedure. Along with the assessment of risk, appropriate safety-oriented moves can also be determined. In DIN V 19250 [5] and 19251 [6] a systematic method for determination of requirement classes with the aid of a risk graph is described. Security requirements can be, e.g., a failure mode and effects analysis (FMEA) according to [7]. The procedural method with the FMEA agricultural fieldwork is thoroughly described in [3, 4].

System security according to the V model

The development of control instrumentation according to a methodical concept eases the procedure, e.g. according to the established so-called V-model [8]. In *figure 1* a recommendation for a suitable V-model is shown. The procedure takes the left branch of specification on system level over function and module levels to the actual implementation and on the right branch once again back to the tested total realisation. The individual levels are networked with each other through iterative system tests, integration tests and module tests. Additionally, figure 1 shows the representative application possibilities for different methods (MIL, FMEA, RCP, HIL,.....) with which an enclosed tool chain from specific ion through to validation [9] can be achieved.

The system integration with verification and validation concludes the development concept. The executing of component tests, test stand trials and field tests should in such cases prove the safety and practicality of the system. The conceived MSR safety instrument must react correctly to all failures. Tests under as extreme as possible environ-

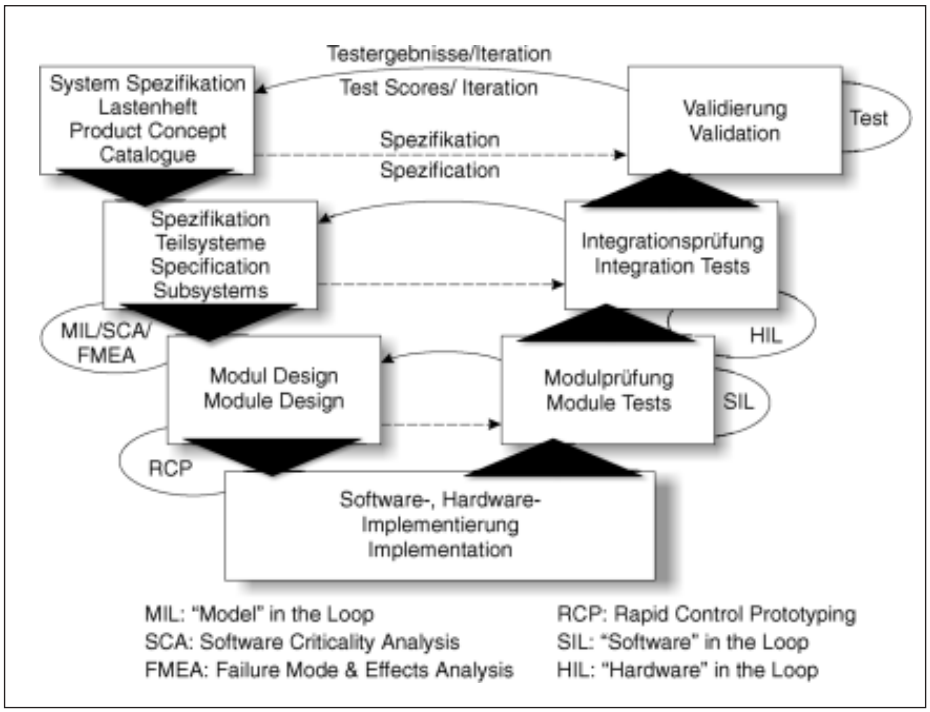

Fig. 1: Adjusted V-Model for development of electronic control units (ECUs)

mental conditions [10] and with regard to electromagnetic resistance (EMV) [11, 12, 13] conclude the validation.

Example of realisation of combination automation

In order to find a system which is as informative as possible in the analysis of procedural safety there should, in the electronic interaction, be several interfaces involved between driver, tractor and implement. Chosen as especially suitable for investigating procedural safety was a drill combination comprising tractor, front packer, power harrow and combi-mounted pneumatic drill. For unrestricted data communication, implement and tractor involved have to be fitted with a CAN-BUS according to ISO 11783 [14]. As application a new type of comprehensive headland management automation was integrated [15, 16]. This concept allows the total procedure from lifting and re-applying the combination to be activated through a single button. This later action determining the virtual insertion or raising point for the combination. The program-controlled mounted implements control therein their interfaces to the tractor (linkage, pto, extra hydraulics) [17, 18] and tractor driving speed in such a precise way that every single unit begins or ends with a work function at the predetermined point.

During passes across the field the central command processing predetermines the seeding rate, maximum driving speed and, as a trial in controlling the work quality of the power harrow, the maximum allowed rpm at the rear pto. These commands are, just as with the headland management not given to the tractor but to the mounted implements. This means that seed drill as well as power harrow can, according to their regulating aims, influence speed of tractor, e.g.

Investigation into safety technology of „implement guided tractor control"

Thoughts on the system synthesis show that individual implement actions on the tractor resources linkage, pto and additional hydraulic spools must occur exclusively for the interface in point. The hierarchy of interfaces and implement must be clear here, and can e.g., occur through interaction with the driver. More critical in the prioritising of momentary regulating action is the speed regulation of the combination. Here, it is possible to have competing implement commands going to the tractor in the case of required tractor speed.

The MSR safety system which is responsible for the prioritising of competing commands on speed was investigated in a risk analysis. For protecting the total system, a system-FMEA was carried out with the tool IQ-FMEA (APIS) which contained a structured procedural method according to VDA 4.2 [7]. With this, further potential failures according to source and effect could be identified and tackled with the help of system-FMEA iteratively integrated into the programming of the tractor computer. To be considered as the result is the hierarchy of commands in combination shown in *figure 2*. The biggest risk is contained in the speed regulating during implement insertion and lifting and during the pass where regulators on the same level can give orders simultaneously to the tractor. Here, prioritisation starts with the smallest value in the first case.

Outlook

Implement combination automation should first be realised in simulation and subsequently with simulated implement commands on the tractor. As next step should be the replacement of the above with real implement commands through ISO implement BUS and thus complete implementation of the function „implement guided tractor control". With field trials the safety actions thus determined should then be tested and recommendations for a „development guideline for safety -associated electronic control in farm machinery" further improved.

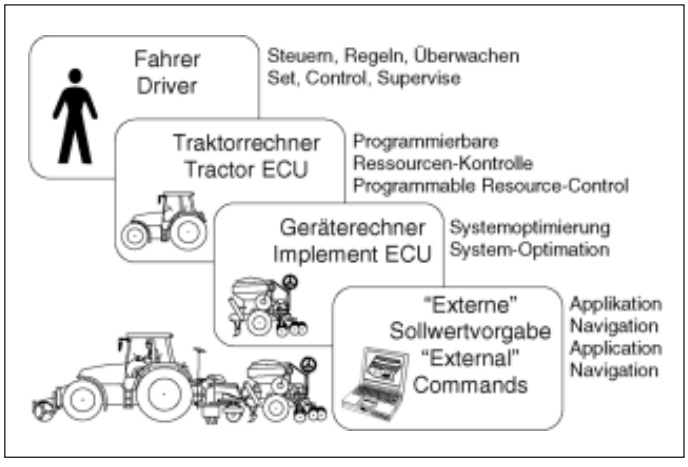

Fig. 2: Control-target-hierarchy of the tractor implement combination