Process Safety Agricultural Machinery Electronics

Implement Guided Tractor Control

Marcus Martinus and **Rüdiger Freimann**
Lehrstuhl für Landmaschinen, Technische Universität München

The project "Process Safety of Agricultural Machinery Electronics" supported by the German Society for the Advancement of Scientific Research (DFG) is intended to study the functional safety of electronically controlled work processes and automated systems in tractor-/implement combinations and self-propelled agricultural machines. The goal is the elaboration of a concept of development steps, methods, and tools which allows for the safety-related development of mechatronic systems. Research focuses on the methods of system- and risk analysis as well as a universal development model for electronic control units, which are described in general and using an example.

Keywords
Functional safety, process safety, automation, electronics, implement-guided tractor control, mobile agricultural machine, FMEA

Introduction

The work processes of tractor-/implement combinations or self-propelled agricultural machines are reaching an increasing degree of automation. If the construction machinery industry and related areas are considered, this development can be noticed in mobile machines in general. In order to guarantee the future operational safety of the systems, the development process of electronics must also meet the new requirements of control units and automated systems.
For the safety-related development of electronic control units, standards which can specially be applied to mobile machines are not currently available except for the draft standard ISO/CD 15998 [1]. As matters stand at present, tractors will also remain exempt from the EC Machinery Directive [2] which stipulates at least general principles regarding the operational safety of machines. Hence, there is no basis which would allow so-called electrical/ electronic/programmable electronic systems (E/E/PES) to be designed and later certified with regard to their functional safety. On 01/01/2002, IEC 61508 "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems" [3] went into effect. Here, a generally applicable development concept is presented which describes the safety-related life cycle (design to validation) of E/E/PE systems. This standard is independent of the system technology used and can hence in principle be applied to all areas of mechatronics. Therefore, it may serve as a basis for the development of application-specific international standards in all areas of application of control systems. For this reason, the DFG project "Process Safety of Agricultural Machinery Electronics" follows the approach of using IEC 61508 as the basis of a safety-related development concept for automated work processes in mobile machines.

Definition of Process Safety

In the DIN V VDE 0801 standard [4], the precursor of IEC 61508, Functional safety has already been defined as the ability of a safety system to perform the actions which are necessary so that the equipment reaches a safe condition or stays in a safe condition. In agricultural machinery and mobile machines in general, however, the equipment does not always consist of a single machine or installation. Instead, it is often a combination of several "intelligent" subsystems, such as a tractor with several front- or rear-mounted implements or a power unit as an energy source with several independent consumers distributed over the entire system.
In order to guarantee work quality, the subsystems are intended to always fulfil their tasks considering the state of the entire system and the other subsystems. Since the operating range of the subsystems often overlaps spatially and since frequently common resources (e.g. the operating hydraulics of the tractor) are used, intercommunication and monitoring also play a main role under the aspect of safety technology.
The functional safety of primary, higher ranking work processes in mobile machines is termed **Process Safety** here. According to **Figure 1**, it is part of the design safety of the system man/machine/environment and stands directly next to immediate and indirect safety technology [5]. Process-monitoring safety functions, which are termed measuring and control protective equipment below, try to guarantee functional safety by coordinating sequences of movements or by making safety-relevant system parameters plausible, for example. Hence, it is the task of a system which meets the requirements of process safety to detect the occurrence of a safety-relevant failure and to transfer the work process to a safe condition while considering all subsystems involved or not to allow it to leave the safe condition. In safety technology, this ability is described as "Fail Safe" behaviour [6].

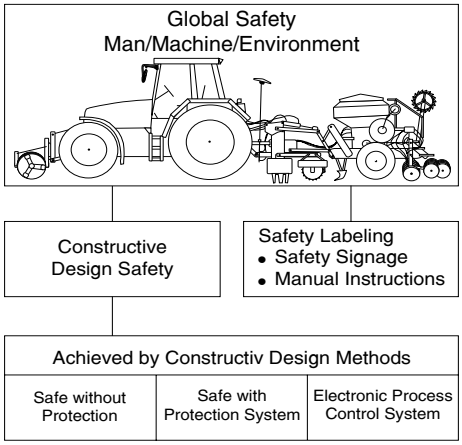

Figure 1: Safety of complex mechatronic agricultural systems using a tractor-/implement combination for winter wheat as an example

According to VDI/VDE 3542 [6], the **safe condition** is defined as the condition of a technical system in which the risk is justifiably low due to the protective measures taken to prevent possible safety-related malfunctions. Before the protective function is designed, the safe condition must be defined concretely. In principle, there are two different ways shown in **Figure 2** to guarantee the safe condition of a system and thus to meet the "fail safe" requirement in the case of a failure [7].

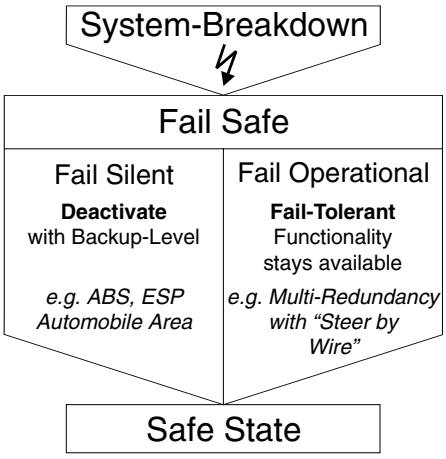

Figure 2: "Fail safe" behaviour (different sources)

The system with "**fail silent**" behaviour is shut down immediately after the detection of a malfunction. In this case, it must be guaranteed that the shutting down of the function does not lead to any critical system conditions. The shutting down of a faulty ABS system in a motor vehicle may serve as an example. When the ABS is shut down, the driver receives a warning signal, but the functionality of the brake remains unimpaired. Systems with "**fail operational**" behaviour, however, must be designed such that they are failure-tolerant. In this case, the system fully maintains its functionality after a malfunction has been detected. Electronic steering systems in motor vehicles ("steer by wire") which feature several channels (redundant design) may serve as examples of such systems [7]. Since a second or n^{th} channel takes over, redundancy enables the system to remain operational even after one channel has broken down.

Development Concept for Automated Work Processes

In order to facilitate the safety-related development of E/E/PE systems and to offer a structured approach, a concept for the examination of process safety was already proposed in the initial phase of the project "Process Safety of Agricultural Machinery Electronics" [5, 8]. Meanwhile, this concept has been conformed to the relevant standards and extended to become a safety-related development concept for automated work processes in mobile machines. **Figure 3** shows the individual development steps from synthesis to system validation. The goal of the concept is, first, to avoid safety-relevant failures and, second, to detect unavoidable failures in time so that the safe condition of the system can be guaranteed ("fail safe"). When developing a safe system, all safety-critical control units must be identified and designed such that they can be monitored and secured by measuring and control protective equipment, if necessary. However, as the number of protective systems increases, the design requirements grow as well. At the same time, the availability of the technical installation diminishes as the number of possible "false alarms" of the safety systems increases. Therefore, a sensible compromise between operational safety and availability is necessary. Below, Figure 3 is used for orientation. The second step, "system and risk analysis", is discussed with particular intensity.

Description of the System Structure in Synthesis

In system synthesis, the structure of the work process is determined. The division into subsystems with lower ranking functions results from the list of requirements to be met by the entire system. The entire system can be shown in the form of a signal flow plan which makes the mutual interfaces of the individual system elements visible [5]. As a result of synthesis, the danger potential of the electronically controlled and automated processes can be determined with regard to the operational safety of the entire system. From the safety-relevant functions of the subsystems, initial results for necessary measuring and control protective equipment can be taken over into the requirements specifications. The following risk analysis pursues the goal of making qualitative risk assessment for each considered measuring and control protective function possible.

Risk Analysis and Risk Graph

After the risk has been evaluated, a decision can be made as to what measures must be taken in order to meet the safety requirements of the protective function. In the precursor standards DIN V 19250 [9] and DIN V 19251 [10], a systematic way of determining requirement levels with the aid of a risk graph is described. The individual measuring and control protective system can be classified using these categories. **Figure 4** shows the risk graph with the resulting requirement levels.

Each measuring and control protective system which has been considered necessary during synthesis is classified using the following risk parameters:

- consequence (C)
- frequency and exposure time (F)
- possibility of avoiding the hazardous event (P)
- probability of the unwanted occurrence (W).

For reasons of clarity and objectivity, it is important that the procedure is applied to each individual protective function and not to complete systems. All measuring and control protective functions of a system must be examined with the aid of this method. Thus, the entire electronic

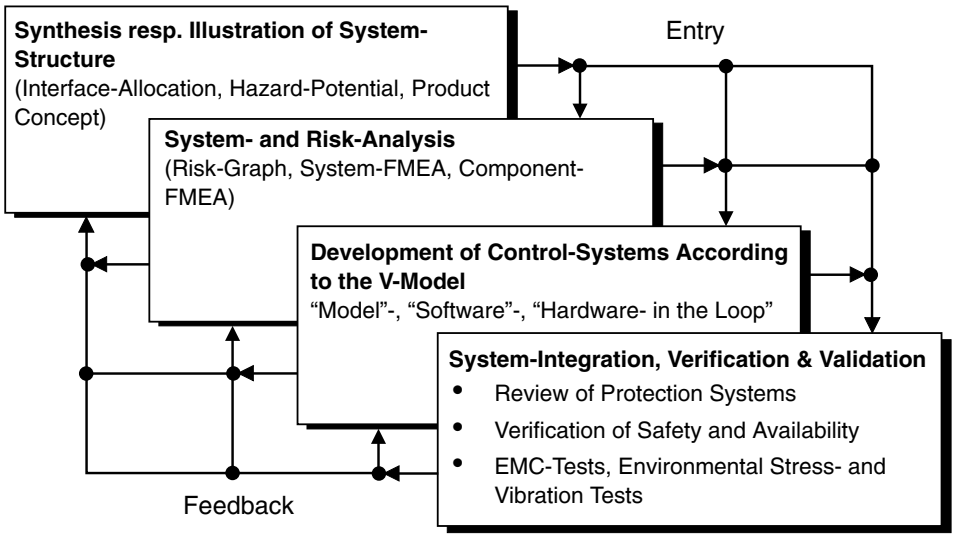

Figure 3: Safety-related development concept for automated work flows in mobile work machines

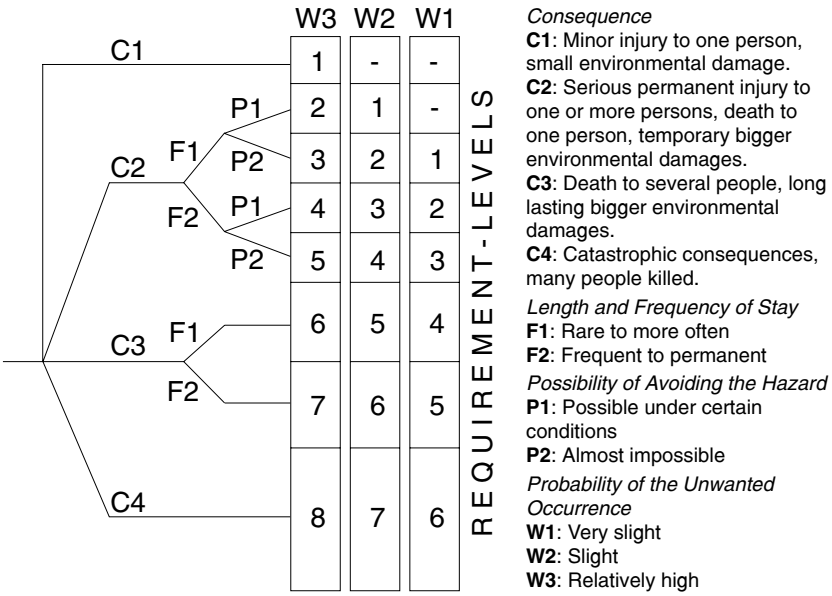

Figure 4: Risk graph for the determination of requirement levels with risk parameters [9]

control system of a self-propelled potato harvester is not examined. Instead, the measuring and control protective equipment which monitors the barrier locking device of the ascent and the descent for the grading personnel is checked, for example.
The parameters C, F, P, and W will be described below.

Consequence (C)
The risk parameter "Consequence C" is considered under different criteria. The kind of object to be protected (persons or the environment) is taken into consideration. As regards the amount of personal damage, a distinction is made according to the criterion of whether one, several, or very many persons (catastrophe) may be affected. Finally, the severity of the injury is considered, which ranges from slight injury to severe injury and death. According to reference [9], this allows the following four degrees to be derived for the parameter C "Consequence":

- C1: slight injury to a person; harmful influences on the environment which do not fall under the Ordinance on Hazardous Incidents, for example [11].
- C2: Severe, irreversible injury to one or several persons or death of a person; temporary significant harmful influences on the environment (cf. Ordinance on Hazardous Incidents).
- C3: Death of several persons; long-lasting, significant harmful influences on the environment (cf. Ordinance on Hazardous Incidents).
- C4: Catastrophic consequences, very many fatalities.

In the risk graph, the determination of the consequence C has the greatest importance. In the first step, it already fixes the range where the resulting requirement level is located. With regard to evaluation, it is stated expressly in the standard that the consequences of an average accident and the usual healing processes are presupposed. In order to guarantee an honest and, as far as possible, objective assessment of the requirement levels, it is important to heed this principle and not to base the evaluation of the consequences on extreme scenarios.
Risk analyses carried out in the areas of mobile machines and motor vehicles have shown that the consequence C3 is virtually never exceeded. Examples of a C3 classification are severe consequences of accidents involving hazardous material transports or buses for passenger transport. The accident of a mobile machine or a motor vehicle can often be classified in category C2 due to the consequences of a typical accident.

Frequency and Exposure Time (F)
Under this parameter, presence in the exposure area is specified with regard to frequency and exposure time using the categories "rare", "rather frequent", and "very often/permanent". This results in the following classification:

- F1: Rare to rather frequent presence in the exposure area.
- F2: Frequent to permanent presence in the exposure area.

In contrast to stationary machinery, the changing environment of the machine must be taken into account when considering work processes with mobile machines. Therefore, two frequencies of exposure to be linked must be assumed:

1. Potential hazard due to the situation "machine in environment". The frequency of the exposure of the machine to potential hazardous situations in the environment is decisive (e.g. a transport ride in city traffic).
2. Potential hazard due to the situation "man in the range of action of the machine". The frequency of persons being exposed to hazards caused by the machine is decisive (e.g. operating personnel on a potato harvester or pedestrians in the street).

A "regular" ride to the field must be considered frequent = F2 even if traffic density in rural areas generally can be expected to be low.

Possibility of Avoiding the Hazardous Event (P)
The possibilities of avoiding hazardous events are also dependent upon different criteria. If a work process is constantly controlled by technically skilled personnel and if the necessary interference with machine control is within the range of "natural" reaction, the failure may be detected in time, and the unwanted occurrence may be avoided. This possibility is not given in processes which are not or not sufficiently controlled. The temporal development of the hazardous condition, no matter if sudden or constantly slow, must be considered in the evaluation as well as the possibility of avoiding the hazard by using potential possibilities of escape or by shutting the system down ("fail silent") if sufficient time is available. Therefore, the risk parameters for the avoidance of hazardous events have been determined as follows:

- P1: Possible under certain conditions.
- P2: Virtually impossible.

Probability of the Unwanted Occurrence (W)
This parameter is used to evaluate the probability of the unwanted occurrence without measuring and control protective equipment being present. Probability is classified into the three categories "very low", "low", and "relatively high":

- W1: Very low probability of the unwanted occurrence means that only very few accidents must be expected.
- W2: Low probability of the unwanted occurrence means that only a few accidents must be expected.
- W3: Relatively high probability of the unwanted occurrence means that accidents must be expected to happen rather frequently.

The condition for the assessment of the parameters W is the consideration of the work process concerned or a comparable process without measuring and control protective equipment being present. If statistical experimental values regarding the probability of occurrence of a failure are not available, stricter evaluation of the situation is recommended if in doubt, especially in the case of this parameter.
In the area of innovative, electronically controlled automated systems in mobile machines, high probabilities of occurrence are therefore frequent. Classification in categories W2 and W3 is predominant.

Work with the Risk Graph

If one follows the chosen path in the risk graph (figure 4) from left to right, there are only three fields where safety-technological measures can be dispensed with if the probability of occurrence is considered. In all other cases, the corresponding requirement level determines the quality of the measuring and control protective equipment. The "risk-parameter path" C2 → F1 → P2 → W2, for example, leads to the requirement level RL 2. If the probability of occurrence is W3, the requirement level is RL3.
Each requirement level results in certain measures which must be taken during the entire safety-related life cycle of the measuring and control protective equipment [3, 4] in order to guarantee the functional safety of the system. The measures or combinations of measures to be taken are classified in failure-avoiding and failure-mastering measures. Failure-avoiding measures reduce the probability of occurrence of the failure during system operation. General rules of quality assurance, the overdimensioning of components, or the avoidance of stress factors may serve as examples of such measures.
Failures occurring during the operation of a system which still worked perfectly at the beginning can only be obviated through failure-mastering measures. The goal of failure-mastering measures is to prevent consequences of a failure on the work process with regard to safety and to reach the safe condition of the entire system ("fail safe") or not to leave it (e.g. plausibility checks or a multiple channel system with a test). In critical cases, it may be necessary to combine individual measures into a package in order to reduce the probability of system failure further. It is important, for example, to combine the two failure-mastering measures "redundancy" and "failure detection and warning signal". Thus it can be prevented that a latent, undiscovered failure of the first channel of a two-channel system results in total system failure after the occurrence of a failure in the second channel.
Risk analysis focuses on the evaluation of a hazardous situation which is caused by the absence or the faulty behaviour of measuring and control protective equipment. As a necessary safeguard, the resulting demands may require a Failure Mode and Effects Analysis (FMEA) according to VDA 4, part 2 [12], for example. With regard to the quality and the availability of the system, the carrying out of FMEA at the system- and, later, the component level is recommended at an early stage of development.

Failure Mode and Effects Analysis (FMEA)

In contrast to risk analysis, FMEA focuses on the failure as the cause of a hazard. This method characterizes potential failure cases according to their reason and consequence and assesses the risk of the failure cases according to probability of occurrence, probability of detection, and significance. The precise mode of procedure of this method has already been described in detail in references [5] and [8]. In order to detect other safety gaps, the entire system and its subsystems are intended to be examined with the aid of a system FMEA using the black box representation of the signal flow plan from system synthesis. As a consequence of the system FMEA, further or improved measuring and control protective equipment could be made mandatory. Depending on the requirement level, it may become necessary to examine the measuring and control protective equipment further at the component level using the aid of a component FMEA.
For a more detailed analysis of safety-critical software modules, so-called "Software Criticality Analysis" (SCA) may be necessary [13, 14]. This is a method similar to the FMEA where the software modules required for the manipulation of safety-relevant functions are determined and the consequences of possible failures in these program parts are shown. Software criticality analysis can use the results of risk analysis directly for the identification and realization of necessary safety-relevant requirements to be met by the software.

System Safeguarding through Development According to the V-Model

The first steps of the safety-related development concept are provided by the system specification for the different electronic control units of the automatic functions. It contains both the functionalities and the safety protection functions (measuring and control protective equipment) of the work process. The development of the control units according to a methodical concept facilitates the further mode of procedure. Meanwhile, the so-called V-model has become firmly established as state of the art in the development processes of modern electronic systems. In this model, the way from the requirement to validation is described at different levels of realization and substantiated through different test possibilities. The V-model was originally a development standard for "IT systems of the German federal government", which is composed of the three modules "procedure model", "method assignment", and "functional tool requirements" [15]. Meanwhile, the procedure model is used in very many areas as a house standard for software development. It is a process model which allows projects according to ISO 9001 to be carried out. This means that it describes the activities and the results which occur during the development of software over the entire life cycle. Method assignment prescribes the methods which should be employed for the execution of the activities and the means which should be used to represent the results. The functional tool requirements determine the functional characteristics of the software tools which are intended to be used when developing software.
If the V-model is used for the development of a concrete control unit, an individual decision can be made about which activities need to be combined with which methods and tools in order to allow for the best possible adaptation to the application case and the relevant requirements of the project [16]. **Figure 5** provides a proposal for such an adapted V-model.
On the left branch, the mode of procedure in the V-model leads from the system level via the functional and modular level further down to detail realizations and on the right branch back to global realization. The individual levels are networked through iterative test possibilities, system tests, integration tests, and module tests. Problems of software integration at the modular level, for example, can place new demands on the corresponding module

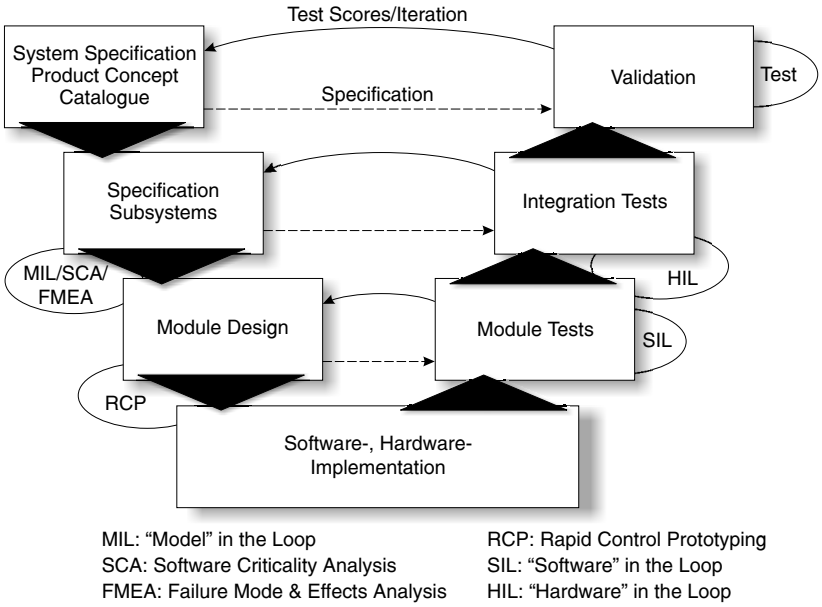

Figure 5: Adapted V-model for the development of electronic control units (ECUs). Explanation of the abbreviations see references [13, 14, 17].

design. Figure 5 shows the individual possibilities of application of different methods (MIL, FMEA, RCP, HIL, …) which allow a closed tool chain from specification through to validation to be obtained [17]. They will be discussed below.

Due to functional specification, the specified requirements of the entire system are distributed over different logistic units (e.g. control systems). The task of the next lower realization level of the modular level is the division of the functions of a control unit into individual modules. For the system to be able to be satisfactorily tested for its function during functional specification and modular design, the representation of the work process with machines, implements, and environmental influences in a mathematically logical simulation is appropriate. In the "**Model in the Loop**" test (MIL), additional control algorithms are integrated into the simulation of the path and can thus be tested at the computer even before programming. In the next step, **Rapid Control Prototyping** (RCP) enables the functionality of individual software modules or entire structures to be tested in real time in the real vehicle or in test installations. For this purpose, the algorithms are isolated from the simulation of the "Model in the Loop" test and implemented on a universal, real-time capable, "high end" control computer. This RCP development tool then serves as a controller in the real system. Common RCP tools enable the control parameters to be altered on-line in the vehicle and thus provide very efficient possibilities of optimisation. In addition to the optimisation of the software control- and program algorithm, this also results in concrete requirements to be met by the target hardware in the series (number of the necessary inputs and outputs, processor capacity, required memory, etc.). Software implementation into the target hardware completes the realization of functional specification by translating the specified functions according to the designed structure into the instructions of a programming language. After software implementation or –integration, the "**Software in the Loop**" test (SIL) is applied. Here, the software model of the MIL test is replaced by a translatable and executable program and integrated into the simulation of the path via an appropriate software interface. The functionality of the C-program can thus be tested at the computer. In integration tests of the control unit (target hardware) and the final testing of the entire system, "**Hardware in the Loop**" tests (HIL) connect the completely programmed control unit with the simulation of the path via a real time interface (HIL environment). The program code can thus be tested on the final target hardware under safe, simulated conditions. The test cases correspond to the risks determined with the aid of FMEA.

With system integration and, later, verification and validation, the development concept for automated work processes is completed. Component tests, test–bench trials, and field tests are intended to prove the safety and the availability of the system. The designed measuring and control protective equipment must react correctly to provoked failures (cf. "fail safe" above).

The testing of the electronic concept of the complete mobile machine should focus on the following points [18]:

- The integrated safety functions must be fulfilled.
- Behaviour in the case of over- and undervoltage, start voltage dips, generator malfunctions, and cable-related malfunctions must be examined.
- The reset behaviour of the systems must be tested.
- Data exchange with other systems must be checked.

In addition, tests should be carried out under the most extreme environmental conditions possible [19]. Since the behaviour of electronic components (e.g. processors, displays, memory modules) is strongly dependent upon extreme temperatures or humidity, system requirements under these conditions must be tested as well.

In the design phase of the work machine or the tractor-/implement combination, certain principles must already be respected with regard to electromagnetic compatibility (EMC) [20] and the suppression of radio interference: on the one hand, the entire system must remain insulated from the irradiation of powerful radio emitters. On the other hand, it may not interfere with stationary radio reception. Within the system limits, the different subsystems, such as control units, adjusting motors, or solenoid valves are often separated by small spatial distances, and generally are supplied by the same electrical system. Therefore, it must be guaranteed that the interactions of the systems do not lead to impermissible malfunctions. After the design phase, there are also different EMC test methods (e.g. stripline method, bulk current injection method) which provide a precise picture of the irradiation resistance of the system to be assessed [21]. Other measuring methods for the characterization of the interfering electromagnetic emission of integrated circuits (ICs) are described in reference [22] and the final draft of the international standard IEC 61967 [23].

Exemplary Realization of the Automation of a Tractor-Implement Combination

For the selection of a suitable tractor-implement combination, an analysis of the work processes on the field was carried out. In order to find the most efficient system possible for the analysis of process safety, several tractor-implement

interfaces for a typical application should be activated in electronic interaction.
Therefore, the basic requirement list for the system to be examined includes:

- tractor-/implement combination with network integration according to ISO 11783 [24]
- practice-relevant work example
- electrical/electronic automation of as many tractor-/implement interfaces as possible
- integration of the driver interfaces (driving- and implement control functions)
- integration of control circuits beyond the system level (tractor-implement communication)
- integration of local (tractor- or implement-internal) control circuits
- integration of "higher ranking control circuits of precision farming" (e.g. application control according to yield maps).

Given these criteria, a cultivation- and sowing combination which consisted of a front packer, a rotary harrow, and a semi-mounted pneumatic drill was chosen as a particularly suitable system for the examination of process safety. The implements and the tractor should be equipped with a BUS (Binary Unit System) for free data communication.
ISO 11783 [24] as the successor system to the German LBS [25] defines four main components in a BUS which connects a tractor and an implement. These components are:

1. Implement ECUs (Electronic Control Units) which are responsible for the actual control of the mounted implements and the tools of agricultural machines.
2. A "virtual terminal" which (without having its own direct function) provides a universal user interface by making screen and operating elements available to all BUS participants (even at the same time!).
3. An internal tractor ECU which makes the information from the output interfaces accessible and gives all BUS participants access to components such as drive, hitches, PTO, electrical system, and hydraulics.
4. A "task controller" which "organizes" and documents work on the field by collecting data and controlling the system and the applications and thus forms the interface with the farm PC.

All interfaces and communication protocols are described and standardized in ISO 11783. The free combinability of tractors and implements from "large" manufacturers with each other and with components and systems from suppliers and smaller manufacturers of special implements is guaranteed.
An internationally supported basis of integral control circuit formation with detailed documentation of tillage, sowing, fertilizing, plant protection, and harvest is technically available. Future machines and implements will increasingly use this linkage beyond their own system boundaries to optimise the entire work process.
By cooperating in the development of the ISO 11783 standard, the Chair of Agricultural Machinery has exerted significant influence on the content of parts 7 [26] and 9 [27]. Especially the "implement-guided tractor control" function was able to be integrated into basic communication. Mounted implements and other services, such as the task controller, can thus directly influence and control tractor functions. Formally, a virtually arbitrary tractor-/implement combination can thus be optimised in the same manner as a specialized self-propelled machine with regard to the harmonization of the work processes.

Automation of Winter Wheat Cultivation

Parallel to the examination of process safety, the chosen tractor-/implement combination was realized as follows with the support of the companies AGCO-Fendt and Lemken: tractor Favorit Vario 716, ring packer (Variopack 110), rotary harrow (Zirkon 7) and drill (Solitär 9) [28]. The network structure corresponds to the structure of ISO 11783 (**figure 6**).
With the realization of the above-described basic requirements, novel, complete automated headland management [29] was integrated into the system at the same time. In this concept, the entire work start and –interruption process of the combination is carried out at one single touch of a button. The only remaining task of the driver is steering. By pressing the button, the virtual work start and -interruption point of the combination are determined. The program-controlled mounted implements then control their interfaces with the tractor (hitches, PTOs, additional hydraulics [30]) and the driving speed of the tractor so precisely that the work function of each individual implement begins and ends at the set point. The set and actual data of the corresponding control circuits are communicated according to ISO 11783 (cf. [31]).
During the row ride, the task controller also determines seed quantity, the maximum driving speed, and – as an attempt of controlling the work result of the rotary harrow – the maximum permissible torque of the rear PTO. This set value as well as that of the headland management are sent to the mounted implements and not to the tractor. Both the drill and the rotary harrow can then influence the driving speed of the tractor, for example, according to their control target.

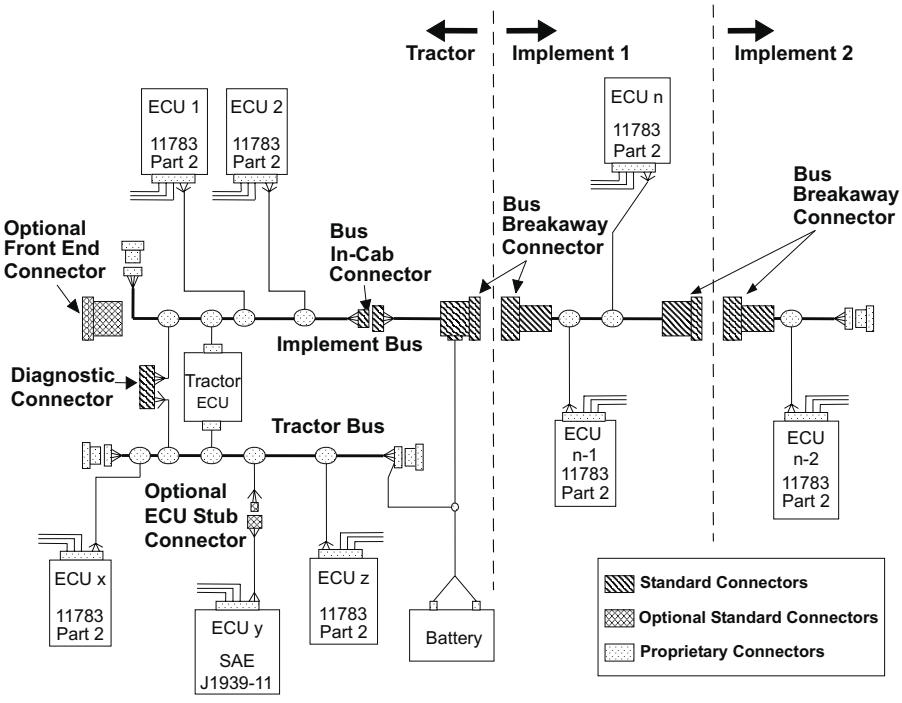

Figure 6: Network layout according to ISO 11783 (including naming) [24]

For CAN communication and control tasks as well as for the integration of additional safety sensors in the mounted implement, control units with 16 bit micro controllers were installed in each implement. The safety sensors must fulfil the following tasks:

- monitoring of endangered/important rotating parts (packer rings, harrow roller, drill blower, …)
- monitoring of the tractor-implement interfaces (3-point hitch, PTO, …)
- monitoring of the safe working and parking condition (position of the parking rest, …)

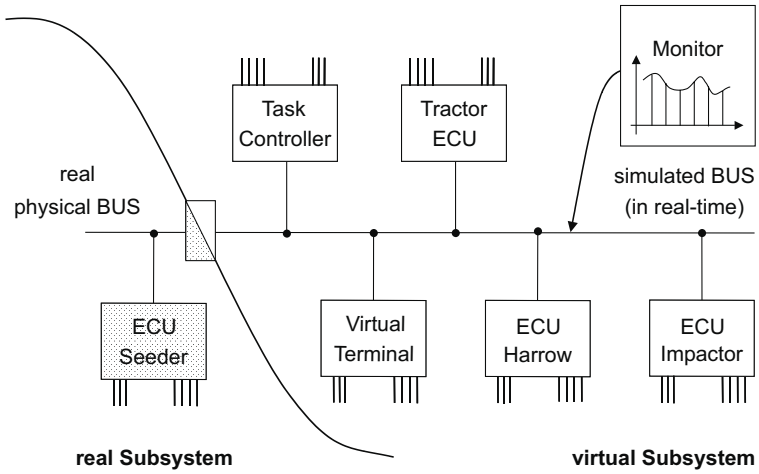

Figure 7: Simulation structure of the tractor-/implement combination with CANoe; combination of a real and a virtual subsystem [31]

Stepwise Realization According to the V-Model

After the definition of function, interfaces, and safety features, the development of program-based automation began. Parallel to the preparation of tractor- and implement equipment, the entire system was simulated with the simulation software Matlab/Simulink from The Mathworks. The model developed here had the task of representing the tractor and the implements in a mathematical reaction model as they are monitored by the control unit. In a second step, this "model in the loop" simulation was extended to comprise CAN communication as a significant component of automation. For this purpose, the software package CANoe from Vector Informatik provides an interface which allows program libraries (DLL) generated from Matlab to be integrated into real CAN communication.

Figure 7 shows the simulation structure of the project with CANoe. In principle, the system can be completely simulated. An integrated monitoring function in the communication process enables it to be observed and analysed (virtual subsystem). The CAN data traffic is modelled in its real time behaviour. With the aid of a hardware interface (in our case a PCMCIA plug-in card for the laptop), communication with one or several real nodes is possible as well (real subsystem).

Both simulation environments – that of communication in CANoe and that of the function and mathematical simulation in Matlab – also enable C-code modules to be integrated. However, this possibility of "software in the loop" simulation was skipped because at that time the hardware of the control unit had already been pre-determined and could be directly integrated into the simulation.

After the complete description of the system, implementation into real hardware was able to be checked directly. It is insignificant whether this hardware has already been installed in the finished implement or whether it only exists as a "board installation" with signal generators for the inlet wiring (hardware in the loop). Hardware development and –testing are thus at least partially independent of the finishing of the complete implement (cf. [32]).

While the controllers for the mounted implements were integrated directly into standard target hardware, the estimation of the required control system equipment (inputs, outputs, processor capacity, and memory requirements) for the tractor ECU was very difficult. The tractor ECU is the central interface for the administration of energy supply for the work process and must hence fulfil important control- and safety functions. For the tractor ECU, the RCP control unit "MicroAutobox" from the dSPACE company was therefore programmed directly based on the simulation with Matlab/Simulink and Stateflow.

The implementation of the hardware has already been completed successfully. In the first step, the integration of ISO 11783 is based on a static communication protocol (without the dynamic claiming of network addresses). The control units of the mounted implements were tested in a simple HIL development environment from the control unit manufacturer using signal generators. During these tests, ISO CAN communication was examined through CANoe simulation. In a further step, the mounted implements were also simulated with the aid of CANoe for the commissioning of the computer in the tractor. During the ride, individual signals and interface instructions can also be manipulated manually using CANoe Interface Panels. This not only allows the reactions of the tractor as a subsystem to be assessed, but it also enables the controller of the mounted implements to be optimised further in simulation.

Safety-Technological Study on "Implement-Guided Tractor Control"

The functional safety of the chosen tractor-/implement combination and its work processes was mainly examined and determined in the first two steps of the development concept, i.e. synthesis and analysis. For cost reasons, it is particularly important to gain an overview of the safety-technological demands of the system and, hence, implicitly the development requirements at the earliest possible time.

In synthesis, the individual implements (ring packer, rotary harrow, drill) and the tractor were shown as black boxes in a signal flow plan and connected through material-, energy-, and information flows [5]. The requirements to be fulfilled by electronic control units and communication structures which are necessary for the execution of the "implement-guided tractor control" functions result from the system structure. Through brainstorming, the hazard potential for man and the environment was estimated in reflection and discussions, and the resulting requirements were taken over into the requirements specification. The access of the individual implements to the tractor resources front- and rear hitch, rear PTO, and additional hydraulic valves must exclusively be limited to the interface considered because generally not more than one implement uses the individual function. Therefore, the implements must be clearly assigned to the interfaces, which can be done through interaction

with the tractor driver. Under safety aspects, the control of the speed of the tractor-/implement combination is more critical with regard to the prioritisation of current controller access to tractor interfaces. When the set speed is determined, competing speed commands from the implements to the tractor are possible. Additionally, the possibility for the driver to interfere must be guaranteed at all times. The hierarchy of the control target generators in the tractor-/implement combination, which is shown in **Figure 8**, must be considered. Speed control during the work start- and interruption process and during row rides involves the greatest risk potential at those points where controllers of the same level, i.e. the mounted implements, can send commands to the tractor at the same time. The measuring and control protective equipment which is responsible for the correct prioritisation of competing speed settings was examined in the following risk analysis.

In order to secure the entire system, a system-FMEA with the tool IQ-FMEA from the APIS company was carried out, which contains the structured procedure according to VDA 4.2 [6]. This allowed the causes and consequences of other potential failures to be identified and the remedial measures from the system-FMEA to be iteratively integrated into the programming of the tractor computer.

For competing speed settings of the mounted implements, the simple concept of prioritising the lowest speed control target and the speed limit value was found. This not only prevents long-term overload situations at the mounted implements (load as a function of throughput/speed), but it also enables a simple fail-safe strategy with speed equals zero to be implemented. Of course, the condition for acceptable availability is robust control circuits in the mounted implements.

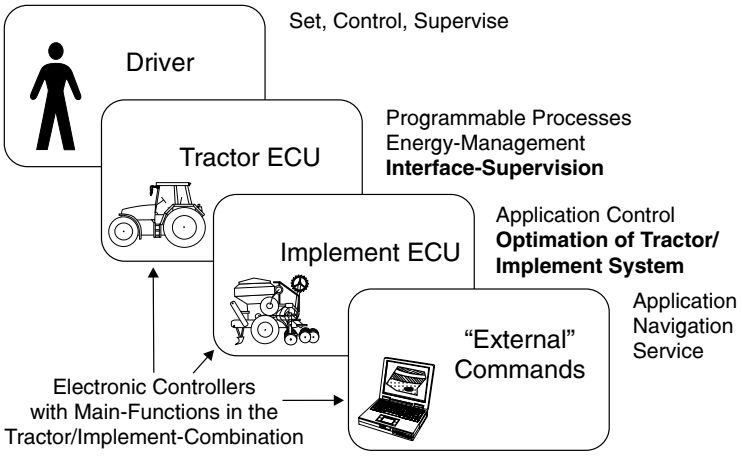

Figure 8: Control target hierarchy of the tractor-/implement combination

Future Prospects

In continuation of the DFG project "Process Security of Agricultural Machinery Electronics", the next planned step is the replacement of the simulated implement settings on the ISO implement BUS by real commands during process automation and, hence, the complete implementation of the "implement-guided tractor control" function for validation in real field use by the autumn of this year. Subsequently, other field trials, which will also include provoked conflict situations, are intended to prove the safety strategies found and, hence, the process security of the system. It will be possible to adapt the methods and tools presented here, such as risk analysis and FMEA, even further to the application case in mobile machines. In further cooperation with authors from the Work Group "Safety/Automation" of the Agricultural Machinery Association in the VDMA, the gained insights are intended to be discussed and evaluated in order to provide generally applicable "Development Guidelines for Safety-Related Electronic Control Systems in Agricultural Machinery".

References

Books are indicated by •.

[1] -,-: Earth-moving machinery – Machine-control systems (MCS) using electronic components - Performance criteria and tests. Normenentwurf ISO/CD 15998, Arbeitsgruppe ISO/TC 127/SC 3, Stand 2000

[2] -,-: Richtlinie 98/37/EG des europäischen Parlamentes und des Rates vom 22. Juni 1998 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten für Maschinen (Maschinenrichtlinie). Brüssel: Kommission der Europäischen Gemeinschaften 2001.

[3] -,-: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/ programmierbarer elektronischer Systeme (E/E/PES). Normenentwurf DIN IEC 65A/254/CDV. Berlin: Beuth Verlag 1998

[4] -,-: Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben. Vornorm DIN V VDE 0801. Berlin: Beuth Verlag 1990

[5] *Martinus, M. und R. Freimann*: Prozeßsicherheit Elektronik bei Traktoren und Landmaschinen. VDI-MEG-Tagung „Landtechnik 1999", Braunschweig 7./8.10.1999. In: VDI-Berichte 1503, S. 99-104. Düsseldorf: VDI-Verlag 1999

[6] -,-: Sicherheitstechnische Begriffe für Automatisierungssysteme - Qualitative Begriffe. Norm VDI/VDE 3542 Blatt 1. Berlin: Beuth Verlag 2000

[7] *Freitag, R. et a*l.: Anforderungen an das Sicherheitskonzept von Lenksystemen mit Steer-by-Wire Funktionalität. VDI-Tagung „Elektronik im Kraftfahrzeug 2001" Baden-Baden 27./28.09.2001. In: VDI-Berichte 1646, S. 837-854, Düsseldorf: VDI-Verlag 2001

[8] *Martinus, M. und R. Freimann*: Prozeßsicherheit automatisierter Abläufe bei Traktoren und Arbeitsmaschinen. Landtechnik 54 (1999) H. 4, S. 222 und 227

[9] -,-: Leittechnik; Grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen. Vornorm DIN V 19250. Berlin: Beuth Verlag 1994

[10] -,-: Leittechnik - MSR-Schutzeinrichtungen - Anforderungen und Maßnahmen zur gesicherten Funktion. Vornorm DIN V 19251. Berlin: Beuth Verlag 1995

[11] -,-: Zwölfte Verordnung zur Durchführung des Bundesimmissionsschutzgesetzes – Störfallverordnung – 12.BImSchV. 26. April 2000, http://eureka.onlinehome.de/extern/giftlager/doc/stoervo.pdf

[12] -,-: Qualitätsmanagement in der Automobilindustrie, Sicherung der Qualität vor Serieneinsatz, Teil 4.2, System-FMEA. Norm VDA 4.2. Frankfurt/M.: Verband der Automobilindustrie e.V. (VDA) 1996

[13] *Peng, W. und D. Wallace*: Software Error Analysis. National Institute of Standards and Technology (NIST), Special Publication 500-209. Gaithersburg 1993

[14] *Beer, A.: X-by-Wire*: Von der Entwicklung zur Einführung. ATZ/MTZ/Automotive Engineering Partners Sonderausgabe März 2001 „Automotive Electronics", S. 80-85

[15] -.-: Das V-Modell - Planung und Durchführung von IT-Vorhaben - Entwicklungsstandard für IT-Systeme des Bundes. http://www.v-modell.iabg.de. München 2001

[16] *Lapp, A. et al.:* Softwareentwicklung für Steuergeräte im Systemverbund - Von der CARTRONIC-Domänenstruktur zum Steuergerätecode. Wie [7], S. 249-276

[17] *Dornseiff, M., M. Stahl, M. Sieger und E. Sax*: Durchgängige Testmethoden für komplexe Steuerungssysteme - Optimierung der Prüftiefe durch effiziente Testprozesse. Wie [7], S. 347-366

[18] *Hietl, H., J. Zehentbauer, H.J. Bierer und R. Fuchs*: Vernetzte Elektronik im Audi A4 - der Produktentstehungsprozess. ATZ/MTZ Sonderausgabe Nov. 2001 „Der neue Audi A4", S. 141-147

[19] -,-: Agricultural Engineering - Testing Resistance for Environmental Conditions for Electrical and Electronical Equipment. Arbeitspapier ISO/WD 15003, Arbeitsgruppe ISO TC 23/SC 19/WG 1, Stand 14.03.2001

[20] -,-: Land- und forstwirtschaftliche Maschinen - Elektromagnetische Verträglichkeit - Prüfverfahren und Bewertungskriterien. Norm DIN EN ISO 14982. Berlin: Beuth Verlag 1998

[21] *Pfaff, W.:* Elektromagnetische Verträglichkeit (EMV) und Funkentstörung. In: Bosch Fachbücher „Autoelektrik Autoelektronik“, 3. Auflage, S.54-69. Braunschweig/Wiesbaden: Vieweg Verlagsgesellschaft 1998

[22] *Klotz, F., T. Müller und A. Graf*: Aussagekräftige EMV Charakterisierung von KfZ-Halbleitern. Wie [7], S. 631-636

[23] -,-: Integrierte Schaltkreise - Messung von elektromagnetischen Aussendungen im Frequenzbereich von 150 kHz bis 1 GHz. Normentwurf DIN EN 61967. Berlin: Beuth Verlag 2000

[24] *Stone, M., K. McKee, W. Formwalt and R. Benneweis*: ISO 11783: An Electronic Communications Protocol for Agricultural Equipment. ASAE Distinguished Lecture Series, Tractor Design No. 23. St. Joseph (USA) 1999

[25] -,-: Landmaschinen und Traktoren. Schnittstellen zur Signalverarbeitung. Norm DIN 9684. Berlin: Beuth Verlag 1997 bis 1999

[26] -,-: Traktoren und Maschinen für die Land- und Forstwirtschaft - Serielles Kontroll- und Kommunikationsnetzwerk - Teil 7: Basisbotschaften. Normentwurf ISO 11783-7. Berlin: Beuth Verlag 2000

[27] -,-: Traktoren und Maschinen für die Land- und Forstwirtschaft - Serielles Kontroll- und Kommunikationsnetzwerk - Teil 9: Steuerelement der Traktorelektronik. Normentwurf ISO 11783-9. Berlin: Beuth Verlag 2000

[28] *Freimann, R. und M. Martinus:* Gerät steuert Traktor: Optimierungsmöglichkeiten der Gespannführung. VDI-MEG-Tagung „Landtechnik 2000“, Braunschweig 10./11.10.2000. In: VDI-Berichte 1544, S. 201-206. Düsseldorf: VDI-Verlag 2000

[29] *Renius, K.Th.:* Entwicklungstendenzen bei Traktor-Geräte-Kombinationen. Vortrag und Diskussion im Arbeitskreis Technik 15.02.2001 Frankfurt/M. VDMA Fachverband Landtechnik 2001

[30] *Schott, W. und H. Coenen*: Übersichten zu Schnittstellen Traktor-Gerät. Interne Studie GKN Walterscheid GmbH 2001

[31] *Freimann, R. und P. Fellmeth*: Prüfung der Kompatibilität von CAN-Netzwerken zur ISO 11783 durch Simulation. VDI-MEG-Tagung „Landtechnik 2001“, Hannover 9./10.11.2001. In: VDI-Berichte 1636, S. 89-94. Düsseldorf: VDI-Verlag 2001

[32] • *Seeger, J.:* Antriebsstrangstrategien eines Traktors bei schwerer Zugarbeit. Diss. TU Braunschweig 2001. Forsch.-Ber. Inst. f. Landmaschinen u. Fluidtechnik TU Braunschweig. Aachen: Shaker Verlag 2001

Acknowledgements

For substantial support and stimulating discussions, we would like to thank the Agricultural Machinery Association in the VDMA and the companies AGCO Fendt, Lemken, and GKN Walterscheid for the generous material help. In particular, thanks are due to the German Society for the Advancement of Scientific Research DFG for the generous financial promotion of this project.

Authors

Dipl.-Ing. Marcus Martinus
Lehrstuhl für Landmaschinen
Technische Universität München
Boltzmannstraße 15
85748 Garching
Tel.: +49/(0)89/289-15906
Fax: +49/(0)89/289-15871
E-mail: martinus@ltm.mw.tum.de

Dipl.-Ing. Rüdiger Freimann
Lehrstuhl für Landmaschinen
Technische Universität München
Boltzmannstraße 15
85748 Garching
Tel.: +49/(0)89/289-15888
Fax: +49/(0)89/289-15871
E-mail: freim@ltm.mw.tum.de