MTT RAPORTTI 6

Safety of autonomous agricultural tractor-implement combinations with ISOBUS capabilities

Ari Ronkainen

MTT

MTT RAPORTTI 6

Safety of autonomous agricultural tractor-implement combinations with ISOBUS capabilities

Master's thesis submitted in partial fulfillment of the requirements for the degree of Master of Science in Technology.

Espoo 18 March 2010

Supervisor Professor Matti Pietola
Instructor Juha Suutarinen PhD (agricultural engineering)

Ari Ronkainen

ISBN: 978-952-487-279-9
ISSN 1798-6419
www-osoite: www.mtt.fi/mttraportti/pdf/mttraportti6.pdf

Kirjoittajat: Ari Ronkainen
Julkaisija ja kustantaja: MTT, 31600 Jokioinen
Julkaisuvuosi: 2010
Kannen kuva: Pasi Suomi

ISOBUS-yhteensopivien maatalous traktori-työkoneyhdistelmien turvallisuus.

Ronkainen, Ari
MTT, Kasvintuotannon tutkimus, Vakolantie 55, 03400 Vihti, ari.ronkainen@mtt.fi

Tiivistelmä

Autonomisten robottien kehitys on edennyt siihen vaiheeseen, että turvallisuus ongelmien ratkaisu on alkanut kiinnostaa valmistajia ja tutkijoita. Laitteen turvallisuus on edellytys laitteen markkinoille pääsylle. Standardi ISO 11783 määrittelee tiedonsiirtoväylän maataloustraktoreiden ja -työkoneiden välille. Standardi määrittelee myös työkoneelle mahdollisuuden ohjata traktoria ja siten mahdollistaa pitkälle automatisoitujen ja autonomisten toimintojen toteutuksen.

Maataloustraktoreiden markkinoille pääsyä säätele Euroopan Unionissa kaksi tärkeää direktiiviä: ns. ”traktori direktiivi” 2003/37/EY ja kone direktiivi 2006/42/EY. Tässä työssä tarkastellaan näiden direktiivien turvallisuusvaatimuksia autonomisten työkoneiden kannalta. Työssä todetaan valtaosan vaatimuksista tulevan konedirektiivistä ja autonomisten työkoneiden valmistamisen ja markkinoille saattamisen olevan näiden direktiivien puitteissa mahdollista.

Ohjausjärjestelmien turvallisuuteen liittyviä standardeja ovat IEC 61508, EN62061 ja EN 13849 ja maatalouskoneille vielä lisäksi ISO/DIS 25119. Työssä tarkastellaan näiden standardien vaatimuksia ja näkemystä turvallisuuteen. Standardeista EN 62061 ja EN 13849 ovat konedirektiivissä tarkoitettuja yhdenmukaistettuja standardeja. Työssä todetaan standardien asettavan teknisten vaatimusten lisäksi myös vaatimuksia kehitysprosessille. Standardit näkevät turvallisuuden ennemminkin prosessina, jossa turvallisuutta rakennetaan järjestelmään sisään, kuin pelkästään teknisinä vaatimuksina.

Työssä tarkastellaan, ISO 11783 standardin määrittelemän, ISOBUS-väylän käyttöä turvakriittisessä viestinnässä. Väylän ominaisuuksia tarkastellaan ohjausjärjestelmien turvallisuuden standardien näkökulmasta ja erityisesti standardin EN 50159-2 näkökulmasta. Väylän todetaan olevan nykyisellään riittämätön korkeaa turvallisuudeneheyttä vaativiin sovelluksiin, mutta muutamilla turvallisuuteen keskittyvillä parannuksilla väylästä saisi riittävän turvallisen. Maatalouskoneiden järjestelmätason sopimattomuudesta johtuvia turvallisuus ongelmia tunnistettiin.
Case-esimerkkinä tassä työssä tarkasteltiin ISOBUS calss 3 yhteensopivan kylvölannoittimen turvallisuutta. Turvallisuutta tarkasteltiin käyttäen ISO 12100 standardin turvallismamisprosessia ja ISO 14121 standardin työkaluja. Havaittujen turvallisuus ongelmien poistamista tarkasteltiin ohjausjärjestelmien turvallisuus standardien näkökulmasta.

Avainsanat:
turvallisuus, kone turvallisuus, toiminnallinen turvallisuus, ISOBUS, maatalous, traktori, ohjausjärjestelmä

Safety of autonomous agricultural tractor-implement combinations with ISOBUS capabilities

Ronkainen, Ari
MTT, Plant Production Research, Vakolantie 55, FI-03400 Vihti, ari.ronkainen@mtt.fi

Abstract

Development of autonomous machinery has advanced to the point where the safety has risen to interest of manufacturers and researchers. Safety is a requirement for machine's access to the market. ISO 11783 standard defines a data transfer bus for data exchange between an agricultural tractor and an implement. Standard also defines a control option where the implement could command the tractor, allowing creation of highly automated and autonomous functions.

The market for agricultural tractors in European Union is controlled by two directives: the so called "tractor directive" 2003/37/EC and "the machine directive" 2006/42/EC. In this study requirements, set by these two directives, for autonomous work machinery are examined. In this study it is found that most requirements are set by the machine directive and it is possible to bring autonomous work machinery to market within the requirements of these directives.

Standards related to the safety of control system are IEC 61508, EN 62061 and EN 13849 and in addition for agricultural machinery ISO/DIS 25119. In this study the requirements and views of these standards are examined. EN 62061 and EN 13849 are harmonized standards meant in the machine directive. It is found in this study that these standards set technical requrements, but in addition to that they also set requirements for design and development process of control systems. These standards keep safety as a process where the safety is built within the system in development phase, rather than a set of technical requirements.

The use of ISOBUS data transfer bus, defined in ISO 11783, in safety-critical communication, is examined in this study. Properties of the bus are examined from the view of safety-related standards of control systems and especially from the view of EN 50159-2 standard. It is found that the ISOBUS is not usable for application requiring high levels of safety integrity. However the bus could be used, if certain safety-related improvements are made. A safety-related problem resulting from the lack of definitions in the system level of agricultural machinery was identified.

In a case-example of this study, safety of ISBUS class 3 compatible seed drill was examined. The safety process described in ISO 12100 standard was used with the help of tools provided in ISO 14121 standard. Removal of identified safety problems was studied from the view of standards related to the safety of control systems.

Keywords:
safety, safety of machinery, functional safety, agriculture, tractor, ISOBUS, control system

Preface

This thesis was done in MTT Agrifood Research Finland's Vihti office known as MTT Vakola. The work on this thesis started in June of 2009 and turned out to be quite exploration to the world of safety engineering. The first task in this thesis was to familiarise my self with the legislation and standards regarding safety and as of now I feel that I have not more than scratched the surface of this subject. The safety is not currently taught as such in our university, which is a shame, because as I have noticed during this thesis work that many aspects of safety are actually same as those good design principles that are taught in our classes, but as safety aspects are not considered at the same time, makes it difficult to connect those good design principles to safety. This makes it more difficult to consider safety aspect later in one's carrier. The safety is no more than rational thinking in the design phase and taking responsibility for one's design work.

This thesis was done for ISOturva project which was funded by the foundation for research of agricultural machines (Maatalouskoneiden tutkimussäätiö) of which big thanks for them.

I would like to thank my supervisor Matti Pietola and my instructor Juha Suutarinen and the whole CropTech team and other employees in MTT Vakola and Timo Oksanen in TKK for their help in this thesis work. In addition would like than all my professors, lecturers and teachers who have not managed to kill my interest for natural sciences. And also thanks to Jarmo Alanen and SFS for the permission to use their pictures.

Vihti 11 March 2010 Ari Ronkainen

Sisällysluettelo

1 Introduction

Service and field robotics and autonomous work machinery have been a hot topic among mobile work machine industry and research for many years. The purpose for research of autonomous robotics is to replace human operators from machinery. Recently there has been a lot of development in the field of navigation, guidance, mapping and control of autonomous machinery. Lately there have been promising cases where a mobile machine has been made autonomous or semi-autonomous, and where problems mentioned above have been solved for these applications. These are cases like Sandvik Automine and automated port equipment by Gotwald. However, these machines work in an isolated environment free of humans in danger zone of the machine. In the field of agricultural machinery, environments are very variable and open, and a human-machine encounter is possible. Here rises the question of machine safety. How do we make sure that a mobile machine operating autonomously is safe to humans around it? Safety of autonomous machinery has quite lately risen into the interest of industry and researchers. Machine safety is quite well covered in traditional machinery, but with autonomous mobile machinery the problem field is completely new and uncharted. The purpose of this study is to map the legal, aspects of machine safety, map the standards and research in the field of machine safety applicable to mobile autonomous machinery and to map some of the problems encountered by the designers of autonomous machinery.

One major problem with autonomous work machinery has been the safety of machinery. Legislation and type approval sets certain safety requirements for machinery, but what are the safety requirements for an autonomous machine without an operator nearby or constantly supervising operation of a machine? The usual case is that technology goes forward and legislation follows behind, but what the current legislation says about autonomous machinery and what can be expected from the legislator in the future when the legislation will catch up with technology? Many manufacturers seem to be very well aware of the safety requirements of their current type of products, as they of course should, but seem to be unaware of the overall legislation and level of requirements. This lack of knowledge prevents many manufacturers, who are interested in developing autonomous work machinery, doing so in an efficient way. Some attempts to develop such machinery have led to machinery that has to be withdrawn from the market because the machine is unsafe /48/ Many research institutions may also be very much unaware of such legislation which might lead them to develop techniques, concepts and test platforms that are difficult to commercialize because they require heavy, expensive or impractical safety systems to be implemented to them.

One purpose of this study is to survey the legislation, mainly so called machine directive (2006/42/EC) and see what it says about the safety requirements. European Union directive 2006/42/EC refers to harmonized standards. These standards are approved by CEN or CENELEC or ETSI and are listed in European Union's gazette (official paper). Following these standards should lead to products that fulfil EU's safety requirements. One purpose of this study is to examine some of these standards and see what they require from or propose for the designers of machines. This study also goes through some other safety related standards which may not be harmonized, but which handle the subjects of safety, agricultural machinery, and guidance- and control systems, which might be of an interest to a developer of autonomous machinery.

In this study we also aim to map some of the safety related problems that designers and developers of autonomous work machinery meet in their work. We want to see whether there are some common types of problems. We survey what kind of solutions, suggestions or requirements there are in standards and in legislation for these problems, if any, and evaluate whether these solutions or requirements are sensible or applicable. We also try to find some kind of rule-of-thumb solutions to problems that might be quite common but are not discussed in common literature.

One major aspect in development of mobile work machinery is data transfer within the machine from system to system and to the outside world from machine to machine controller. Usually a field bus is used in communication within the machine. In agricultural machinery a field bus system of interest is ISOBUS field bus. In ISOBUS Class3 devices attached to the bus are allowed to send commands that command the operations of the power train and steering. This field bus system is to be the backbone of first autonomous mobile work machinery in agriculture. This study discusses some issues of safety of ISOBUS and some other CAN 2.0 based bus systems in safety critical solutions such as X-by-wire. This study discusses also very limitedly about the data transfer between the outside world and the machine, mainly related to remote control of machines.

Safety and reliability go hand in hand, especially in safety related systems safety functions must be performed extremely reliably. Reliability is also required in systems which allow machines to operate safely. In autonomous work machinery these are systems like X-by-wire and obstacle detection. In many cases reliability of safety systems or systems supporting safe operation is a combination of component reliability and software reliability. Software reliability is a result of many factors such as its ability to cope with failures of hardware and other software modules and its ability to perform its intended function. Software which function is to identify a human from laser scanner data is a good example of a system supporting safe operation, where reliability of software is depended from its ability to detect humans and its stability.

Software safety and reliability is a huge subject and field of problems, where a lot of research is being made. In this study we discuss safety of software only lightly, and focus on requirements set for safety related software and for development of such software.

The purpose of the literature review in this study is to act as a small guide to safety of autonomous machinery and their legal requirements for the MTT Agrifood research Finland and its partners.

We also do case studies where we apply results and methods from literature review to practical use. In the case we examine the safety of an ISOBUS3 capable tractor seeding machine combination where the seeding machine has location and guidance capabilities and can control tractors implement hydraulics. We do a safety analysis according to ISO 12100 standard and review the process. The purpose for this is to go through the process and gather knowledge about how it is done and how useful it is. Again, this is supposed to act as a small guide to the process.

2 Literature review and the state of the art

2.1 Legislation

There are two European Parliament's and European Council's directives that are of interest for designer and manufacturer of agricultural machinery. These are the so called "machine directive" (2006/42/EC) and the so called "tractor directive" (2003/37/EC). The Machine directive covers the general safety of machinery and the tractor directive defines the EC type-approval for agricultural vehicles. There are, of course, many other directives that effect the development of machinery, like the separate directives mentioned in the tractor directive, but these two are the main directives that apply to all major agricultural machinery. The others usually cover some specific area of machinery.

The machine directive is implemented in Finland in the statute of the Council of State 12.6.2008/400 and the tractor directive in the statute of the Council of State 356/2005.

There is a third statute of interest; the statute number 403/2008, that governs safety of equipment in use and their inspections. This statute governs safety issues from a view of occupational safety and obliges the employer to provide his employees suitable and safe equipment, and to give instructions on safe use of machinery as well as to supervise the safe use of equipment. This statute is not examined further in this work for it sets the requirements for the employer and not to the manufacturer of machinery. It can also be assumed that machinery in compliance with the machine directive can be assumed safe if operated as intended and maintained as intended.

2.1.1 Machine directive

European parliament's and European Council's directive 2006/42/EC has been implemented in Finland as a statute of the Council of State 12.6.2008/400 by the law itself (ipso jure) "Laki eräiden teknisten laitteiden vaatimuksenmukaisuudesta 26.11.2004/1016" 4th section 2nd paragraph and "Laki kulutustavaroiden ja kuluttajapalvelusten turvallisuudesta 30.1.2004/75" 4th section. This statute is according 2nd paragraph applied to machinery; interchangeable equipment; safety components; lifting accessories; chains, ropes and webbing for lifting; removable mechanical transmission devices; partly completed machinery.

According to the statute's 4th paragraph by machinery is meant:

- an assembly, fitted with or intended to be fitted with a drive system other than directly applied human or animal effort, consisting of linked parts or components, at least one of which moves, and which are joined together for a specific application,

- an assembly referred to in the first indent, missing only the components to connect it on site or to sources of energy and motion,

- an assembly referred to in the first and second indents, ready to be installed and able to function as it stands only if mounted on a means of transport, or installed in a building or a structure,

- assemblies of machinery referred to in the first, second and third indents or partly completed machinery, which, in order to achieve the same end, are arranged and controlled so that they function as an integral whole,
- an assembly of linked parts or components, at least one of which moves and which are joined together, intended for lifting loads and whose only power source is directly applied human effort.

By interchangeable equipment is meant a device which:" after the putting into service of machinery or of a tractor, is assembled with that machinery or tractor by the operator himself in order to change its function or attribute a new function, in so far as this equipment is not a tool"./39/
In paragraph 5 of the section 3 of the statute is stated that this statute is not applied to

- agricultural and forestry tractors for the risks covered by the Directive 2003/37/EC, with the exclusion of machinery mounted on these vehicles,
- motor vehicles and their trailers covered by Council Directive 70/156/EEC of 6 February 1970 on the approximation of the laws of the Member States relating to the type-approval of motor vehicles and their trailers, with the exclusion of machinery mounted on these vehicles.

Basically this states that this statute does not override or conflict with other legislation concerning agricultural tractors, but it also states that all other risks of agricultural tractors are covered by this statute.

This statute is very general and deals with basic and general safety of machinery. It means also that normal EC-type approval process is applied as normal to tractors. This is also for autonomous tractors, because of the definition of tractor in EC directive 2003/37/EC /40/.

Paragraph 8 of the section 3 states that this statute is not applied to machinery specially designed and constructed for research purposes for temporary use in laboratories. 8th paragraph of the 3rd section relieves research purpose machines from obligations of this statute. This makes it possible to do research and development and to test unsafe equipment or equipment that has not been designed for safety. Safety is usually not a concern when new ideas are tested and proofs of concept are created. However this may lead to a lack of knowledge about safety issues in research facilities. Lack of safety might be a dire problem when concepts created in pure research facilities are commercialized.

Section 5 states that manufacturer of machinery or this authorized agent must prior to machines release to market or machines introduction:

1) make sure that the machine fulfills safety- and health requirements form statutes annex I
2) make sure that technical file required in statute's annex VII section A is available
3) make sure that machine is equipped with required information such as instructions
4) make sure that machine is evaluated according to the section 7
5) create declaration of EC-conformity according to annex II section A and make sure that it is supplied with the machine
6) attach CE-marking according to section 9

Manufacturer of machinery or authorized agent of this must have necessary means to make sure that machine fulfils safety- and health requirements form statutes annex I. If machinery is under other legislation and directives concerning CE-marking, also those aspects must be fulfilled.

7th section declares methods for proving compliance.

If a machine is not mentioned in statutes annex IV compliance can be proven using method described in the annex VIII.

If the machine is mentioned in the annex IV and is designed and manufactured according to harmonized standards, which cover the entire product, compliance can be proven by:

- using method described in the annex VIII
- or with EC-type approval method described in annex IX and using method described in the annex VII
- or using method described in the annex X

If the machine is mentioned in the annex IV an is not designed and manufactured accordingly to all relevant harmonized standards or there is no harmonized standards compliance can be proven by:

- EC type approval according to the annex IX and method described in annex VIII
- or by method described in the annex X

Agricultural machinery is not mentioned in the annex IV, except for cardan shafts, but is covered by directive 2003/37/EC which requires EC-type approval.

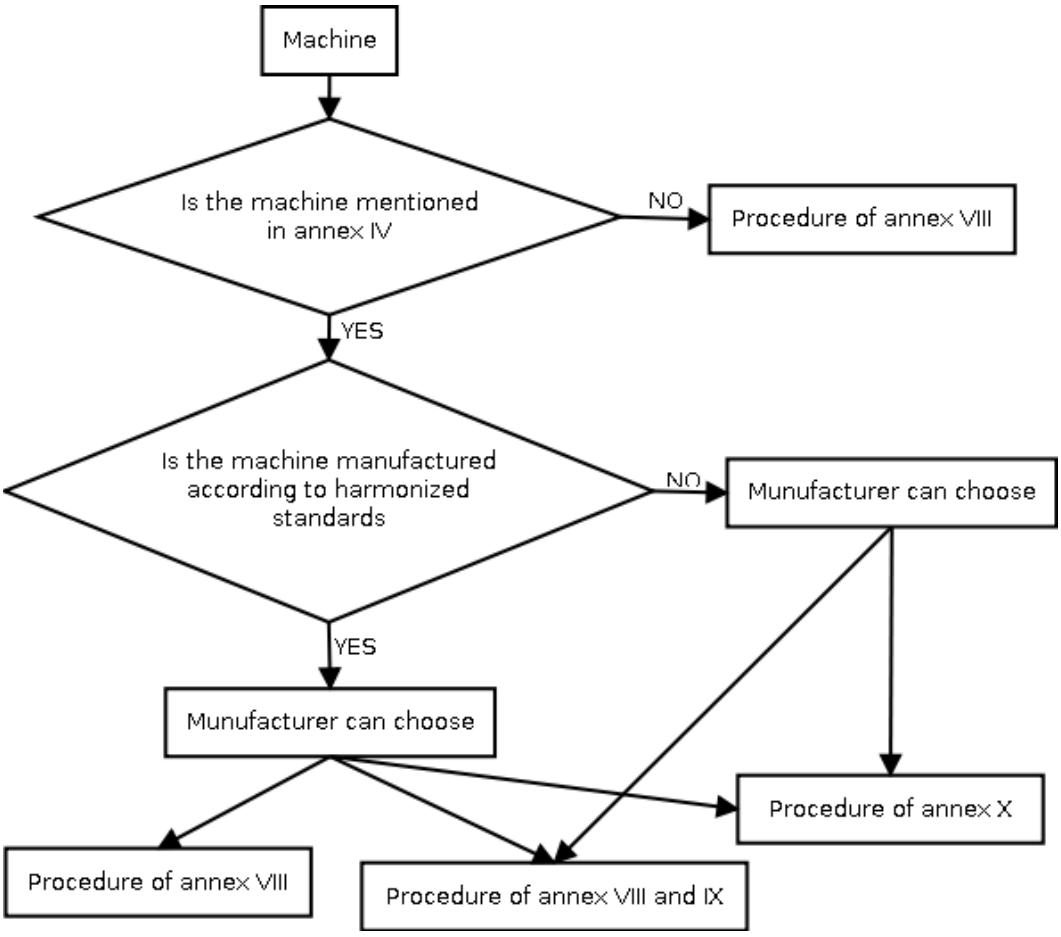


Figure 1 Selection of method for proofing conformity

6th section states, that when using harmonized standards, fulfilling necessary requirements covered by that standard, can be expected.

9th and 10th sections deal with CE-marking. Details and requirements for CE-marking are described in annex III. CE-marking is confirmation form the manufacturer that the machine is made according to legislation.

11th section requires that all information for machine, warnings and instructions must be in Finnish and in Swedish if the machine is to be brought to market in Finland. They can be in only one language if the machine is brought to market in only single language area of Finland, which is not the case in agricultural machinery. Annex I contains more requirements for information, warnings and instructions, which according to 11th section must be complied.

Annex I of this statute contains different requirements for safety of machinery. Its section 1.1.2 contains principles for safety. These principles are the same as in ISO 12100 standard. Annex I is the largest and most detailed part of this statute. In 3rd clause of general principles section of this annex it is stated that all requirements listed in this annex might not be possible to achieve with some machines, so current state of the art is considered and machines must be build as good as the current state of the art is.

Annex II contains requirements for EC declaration of compliance. Annex III contains requirements for CE-marking and annex VII has the requirements for technical file required by 5th section and declaration of EC conformity.

Annexes VIII to X contain methods for proving conformity with this statute. Methods described in annexes IX and X (EC-type approval and complete quality assurance) require involvement of a third party. In this case the third party is notified body such as MTT. These annexes contain also requirements for those audition bodies.

A guide for applying machine directive or EC directive 2006/42/EC was published by European Commission on 9th of December 2009.

The main point of this statute and the directive, that the statute is based on, is that the manufacturer must make a risk assessment for his products, and reduce unnecessary risks. The problem is that the directive requires that the manufacturer also recognizes possible misuse of his product. The directive and statute use the term “reasonably foreseeable misuse”. This term is very vague and whether the manufacturer has taken this reasonably foreseeable misuse into account in his risk assessment process may have to be resolved by the court of law in case of an injurious accident. Under the authority by the law 26.11.2004/1016 itself industrial safety authority can withdraw the product from the market or limit its marketing and for products aimed for consumer market under the authority by the law itself Consumer Office can withdraw unsafe products from the market or Customs Office can ban import of such products. According to EC-directive 2006/42/EC article 11 if a member state finds unsafe machinery it must inform European Commission of its findings. European commission will then hear all parties involved and make a decision whether the actions of the authorities have been correct and inform other member states of its findings. Therefore it is European Commission who has the authority to decide whether the machine has been safe.

The risk assessment and reduction process must be documented accurately, if manufacturer wishes to show that risk reduction has been made adequately. If manufacturer has not taken foreseeable misuse into account in the risk assessment process, has not made risk assessment or it is poorly documented this is always aggravating for the manufacturer. (/36/ annex VII section A clause 3). If the risk

assessment and reduction has been made and documented properly, the manufacturer can claim in a court of law or for European Commission in a case of accident due to misuse, that it was not reasonably foreseeable for the manufacturer.

Other main point is that the manufacturer is responsible for safety of his products. This creates a challenge for agricultural machinery, where different products are used in combination with each other and where function of one machine is dependant from function of another. According to definitions in machine directive 2006/42EC and tractor directive 2003/37/EC tractor and its implements are separate machines and coupling them together does not make them into a machine line where the responsibility is with the party who assembled the line. In regular agricultural machinery the interface between the tractor and its implements is well defined, so manufacturers of tractors know which kinds of implements might be attached to them, and manufacturers of implements know to what kind of machinery their product is attached to. This makes it relatively easy for manufacturer to define their responsibilities roughly to "we are responsible for what our machine does". Traditional agricultural machinery is also well covered by standards. Problems arise with more sophisticated systems like tractors and implements with ISOBUS class III capability, where implements can give certain commands to tractor. With autonomous systems, where both systems might give commands to each others without the operator, who is responsible for dangerous operation of such machine combinations, where the manufacturers of different parts of the system might be different.

In the case of ISOBUS class III equipped machinery the answer for liability question is in my opinion quite clear. Later in this text we discuss ISOBUSS field bus systems in more detail and explain more in detail the properties of the bus. However the implements field bus is connected to tractors electronic control unit (ECU), not directly to tractors internal bus, so tractor's ECU acts as a bridge between the implement and tractor's functions. Now should tractor's ECU contain a safety system that prevents the implement from giving dangerous commands? The answer in my opinion is yes, for it is easily foreseeable that the implement might not function properly. Is the manufacturer of the tractor responsible for dangerous operation due to implement? In my opinion no, for it is the implement which is giving dangerous commands and therefore manufacturer of the implement is responsible for safe operation of ones products. The manufacturer of the implement can not rely on tractor's ECU's safety functions. It is foreseeable that implement might give dangerous commands, but it is not foreseeable what those commands are. And also, it can be held foreseeable that tractors safety functions don't work properly.

IEC 61508 and EN 26061 standards also state that one can not trust components of another without analysing compatibility and functionality with ones own system. So it could be stated that this kind of a machine is also responsible for the commands it sends, however proving who sent and what in a court of law might be a whole different case. But, of course, the manufacturer of the tractor should try to build a safety system that would prevent dangerous operation due to implement.

In ISO/DIS 10975 draft standard for safety requirements for auto-guidance systems of agricultural machinery it is stated that tractor must return under operator control when primary steering devices are manipulated/41/. For this function the responsible party is the manufacturer of the tractor for it is clearly function of tractors ECU to perform this function, but also auto-guidance systems' ECU should react to it. In the same draft standard it is stated that the auto-guidance shall be disabled when signals used for steering such as satellite GPS signal and/or crop feeder data is lost. For this function the party

responsible is the one which has implemented the auto-guidance system, for this is clearly function of auto-guidance's ECU. Note that the auto-guidance system might have been made by a third party, but integrated by some other. The reader must be aware that these are opinions of the writer and these examples are not tested in a court of law, which is the only authority to say who was responsible and for what with certainty.

Machine directive's requirements for control systems

In EC directive 2006/42/EC annex I clause 1.2 there are clear requirements for control systems of machinery. Requirements are in a clear list that could be used as a check list when designing control systems. Clause 1.2 is presented here in annex III as it is in original English language version of the directive.

To summarize the main points of this part: Unexpected start of machine or unexpected transition to un-safe mode is not to be allowed, and starting and moving to un-safe state is possible only when it is safe to do so. Controlling devices must be easily operate-able and understandable. The machine must be stoppable and once stopping command is given it can not be overridden and stopped state is to be maintained and supervised. Emergency stop is not a safety feature but rather a supporting function. Emergency stop must stay on and releasing emergency stop shall not lead to starting of machine. Only one command mode is allowed at a time. Irregularities at the power supply shall not cause danger.

For manufacturer of agricultural machinery clause 1.2.4.4 is of interest for it sets requirements for assembled machinery. It states that if machines are designed to work together then stopping of one machine must lead to stopping of other machine if continued operation will lead to a dangerous situation.

2.1.2 Tractor directive

European parliament's and council's directive 2003/37/EC on type-approval of agricultural or forestry tractors, their trailers and interchangeable towed machinery, together with their systems, component and separate technical units is usually referred as the tractor directive. This directive lays out the procedure and requirements for EC type-approval for these vehicles built in one or more stages. Vehicles maximum design speed must be more than 6 km/h for this directive to apply.

The directive defines a vehicle as: "any tractor, trailer or interchangeable towed machinery, whether complete, incomplete or completed, which is intended to be used in agriculture or forestry" and tractor as "any motorised, wheeled or tracked agricultural or forestry tractor having at least two axles and a maximum design speed of not less than 6 km/h, the main function of which lies in its tractive power and which has been especially designed to pull, push, carry and actuate certain interchangeable equipment designed to perform agricultural or forestry work, or to tow agricultural or forestry trailers; it may be adapted to carry a load in the context of agricultural or forestry work and/or may be equipped with passenger seats." This definition is important for a builder of autonomous or automated agricultural robots or tractors as even autonomous tractors are to be evaluated according to this directive if its design speed is over 6 km/h. The definition of the tractor does not say anything of the need or the location of the operator. This directive is also applied to implements attached to tractors if the implements if the implement is towable i.e. does touch the ground during transport.

This directive does not apply to skidders or forwarders defined in ISO 6814:2000 standard, forestry machinery based on earth mowing machinery's chassis defined in ISO 6165:2001 standard or to interchangeable machinery that is fully raised from the ground during transport.

Articles 1 and 2 define the scope of this directive and give definitions used in this directive.

Article 3 defines the application process for EC type-approval and article 4 defines the approval process. 2nd clause of the fourth article states that if a member state finds a vehicle, component, system or a separate technical unit that fulfils the requirements of type-approval but poses a serious risk to road, environmental or occupational safety it may refuse the EC type-approval.

Article 5 covers amendments to EC type-approvals. Article 6 defines the certificate of conformity and EC type-approval mark and their use. Article 7 covers machinery's registration, sale and entry into service. It states that each member state must register and allow any machinery with valid EC type-approval certificate of compliance to be sold and allow incomplete vehicles to be sold, but may refuse their registration before they are completed. Each member state must also allow sale or entry into service of any components, systems or technical units if these comply with corresponding separate directives and requirements of third clause of article 6.

Article 8 defines exemptions for this directive. It states that requirements of article 7 clause 1 shall not apply to vehicles intended for use in armed forces, civil protection, fire-fighting or public order services or vehicles type-approved according to the second clause of this article. The second article states that each member state may, if requested by the manufacturer, exempt vehicles referred in articles 9, 10 and 11 from one or more provisions of one or more separate directives.

Vehicles referred in article 9 are vehicles produced in small series. The number of vehicles allowed to be manufactured and put to use per year is set in annex V section A. Each member state can allow or refuse the sale of these vehicles in their territory or limit the number of vehicles allowed for sale in their territory.

Vehicles referred in article 10 are the end-of-series vehicles. These are vehicles whose type-approval expires before their date of sale. Each member state can allow, form a request of a manufacturer, allow sale of these vehicles on special conditions set in this article and in annex V clause B of this directive.

Vehicles, systems, components or separate technical units referred to in article 11 are units that are incompatible with this directive, due to the techniques or principles that they use and are incompatible with the separate directives. The separate directives are directives that cover the technical requirements of some certain part, component or system, used in vehicles or their sub-parts. These separate directives are listed in this directive's annex II. These directives cover areas like windshield vipers, driver seats and noise levels. The manufacturer must provide information why the used techniques or principles are not compatible with the separate directives and a description of the possible safety, environmental and occupational safety issues raised. The manufacturer must also present description of the tests carried out, and their results to guarantee that the level of safety is at least equivalent to the level presented in separate directives. The European Commission will then present the assisting committee referred to in directive's article 20a draft decision and in accordance with the procedure defined also in the 20th article the Commission will decide whether to grant the EC type-approval. If the request is approved

the member state may grant an EC type-approval under this directive. When the separate directives are changed to cover the technical progress, EC type-approvals are to be changed to type-approvals that comply with this directive. The type-approval granted under this article may have restrictions in their validity; however the validity shall be no less than 36 months.

This is an important article together with article 8. These mean that machinery using novel techniques can be manufactured and brought to market as long as the level of safety achieved with novel techniques is at least at the same level as with existing technology.

The article 13 requires that necessary arrangements must be made in manufacture to guarantee that produced machinery is in compliance with the type-approval. Methods for this and for verification are given in annex IV. Article 16 states that when a member state that granted EC type-approval finds a vehicle that does not comply with the approved type within the tolerances set in separate directives or with in deviations authorised by article 5, it must take action to ensure that requirements of the type approval are met. If another member state finds non complying vehicle, it shall according to article 17 inform the authority of the member state, which granted type-approval to audit this vehicle.

According to article 21 each member state must name the authorities who can grant the EC type-approval and their fields of responsibility and the testing methods they may perform. These bodies must comply with to the harmonised standard EN-ISO/IEC 17025:2000.

The tractor directive covers more traditional areas of safety and performance of tractors or vehicles. It covers areas such as brakes, noise levels, coupling devices, power-take-off and register plates. These are, of course, matters that manufacturer of autonomous machinery must take into account and fulfil their requirements, but this directive says nothing about the control systems of the vehicles. So the main source of requirements set by the legislator for manufacturer of autonomous agricultural machinery regarding those autonomous functions come from the machine directive, as it is stated in machine directive that it will be applied to all risks not covered by the tractor directive. If autonomous or highly automated machinery will appear in the market, the directive should change to meet these machines and the also this directive would become more of an importance when developing control systems for autonomous or highly automated agricultural vehicles.

2.2 Applicable standards

Harmonized standards are standards approved by CEN, CENELEC or ETSI and are noted in European Union's gazette. /39/ /36/ New standards published by European standardisation associations have annex Z, where it is stated which directives the standard is aimed to fulfil at the moment of publication of the standard, and which European Union's directives can be expected to be fulfilled if the standard is followed. Notes in annex Z do not mean that the standard is harmonized. Only listing EU's gazette means unification. /15/

Use of harmonized standards is not required to fulfil EU directives. However, many EN standards are prepared having unification in mind, which has led into problems in making EN standards accepted internationally and has politicised preparation and acceptance process in Europe. This development is heavily criticized by Viljanen. /15/

Safety-related standards are divided into three hierarchical categories. Type-A standards are basic standards that give basic principles, concepts and aspects. These standards can be applied to any product or process. These standards also define guidelines for type-B and –C standards. If B- or C-type standards have differences then type–C is obeyed. /1/

Type-B standards are generic standards that deal with one safety aspect or one field of systems. These standards can be applied to a wide range of machinery. These standards can for example handle safety aspects of control systems or safety components.

Type-C standard are machine (specific) standards. These standards deal with safety aspects of particular machines or specific group of machines. These standards go in great detail in requirements for designs and have specific views on typical safety issues in field of question. If type-C standard deviates from type-B standard type-C standard takes precedence/1/ .

Following harmonized type-A or –B standards does not guarantee that all requirements set by the legislator are met, following harmonized type-C standard usually does. Case where following type-C standard would lead to product not suitable for market, would be where processes described in standards are not executed properly, or the product would have features that are not cowered by the standard.

There are several standards that could and should be considered when designing automated equipment. The first and most important is ISO 12100 that governs the whole area of safety of machinery. ISO 14121 is an important tool standard when using ISO 12100, as it contains methods for identifying and estimating risk. IEC 61508, EN 62061 and EN 13849 are usable for design of control systems. In addition there are loads of standards for data communications. In this work we focus on ISO 11783, which specifies serial communications network for agricultural machinery. Others worth mentioning are EN 50519 and massive IEC 60870. There are also interesting standard for specific safety-related functions such as prevention of unexpected start-up ISO 14118 and SFS-EN 1037, emergency stop ISO 13850, protective equipment to detect the presence of persons IEC/TS 62046:2008 and electro sensitive protective equipment IEC 61496 (also EN 61496). Some of these are presented later in this text.

Selecting between suitable standards, especially for design of safety-related parts of control systems, can be a tricky task, as there are three applicable standards and for agricultural machinery four, if ISO 25119 is passed. All these standards cover the same area, but have slightly different approaches. Some have more general scopes and are more laborious than others, but cover wider field of applications. Many standards that cover safety-related systems have some view on the development process, as in many standards the safety is built in the system during the development process. Selecting the one that has the most similar view on the process than the one's trying to implement the standard, would be quite wise choice. Also selecting a standard that has suitable scope is important. The one with widest scope the IEC 61508 might also be the most laborious to use, but can it can be used on almost any application.

2.2.1 ISO-12100 Safety of machinery - Basic concepts, general principles for esign

SFS-EN ISO 12100 is the top standard in safety of machinery. It is a type-A standard and a harmonized standard. This standard lays out principles of safe design, and describes a risk assessment method that is to be used to determine whether the machine can be released to market. SFS-EN ISO 12100 replaces EN 292 which also handled safety of machinery. It also introduces concept of inherently safe design. The standard lists many

requirements from counsel of state's statute 12.6.2008/400 annex one or European commission's directive 2006/42/EC annex one and requirements and instructions for machine's instruction manual and marking of residual risks. It could be said that ISO 12100 is counsel of state's statute 12.6.2008/400 annex one or European commission's directive 2006/42/EC annex one translated into engineering language.

ISO 12100 approaches safety trough design process. ISO 12100 sees development of safe equipment as an iterative process, where process begins by defining limits of the machine (concept phase in V model of product development) then doing hazard identification. From identified hazards risk estimation and evaluation is made. Then a decision is made whether there is a need for risk reduction. If yes, then a three-step-method for risk reduction is made. Then hazards and risks are re-analysed to see whether the risks are reduced enough and whether new hazards have appeared. This process is repeated until risks are at an acceptable level. If risk can not be reduced enough the limits of the machine must be changed i.e. new concept is needed. This process can be applied to whole machine, or to a part of it, depending on the need and phase of the development process. This process should be documented well in order to prove conformity with this standard. This documentation could be used in a technical file for the machine, which is required by the legislation, for documentation of required safety analysis. As a personal recommendation I would apply this process at least in the concept phase of product development process and again later when the machine architecture is laid out and thus we have a better understanding of the limits of the machine.

ISO 12100 presents a three step process to reduce risk. The first step is inherently safe design. By this ISO 12100 means that once hazards are identified the source of that hazard should be removed thus eliminating the risk by that hazard. For example if there is a risk of explosion due to sparks from an electric motor then why not replace it with pneumatic one or remove it from sensitive area or remove the substance that could explode. This example was quite classical and involved mainly actions done for hardware, but this approach is similarly applicable for software, processes and organisational behaviour. In many cases inherently safe design is the only way to reduce risk because the following two means may not be applicable, especially in software related issues.

The second step is safeguarding. It means reducing risks by introducing complementary protective measures. ISO 12100 tries to avoid using words "safe-" or "safety-" for it may give false image of safety. It uses words like "protective" instead. Use of words like "safety" gives indeed a false image of safety, for if the machine would be truly safe it would need no safeguards or "safety equipment" at all. Word "safeguard" is used because it is generally used. In this step the risk is reduced by external methods which should be used only if hazards can not be removed through safe design.

Third and last step is reduction of risk by information for use. This means instructions for use, warning signs, organisational instructions, training of operators and so on. This is the least favourable way for risk reduction for it does not guarantee any risk reduction at all. Instructions and warnings can be ignored by the user quite easily.

By residual risk ISO 12100 means risk that is left after all methods stated above are used. This is the risk that can not be removed. According to ISO 12100 all risks can not be eliminated. If residual risk is assessed to be small enough to be acceptable, risk reduction process can be stopped and machine released to the market. The machine directive demands that manufacturer of the machine informs the user for residual risks. ISO 12100

separates the residual risk after protective measures taken by the designer and the residual risk after all protective measures have been implemented.

What is acceptable risk is much left under qualitative and subjective estimation of the designer. In section 3.17 of the SFS-EN ISO 12100-1:2003 the standard states:

“Adequate risk reduction

risk reduction at least in accordance with the legal requirements under consideration of the current state of the art

NOTE: Criteria for determining when adequate risk reduction is achieved are given in 5.5”

So, the level of adequate risk reduction depends on the social-legal environment where the machine is designed in and for and from level of technology.

For hazard identification and risk assessment ISO 12100 states that all phases of product life cycle must be covered and all possible states of machine must be covered whether the machine is functioning normally or in faulty state. Also unintended behaviour of the operator or foreseeable misuse of the machine must be covered. ISO 12100 does not give instructions on how such analysis should be made. It refers to ISO 14121 standard for this assessment, but the reference is not normative. This means that also some other adequate method for risk assessment can be used and still be in conformity with ISO 12100 standard. In fact, ISO 12100 has no normative references for it was designed to be the top standard for safety to which all other standards may refer to.

2.2.2 SFS-IEC 61508 Functional safety of electrical/electronic/ programmable electronic safety-related systems.

SFS-IEC 61508 is titled “Functional safety of electrical/electronic/programmable electronic safety-related systems”. Functional safety is safety that is acquired through functions or actions. A thermostat is an example of device of functional safety where thermal insulation is not, though they both are components of safety. Aberration E/E/PE is used here and in standard for electrical/electronic/programmable electronic and SRS for safety-related system. The standard is applicable when one or more E/E/PE SRS is implemented to machine. It is not suited if there is only one E/E/PE SRS in machine and this SRS is very simple and it’s required safety integrity level is less than one.

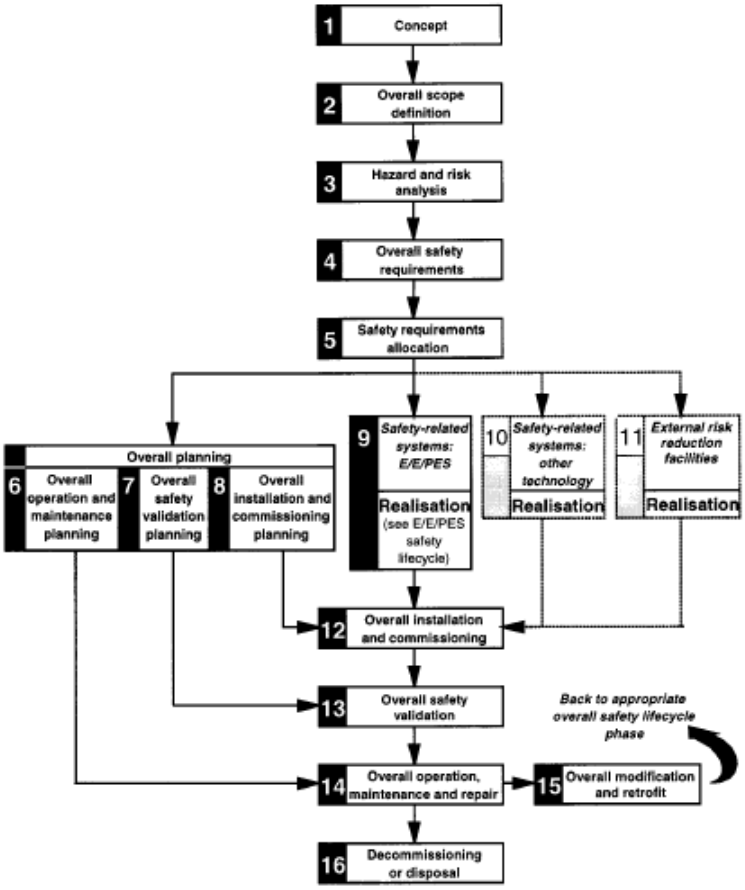
SFS-IEC 61508 is general top-level standard. It has heavy emphasis on safety as a part of development process. SFS-IEC 61508 requires organised and well documented management planning and validation of E/E/PE SRS. IEC 61508 is not a harmonized standard.

The standard has seven parts. Fist part contains general requirements; second and third parts provide additional and more specific requirements for E/E/PE SRS for hardware (part2) and software (part3). Fourth part contains aberrations and definitions, fifth part contains guidelines for applying part one, sixth part gives guidelines for applying parts two and three and seventh gives an overview of techniques and measures.

The first part gives requirements for documentation made during the development process; what documentation should contain and how it should de organised and archived. Good documentation is required to prove conformity with this standard. The first part also sets requirements for management of functional safety. It requires that persons and organisations responsible for certain aspects of SRS are identified and that their responsibilities are defined. These actors must then take necessary actions to acquire

required functional safety and define required strategies, procedures and methods for development, analysis, management, decision making, documentation and for communication.

To manage complex systems SFS-IEC 61508 introduces overall safety lifecycle, which is illustrated in Figure 2. In this presentation lifecycle of product and E/E/PE SRS is divided into smaller more easily manageable parts that go hand in hand with product's normal lifecycle. So basically SFS-IEC61508 just makes safety a part of product's normal development process, assuming that this development is made, with sufficient organisation and documentation.



NOTE 1 Activities relating to **verification, management of functional safety** and **functional safety assessment** are not shown for reasons of clarity but are relevent to all overall, E/E/PES and software safety lifecycle phases.

NOTE 2 The phases represented by boxes 10 and 11 are outside the scope of this standard.

NOTE 3 IEC 61508-2 and IEC 61508-3 deal with box 9 (realisation) but they also deal, where relevant, with the programmable electronic (hardware and software) aspects of boxes 13, 14 and 15.

Figure 2 Overall safety lifecycle

Figure 2 Overall safety lifecycle according to IEC 61508 /3/

Overall safety lifecycle begins with the concept phase. In this phase it is necessary to acquire sufficient knowledge of machines environment (physical, legal, social, etc.) to fulfil the needs for development of E/E/PE SRS. Aberration EUC is used here and in the standard for equipment under control, which is the machine where the E/E/PE control system is to be implemented.

In overall scope definition phase the boundary between EUC and its control system is to be defined and the scope of hazard and risk analysis is to be specified.

In hazard and risk analysis phase a hazard and risk analysis is to be carried out to all states and functions of EUC and its control system in all operation conditions even including misuse. Chains of events leading to these hazardous situations need to be determined. It might be necessary to repeat this phase later in the process.

In overall safety requirements phase, specification for overall safety in terms of safety functions requirements and safety integrity requirements is determined. This includes requirements for E/E/PE SRS; SRS based on other technology, inherently safe design and external risk reduction means. These requirements must guarantee sufficient risk reduction for all risks identified in previous phase.

In safety requirements allocation phase each safety function and requirement defined in previous phase are allocated to specified E/E/PE SRS or SRS based on other technology or external safety reduction system/facility and to allocate safety integrity level to each safety function. Allocation process might be iterative process if it is noted that designated SRS does not fulfil its requirements. In my opinion this is very important phase in development, for it gives clarity what should be done and by which system. Good documentation of this phase makes it possible to find out how the system works later when for example modifications are planned. This phase also clarifies the design process of E/E/PE:s.

After allocation phase design process splits to several planning and realisation phases that can be done simultaneously. Overall planning includes planning of operation and maintenance, planning of overall safety validation and planning of overall installation and decommissioning for E/E/PE SRS. At the same time realisation of E/E/PE SRS and other SRS' can be made. SRS based on other technology than E/E/PE and external risk reduction are outside the scope of this standard, but the standard states that in this phase it must be made sure that these systems fulfil requirements set to them.

At the same time with planning and realisation phase, system and component level design of machinery goes on if E/E/PE is to be designed to new machinery.

Realisation phase of E/E/PE SRS is illustrated in Figure 3. Realisation phase of E/E/PE SRS is divided to realisation of hardware and realisation of software. Realisation begins by defining requirements for SRS and after that defining safety function and safety integrity level for SRS. After specification design and development of SRS can begin and simultaneously SRS validation plan can be made. After design and planning integration of SRS can be made and simultaneously maintenance and operation procedures can be created. After integration of SRS a validation of system is to be made according to validation plan created earlier. Standard's parts two and three give more accurate requirements for E/E/PE SRS.

After realisation and planning phase comes overall installation and commissioning phase. Installation and commissioning is to be made according to installation and commissioning plan created earlier. This is to guarantee that E/E/PE is installed correctly so that its capability to function as intended is not compromised because of installation or compatibility errors.

After installation and commissioning overall safety validation is made according to validation plan created earlier.

The purpose of operation maintenance and repair phase is to ensure safety of E/E/PE SRS and EUC. Operation and maintenance is to be made according to operation and maintenance plan. The plan can be modified should there be the need for it but it must be documented and made according to procedures defined.

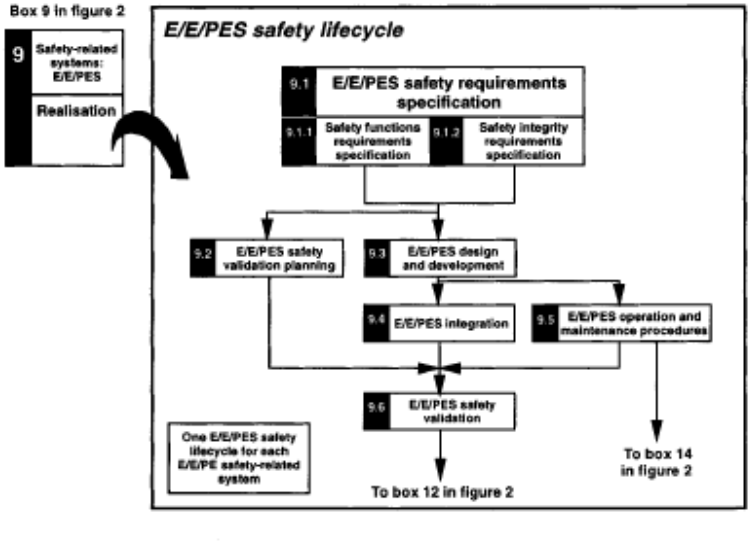


Figure 3 E/E/PES safety lifecycle (in realisation phase)

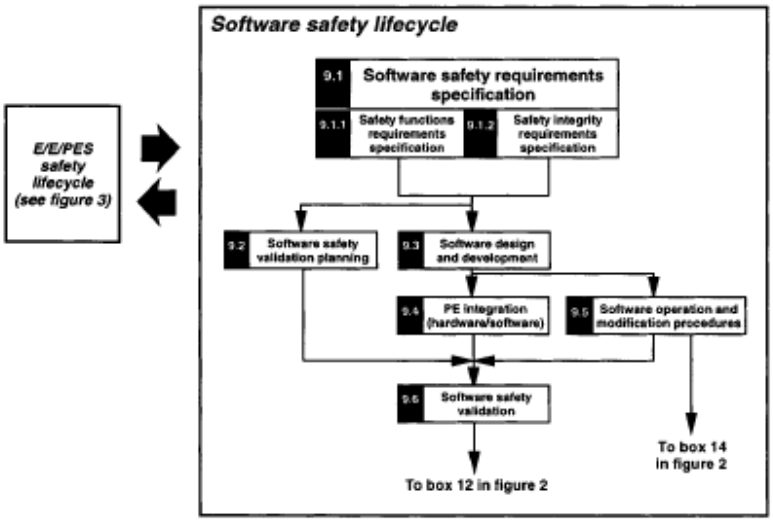


Figure 4 Software safety lifecycle (in realisation phase)

Figure 3 E/E/PE and software safety lifecycles according to IEC 61508 /3/

Should there be a need for modification or retrofit, a request for modification or retrofit is to be made according to the management procedures defined. The aim of this is, that the need and plan for retrofit or modification is documented and process risk analysis is made so that functional safety of EUC is not compromised. The standard requires that documentation of these activities is chronological, so that the evolution of system can be observed.

In decommissioning or disposal phase, decommissioning or disposal of EUC or some EUC' E/E/PE SRS is to be made so that the functional safety for E/E/PE SRS is appropriate according to circumstances in decommissioning or disposal. A request for disposal or decommissioning is to be made according to management procedures defined and decommissioning or disposal activities are to be documented in chronological order.

Second and third part of IEC 61508 covers the development of the E/E/PE. In these more detailed requirements for properties of E/E/PE are given. IEC 61508-2 focuses on the architecture and hardware side of E/E/PE, where IEC 61508-3 focuses on development of software.

In IEC 61508-2 some architectural constraints are presented for hardware design and these have been some what criticized. For example /31/ criticizes these and claims that they may give false indications of functionality. Otherwise IEC 61508-2 presents methods to determine achieved SIL for given system, and also requirements which must be fulfilled to claim some SIL.

In IEC 61508-3 development of software for safety related system is handled. In that part, requirements for development process are set, as well as requirements for used tools and methods. In IEC 61508-3 requirement for software testing is also set as well as lists of testing methods to be used.

2.2.3 SFS-EN 26061 Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems

SFS-EN 26061 is titled "Safety of machinery. Functional safety of safety-related electrical, electronic and programmable electronic control systems.". This standard has almost the same title as SFS-IEC 61508. SFS-EN 26061 is a machine standard and should be applied to machinery, where IEC 61508 is general standard that could for example be applied to processes in addition to machinery and has more details for management of safety. IEC 61508 contains seven parts where EN 26061 has just one (quite thick) part. SFS-EN 26061 is a harmonized standard. SFS-EN 26061 uses aberration SRECS (safety-related electronic control system) for electrical/electronic/programmable electronic safety related control system.

SFS-EN 62061 defines requirements for design, integration and validation of SRECS. This standard manages only close proximity safety of the machine. It is not applicable to non-electrical control system and does not cover electrical safety.

Standard deals with management of functional safety, lays requirements for specification of safety-related control functions, design and implementation of safety-related control systems and specifies requirements for information for use of the SRECS, validation process of the SRECS and modification procedure of the SRECS. It should be noted that there is difference in safety function and safety systems. Safety function is an action and to perform it actions of several different safety systems may be required. In ISO 12100 and in SFS-EN 26061 safety function is defined as "function of a machine whose failure can result in an immediate increase of the risk(s)".

Requirements for management of functional safety are similar in SFS-EN 26061 and in SFS-IEC 65108, but in SFS-EN 26061 they are less detailed and more compact than in SFS-IEC 65108.

SFS-EN 26061 has only three SIL levels, fourth most rigorous level specified in SFS-IEC 65108 is left out. In /12/ it is said that systems are nearly impossible to test for their SIL if their requirement is 4. In /12/ is also stated that higher SIL levels than 4 are unnecessary for if system requires higher SIL levels it can be claimed that system was inherently so unsafe that it should never be realised.

SFS-EN 62061 presents architectural constraints to relate system reliability and safety. If a system has 0 fault tolerance i.e. one fault can cause system to fail, over 90% of failures must be safe failures, so that machine fails into safe state to reach SIL2 or higher. These constraints are similar to those in IEC 65108 and have been under some criticism. SFS-EN 62061 presents some means to estimate random system failures and requirements for design process to prevent random and systematic failures.

SFS-EN 62061 presents requirements for development of safety-related software. It requires that for each piece of software clear allocation of functions is made and that requirements are specified clearly. It also requires that software is developed according to IEC 65108-3. SFS-EN 61062 also presents requirements for testing and validation of SRECS as well as for installation of SRECS and for instructions for use and documentation.

Annex A of SFS-EN 61062 has one method to determine required SIL it uses risk matrix much like one presented in SFS-EN ISO14121. In this risk matrix one factor is severity of harm and other is class of risk, where risk is classified according to its frequency, probability and avoidability. This is quite straightforward qualitative assessing method, so it has its limits, but when safety integrity level is in this standard only three-level classification system it is quite adequate.

Annex B has an example SRECS design and in annex C there is an informative guide to embedded software design and development. Annex F has a method for determining common cause failure factor used in reliability estimation calculations defined in the standard. Method is a questionnaire where a score is calculated and then converted into common cause failure factor. Again here is a very rough method based on qualitative methods. But this kind of methods are quite common in real-life safety engineering because we are dealing with probabilities and there is usually not enough information for reliability assessment.

2.2.4 SFS-EN ISO 13849 Safety of machinery - Safety-related parts of control systems

SFS-EN ISO 13849 is titled “Safety of machinery – Safety-related parts of control systems”. EN 13849 is a harmonized standard. This standard has more of a component based approach to safety. The standard defines a performance level (PL) to all components. Performance levels correspond to safety integrity levels, and a comparison table is given in the standard. The standard presents a way to determine PL for given system when system architecture and safety-related characteristics, such as mean time to failure and diagnostic coverage are given.

EN 13849 does not guide the design process as IEC 61508 and EN 62061 do. The approach in EN 13849 is fist to analyse the hazard and then using a risk graph determine

the requirement level for the safety-related system and then design and check that the designed system shall fulfil the requirements set earlier.

EN 13849 is also applicable to other than E/E/PE based systems. However this standard is not suitable to large and complex E/E/PE systems. Complex systems can be used in a system whose design is made according to EN 13849, but then the complex subsystem is to be made according to some other suitable standard, such as EN 62061, and the system is encapsulated so that it can be handled as its own separate component.

2.2.5 ISO/DIS 10975 draft Tractors and machinery for agriculture - Auto-guidance systems for operator-controlled tractors and self-propelled machines - Safety requirements

This standard is titled “Tractors and machinery for agriculture – Auto guidance systems – Safety requirements.”. Auto guidance systems are systems to assist the driver of a tractor. They take over the steering of the tractor and steers the tractor according to some desired trajectory. These systems usually use GPS-system as their source of navigation data, but other methods can also be used.

This draft standard is presented here because it has good principles that could be applied to other systems as well. It requires that presence of the operator is to be monitored as this is an assistive system, the operator must be at all times presenr and capable to interfere to the operation of the system. It requires that when a machine is started-up the system shall assume a passive or disabled state, so that there is no unexpected start of automated functioning. The system shall be able to start automated operation only in specified circumstances and from a request by the operator and the system shall clearly indicate its state and transfers between the states. The system shall leave the active or automated state when the operator tries to use the normal means of steering as the steering wheel and the effort needed to operate those controls shall not exceed the normal specified standards. Also, if the signals used for navigation are lost, the operation shall stop.

I find the principle that the automated operation is to stop when primary controls are affected to be a good one, for in sudden situations it is more natural for the operator to grab those controls than to start searching for the off button of the system.

2.2.6 ISO/DIS 25119 draft Tractors and machinery for agriculture and forestry - Safety-related parts of control systems

ISO draft standard 25119 “Tractors and machinery for agriculture and forestry – Safety-related parts of control systems” is still in draft phase so it is possible that there will be modifications to this standard before it is published. The standard consists of four parts covering the whole lifecycle of a safety related control system. Even though the title is just safety-related parts of control systems, the focus of this standard is in E/E/PE SRS.

ISO/DIS 25119 draft has quite straightforward approach to the issue and covers all areas quite nicely. It is easier to follow than the other more general standards covering safety-related control systems. It also has, in my opinion, the best description of the safety process integrating to the product development process. The process model is similar to the overall safety lifecycle model presented in IEC 61508, but in ISO/DIS 25119 the system realisation and design phase is presented in the V-model of product development. In ISO/DIS 25119 the realisation phase of IEC 61508 is divided into system design which follows the V- model illustrated in figure, which is then divided to development of hard- and software. System and hardware design is covered in part two of the standard and

software in part three. ISO/DIS 25119 sets requirements for hardware and software separately. A system acquiring some AgPL can be composed from hardware meeting some requirements and software meeting other requirements. Different possibilities to combine system are presented in

Table 7 later in chapter 3.2.1. Software requirement level SRL is used to set requirements and to indicate the integrity of the software.

ISO 25119 presents agricultural performance level (AgPL) which is agricultural technology's version of PL presented in EN 13849 and SIL presented EN 62061 and IEC 61508. Requirements set in ISO/DIS 25119 draft standard are in line with IEC 61508 and EN 62061

ISO 25119 addresses only the evaluation of the safety aspects of the E/E/PES.

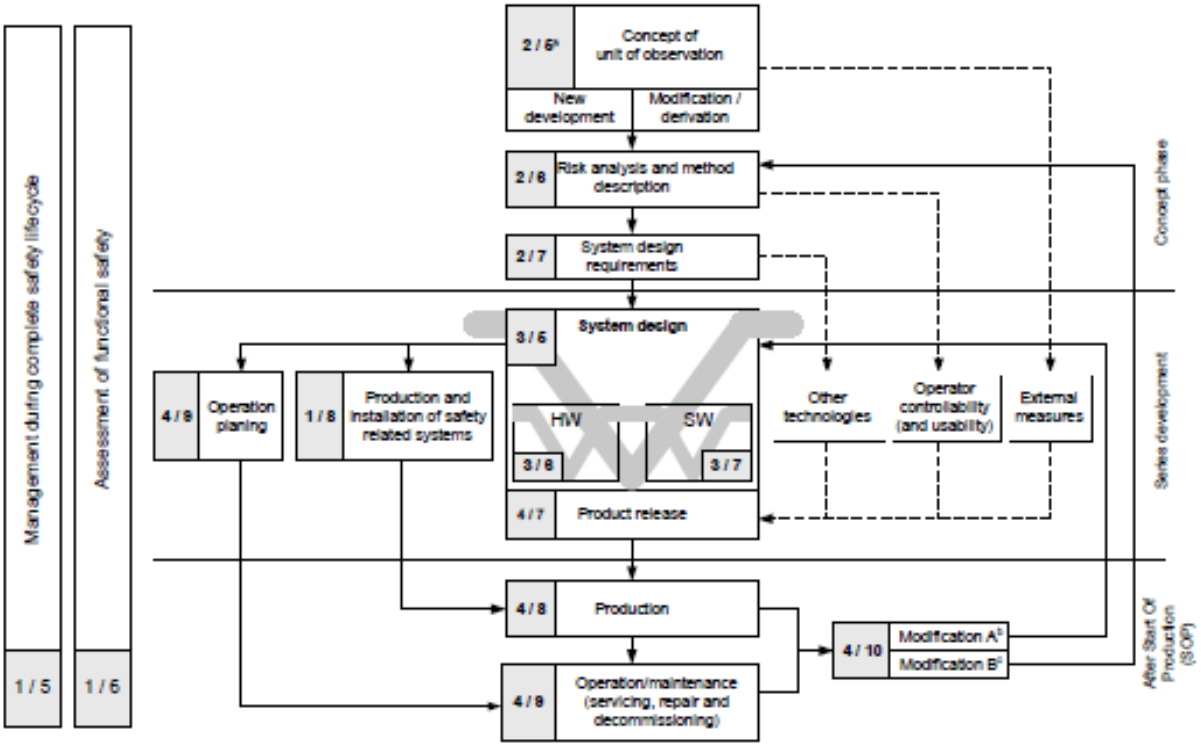


Figure 2 - Safety lifecycle

Key

[a] 2 equals ISO 25119-2, "5" equals of ISO 25119-2:— Clause 5

[b] If machine functions are not effected then go on to ISO 25119-3:—, Clause 5.

[c] If machine functions are effected then hazard and risk analysis according to ISO 25119-2:—, Clause 6

Figure 4 Safety lifecycle according to ISO/DIS 25119

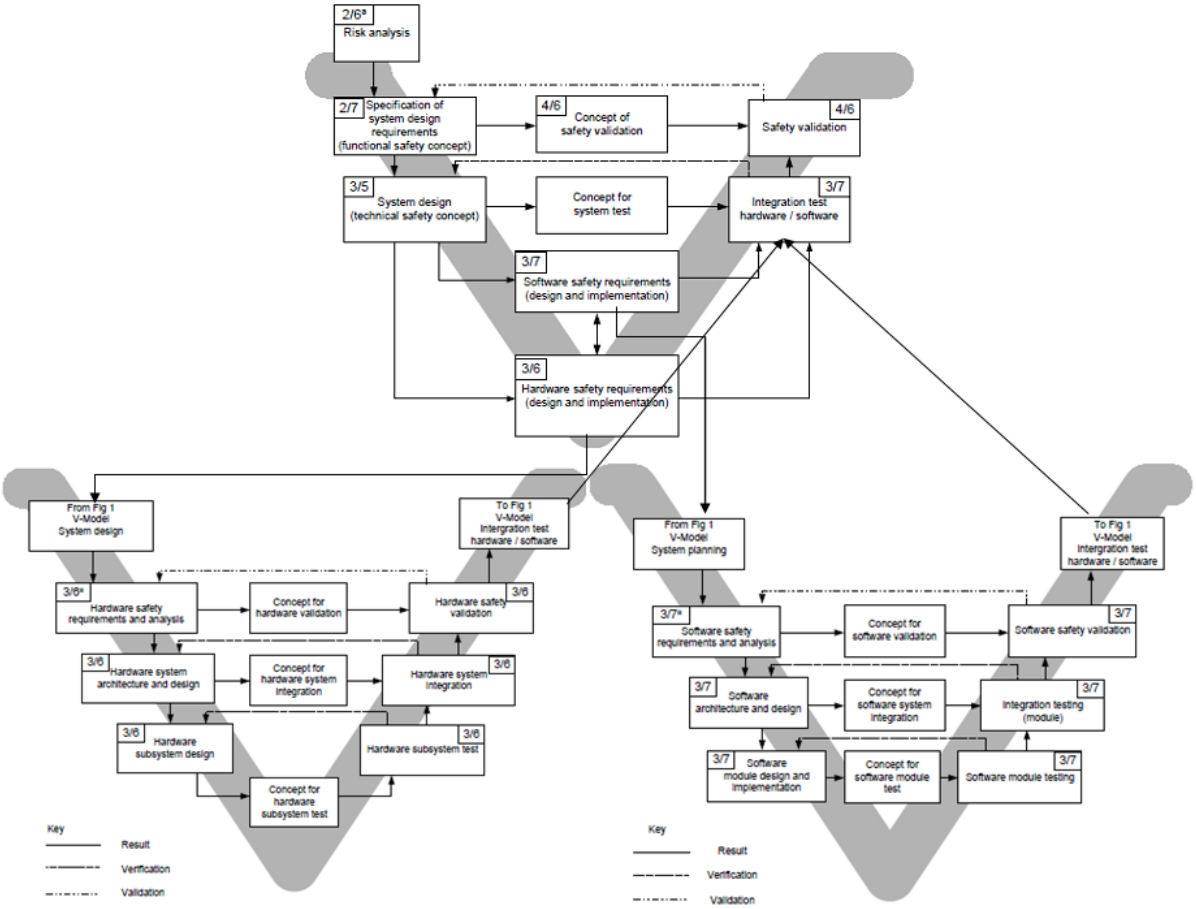


Figure 5 Software and hardware development process according to ISO/DIS 25119. Image composed by the author from figures of ISO/DIS25119.

2.3 Bus systems

Field busses are communication busses used in distributed computer systems. Field busses were created to reduce the need for cabling and to simplify growing need for communication between computers when embedded and distributed systems began to emerge. When using a bus for communication all devices are connected to the bus and the communication goes through that bus, and not through hardwiring between different modules. Devices connected to bus are called nodes. For communication between nodes certain laws are needed so that different nodes can understand each others regardless of what kind of other devices there are in the bus. This is a bus protocol. Also definitions for physical and electrical properties for bus are needed. When a bus system is used to transfer a safety critical message it becomes a part of a safety critical system and its safety needs to be analysed and considered.

Bus systems are often divided into seven layers according to OSI or open systems interconnection model specified in ISO 7498 standard. The OSI model is illustrated in Figure 6. It is not required that any standard based on the model to be partitioned explicitly into seven OSI layer, as long as fundamental functionality is supported./17/ .

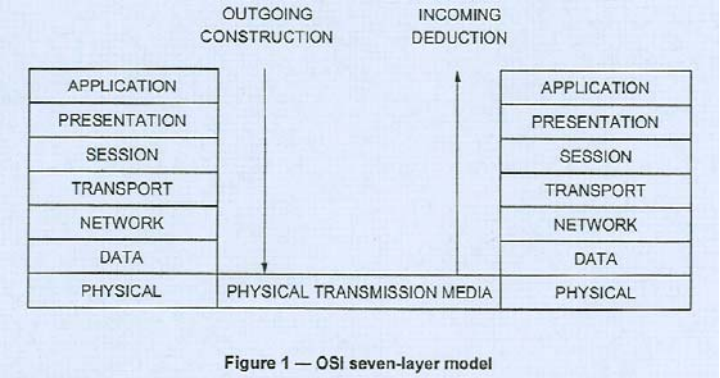


Figure 1 — OSI seven-layer model

Figure 6 OSI model /17/

Physical transmission media is the part that connects different nodes to each other. Most used transmission media is twisted pair cable but also other medias are used such as optical cable or wireless communication.

Transceiver reads bus traffic and stores data from the bus, performs checks to received data, monitors bus messages and sends received and stored messages to application. It also receives messages from application, packs them to suitable format and sends them to bus. Node maker usually buys these parts from commercial supplier. These off-the-shelf solutions include required electronics and software with interface so that the application layer does not need to handle bus traffic functions. Properties and functions of the transceivers are defined in the bus specification or standard.

As signals sent for application are extracted from bus messages many faults are masked as small number of more general failures. These failures are listed in EN 50195-2 standard and few additional failures or threats are added by Alanen et al. in their research paper “Safety of Digital Communications in Machines (VTT 2004) /9/ . These threats are listed in Table 1 Application level signal threats according to /9/. It can be seen from the table that these threats correspond to specific HAZOP guidewords. Another note is that EN 50195 is actually a railway standard for communication in systems like signalling systems. These railway standards dealing with communication systems are often referred in literature when hazards of communication systems are discussed. For application it is completely irrelevant what caused the error as the faults are masked to these types. Defences can be built against these threats. Application level signal threats can originate from numerous root cause failures. In Figure 7 some root causes are listed. In Figure 7 also the development from root cause to application signal threat is illustrated as well as possible defences at different levels of bus architecture.

Table 1 Application level signal threats according to /9/

Threats form /9/	HAZOP guideword
Repetition	More, As well as
Deletion	No, Part of, Less
Insertion	As well as
Incorrect sequence	Before, After
Corruption	More, Less
Delay	Late
Too early message	Early
Excessive jitter	-
Masquerade	Other than
Inconsistency	Other than

Alanen et al have also listed possible defences against communication threats in message level and in architectural level /9/ . These defences are presented in Table 2. Some bus specifications include some of these defences in different levels of those buses' architecture. Table 3 clarifies the meanings of defences listed in Table 2.

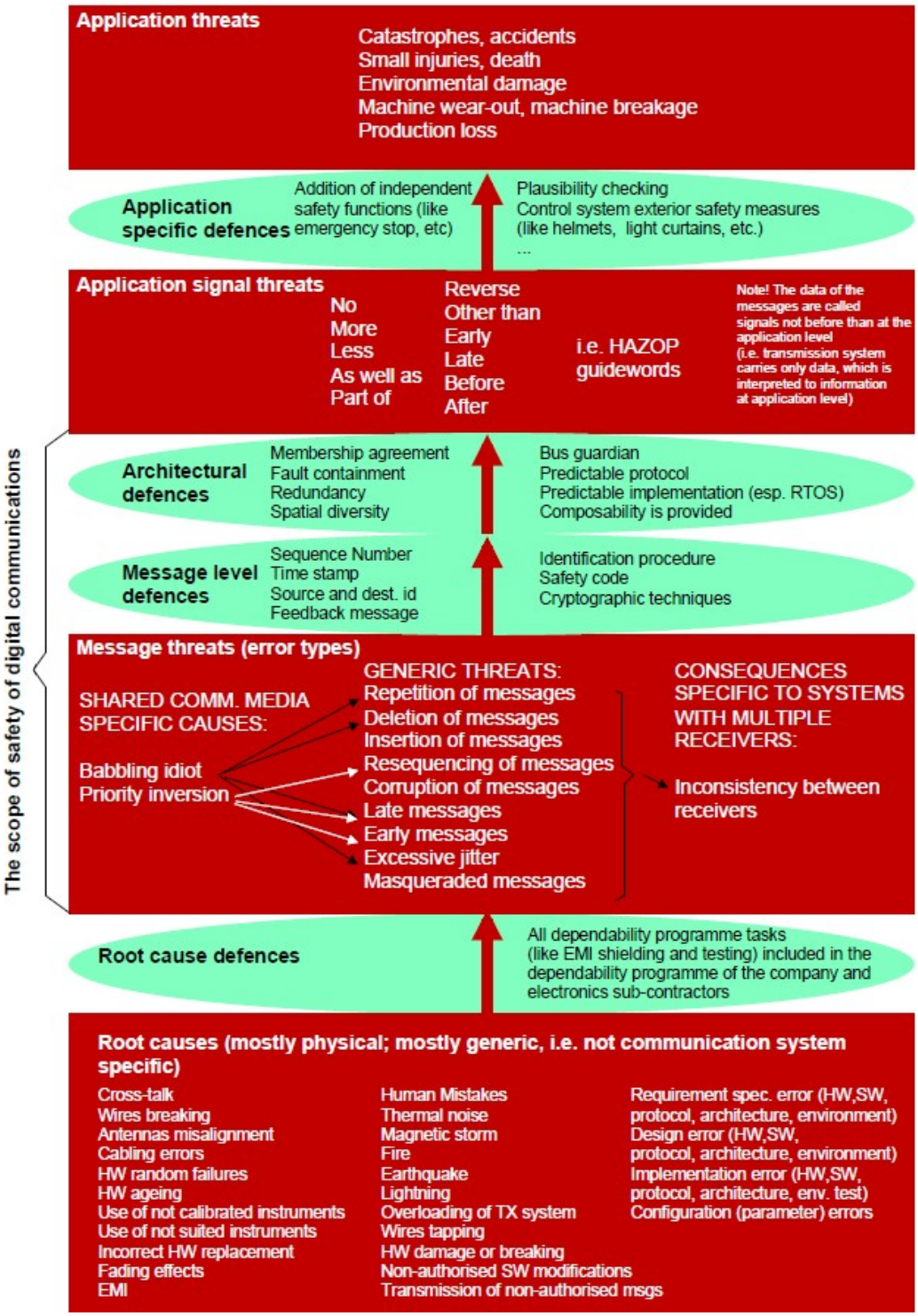


Figure 7 Communication failure root causes and their development to harm. Image taken from /9/

.

Table 2 Communication threats and possible defences according to EN 50159-2 and /9/

Threat	Possible defences
Repetition	Sequence number Timestamp Redundancy/Replication Time triggered architecture Bus guardian Inhibit times
Deletion	Sequence number Time out Feedback/acknowledgement Redundancy/Replication Time triggered architecture
Insertion	Sequence number Source and destination identifiers Feedback/acknowledgement Identification procedure CRC Redundancy/Replication Identifier's Hamming distance
Incorrect sequence	Sequence number Timestamp Redundancy/Replication Time triggered architecture
Corruption	Feedback/acknowledgement CRC Cryptographic techniques Redundancy/Replication
Late	Timestamp Time out Feedback/acknowledgement Time triggered architecture Message prioritisation Inhibit times
Early	Timestamp Time triggered architecture
Excessive jitter	Timestamp Time triggered architecture Message prioritisation Inhibit times
Masquerade	Feedback/acknowledgement Identification procedure CRC Cryptographic techniques Identifier's Hamming distance
Inconsistency	Membership control Atomic broadcast

Table 3 Descriptions of defence methods. Table taken from /9/

Defence method	Description	Used against this threat
Sequence number	Each message has a consecutive number. In the simplest case the message includes a toggle bit.	Repetition, deletion, insertion, incorrect sequence
Time stamp	Each message has a time code, which describes the sending time.	Repetition, incorrect sequence, delay
Timeout (for example, watchdog)	Receiver accepts messages only when they arrive in time or during a predefined time window. Usually exception handling is used to react upon delayed messages.	Deletion, delay
Source and destination identifier	Each message has a source and/or destination address or other code.	Insertion
Feedback message (acknowledgements and echoes)	After receiving a message the module sends a positive or negative acknowledgement or after receiving a message the module sends the whole message or a checksum back.	Insertion, masquerade
Identification procedure	The members of the network check the identity of the other members prior to the start of the system or prior to the transmission of a specific message. Identity may include, for example, information about software and hardware versions.	Insertion, masquerade
Safety code (for example, CRC cyclic redundancy check)	The method adds into the message a checking code; also other types of data consistency checks are available.	Corruption
Cryptographic techniques	Authentication is applied and cryptographic code is added to the message to protect against malicious attacks.	Corruption, masquerade
Redundancy (replication):	The messages are transferred periodically even though no changes in values have occurred; a message may be replicated (for example, sent twice with the other message inverted); the communication subsystem may be replicated.	Repetition, deletion, insertion, incorrect sequence, corruption
Membership control	The members of the network monitor each other and execute exception handling in case of malfunction in one of the members.	Inconsistency
Atomic broadcast	Communication protocol with atomic broadcast ensures that all messages are delivered in the same order to all correct processors in the system and all consumers of the data have a consistent view of data (all accept the data or all reject it).	Inconsistency
Time-triggered architecture	Messages are scheduled in regard to time. The time schedule is often pre-fixed by the system designer.	Repetition, deletion, incorrect sequence, corruption, timing errors, excessive jitter
Bus guardian	Transmission of messages is controlled by a hardware that opens and closes the access path for the transmitter to the communication media.	Repetition
Prioritisation of messages	The messages are prioritised to enable safety-critical messages to access the bus with minimum delay.	Late, excessive jitter
Inhibit times	Similar to bus guardian, but can be implemented by software at the communication subsystem; after transmitting a certain message, that particular message is put in “quarantine” for a given period of time before it can be transmitted again by the particular transmitter.	Repetition, late, excessive jitter
Hamming distance applied to node addresses or message identifiers	The node addresses or message identifiers are selected so that any single bit failure in the address or in the identifier produces a non-used address or identifier and can thus be noticed by the receivers.	Insertion, masquerade

When considering safety of a general bus system often standards EN 50159-1 and EN 50159-2 are referred to in literature. EN 50159-1 discusses safety-related communication in non-trusted but closed network and EN 50159-2 in open non-trusted network. Safety-related communication in an open non-trusted network is of interest in mobile work machinery for it is the most widely used system. CAN network for example is open non-trusted network. However even originally open network can be considered closed when it is guaranteed that no additional nodes are added to the system after it has been implemented. Many mobile work machines are of this kind, but when there is exchangeable equipment that is connected to bus system then the system is open. This is especially the case with agricultural machinery using ISOBUS communication network. These standards define common threats and defences against them.

IEC 61508 discusses communication in networks quite shortly. It requires that the propablibility of undetected communication failure is to be estimated and this estimation is to be taken into account when propablibility is estimated.

IEC 61508-2 clause 7.4.8 Requirements for data communications:

“7.4.8.1 When any form of data communication is used in the implementation of safety function then the probability of undetected failure of the communications process shall be estimated taking into account transmission errors, repetitions, deletion, insertion, re-sequencing, corruption delay and masquerade. This probability shall be taken into account when estimating the probability of dangerous failure of the safety function due to random hardware failures. (see 7.4.3.2.2)

Note The term masquerade means that the true contents of a message are not correctly identified. For example a message from a non-safety component is incorrectly identified as a message from a safety component.

7.4.8.2 In particular, the following parameters shall be taken into account when estimating the probability of failure of the safety function due to the communications process:
a) the residual error rate (see IEV 371-08-05)

b) the rate of residual information loss (see IEV 371-08-09)

c) the limits, and variability, of the rate of information transfer (bit rate)

d) the limits, and variability, of the information propagation delay time.

Note 1 It can be shown that the probability of a dangerous failure per hour is equal to the quotient of the residual error probability and the message length (in bits) multiplied by the bus transmission rate for safety related messages and a factor of 3600. Note 2 Further information can be found in IEC 60870-5-1 and in EN 50159-1 and EN 50159-2.”

IEC 61508 states that if some component, hardware or software, handles both safety-related and non-safety-related functions, then also the non-safety-related functions are to be treated as safety-related. This would lead to very laborious work when assessing safety of bus system, for every signal and node in bus system is to be considered safety wise. This leads to a *white channel approach*, where the whole communication system is designed to meet requirements of IEC 56108-2&3. The other approach is so called *black channel approach*. In black channel approach additional safety related transmission function is created to treat possible failures of communication system. This may mean for example adding extra safety features to message frame.

In EN 62061 issues with data communications are scattered around standard, but mainly it requires that similar assessment of possible communication failures including transmission errors are to be considered. It also requires checks for data integrity and reasonableness at the application level.

IEC 61784-3 standard lays out general rules for functional safety of field buses from principles of IEC 61508 series and other safety standards as from other field bus standard by IEC like IEC 61158. It addresses the same communication errors as described earlier and how to seek protection from them, and effectiveness of different techniques against these errors. In this standard the relationship between residual error rate and SIL is presented.

Evaluating safety integrity for bus system is problematic, for bus system is often bought off-the-shelf solution, and therefore estimation of SIL level is difficult, if no specification is provided. Also other than safety-related systems are often connected to bus, and these systems may also be off-the-shelf solutions without any SIL assessment. And therefore white channel approach is often impossible. The black channel approach is also problematic, for to use of-the-shelf solutions or other solutions by other manufacturers. This forces us to use some certain bus system or protocol, where safety issues may be considered sufficiently or not. Fortunately many bus systems contain some safety features, whether these are sufficient is another question though.

There are many different approaches bus systems take on safety features. Some take actions on physical layer, for example by adding extra transmission media for safety critical functions. This may mean adding an extra wire for shutdown command. Some have features at transmission level and in message frame, For example cyclic redundancy checks. Some have safety features at the application level /16/ . For example additional information in message frames application data frame, that is checked at the application level.

Surprisingly, most of the communication failures are because of hardware faults. Most common types of hardware faults are problems with wiring and poor EMC design /16/ . Therefore most of the bus specifications require that cabling and other electrical installations are made according to proper standards.

The IEC 870-5-1:1990 Telecontrol equipment and systems – transmission frame formats (Current name IEC 60870-5-1) specifies three service classes for data link layers:

S1 Send – No reply
S2 Send – Acknowledgement
S3 Request – Response

/10/

In class S1 message is sent and no reply is expected. This class is used in repeated oneway communications.

In class S2 message is sent and some kind of response or acknowledgement is expected to indicate that message is received or the reception has failed. No reply means failed transmission. This class is used when transmissions are random.

In class S3 message is sent when the receiving end requests data to be sent./10/

2.3.1 CAN

CAN or Controller Area Network bus is a field bus developed by Robert Bosch gmbh in the 1980’s for automobile use /52/. It is event-based bus system that is now widely used field bus especially in mobile work machinery. Just very lately development of technology has reached a point where limitations of CAN bus start to have an effect on development. On the other hand, it could be said that now all possibilities of CAN bus start to be understood and utilised. One main benefits of CAN bus is that it has an ample supply of devices supporting it available off-the-shelf. CAN bus has been standardised in ISO 11898 standard. CAN bus in now widely used in different fields of industry, and it is very popular in mobile work machinery. The CAN standard specifies only two lowest levels of OSI model, so there are few CAN based protocols that build on CAN bus and its message frame, such as CANOpen, SAE J1939 and ISOBUS. The CAN bus is service class S2 bus.

The message frame can be of four types: normal or extended message frame, remote frame, or error flag. In Figure 8 normal CAN message frame is illustrated. Extended format is basically similar but has a second additional 18 bit identifier field. CAN bus has a message priority system. If two nodes in the bus try to transmit simultaneously, message identifiers are used for arbitration. Message with lower numerical value of message identifier is allowed to be send first.

Message arbitration, checking, acknowledging, rejecting and error monitoring is usually implemented in communications circuit, and application creator does not need to consider them. However these functions need to be considered if communication used are safety critical.

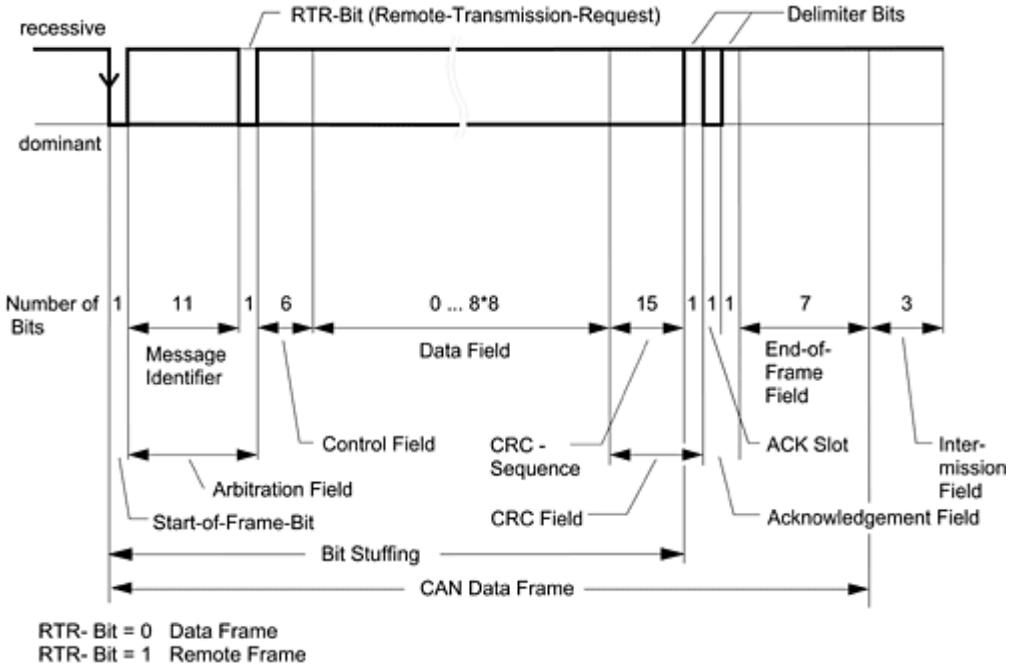


Figure 8 CAN-message frame

CAN bus emphasis high data reliability. If any node in the bus detects an error it will immediately signal an error and all nodes will discard that message and sender will attempt to re-transmit the message. Each transceiver has error counters for transmit errors and receive errors. Transmit error counter increases when sending a message fails and receive error counter is incremented when the node sends an error frame. If the count, on either one of the counters reaches 127, the node moves to error passive state. In this state the node will no longer transmit active error frames. This is to prevent the possibility that some node could behave faulty in a way that it detects all messages as faulty ones and block the whole network with error frames. If the transmit error counter reaches a number greater than 255 the node will move to bus off state. It will no longer transmit to the bus. This is to prevent faulty nodes to transmit erroneous messages to the buss. This is also the CAN bus's fail-silent function. That function is designed to allow the rest of the nodes to communicate. However failure of a node may go undetected by other nodes in the network. The error counters are decremented whenever the function is performed successfully. However a node can not move from bus off state unless it is reset.

Several checks are performed to each CAN data frame. CRC checksum is calculated from the start-of-frame-, arbitration-, control- and data-fields and then compared to the value in CRC field. If these checksums are not identical an error is detected. Transmitter will

detect an error when there is no reply during the ACK slot. A form error is detected when any of the fix formatted bits in the CRC, ACK or end-of-frame fields is in wrong state. CAN transceivers perform checks listed in Table 4

Table 4 Checks performed by CAN transceivers

Node	Check
Transmitting node	-is the bus bit same as the one written on it -is the acknowledge bit dominant
Receiving node	-CRC check -bit stuffing rule check
Both nodes	-status of the fixed bits

These checks guarantee that:

- all global errors are detected
- all local errors at the sender are detected
- random bit errors are detected, if the number of errors is 5 at most
- errors at consecutive bits are detected, if the number of errors is 15 at most
- if the number of bit errors is odd, they are detected

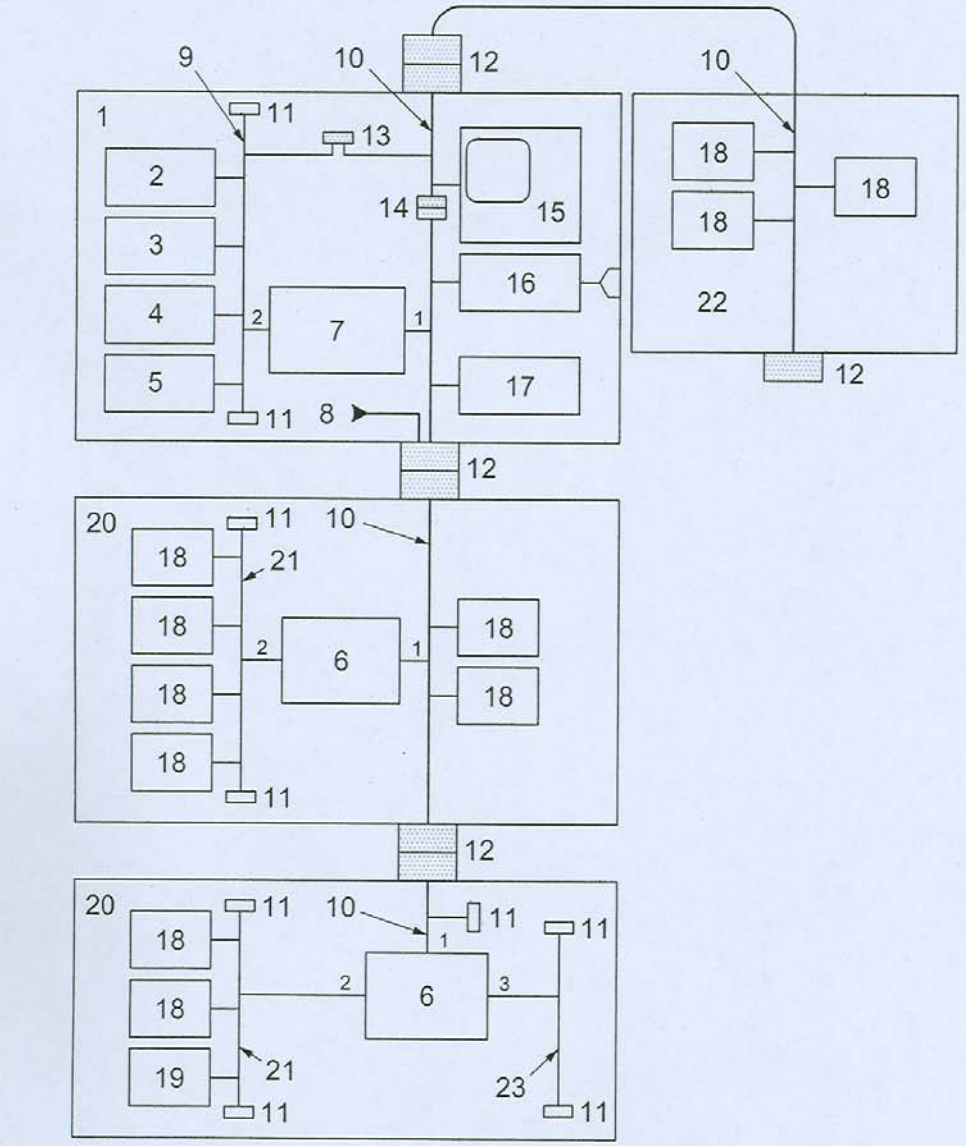
/10/

2.3.2 ISOBUS

ISOBUS is CAN-based field bus designed for agricultural use. ISOBUS is standardised in ISO 11783 standard. ISOBUS was created to standardise communications between electronic control units of agricultural machinery. Manufacturer field and the field of different implementations is greatly diverse in agricultural machinery industry. Therefore the need for standardised communication has been clear since the mechatronization of agricultural machinery.

ISOBUS has similar physical layer, transmission method, transmission format and message acceptation criteria, as CAN bus. To allow communication between implements of different manufacturers also message frame contents have been standardised. ISOBUS uses extended CAN format and in ISOBUS standard contents of identification fields are specified as well as contents of some message fields. For some message frames a transmission rate is specified. These messages with specified transmission rate can be used as heartbeat messages for systems using messages with specified transmission rate. Otherwise messaging is either event-based or request-based.

ISOBUS standard also specifies some special network nodes such as virtual terminal, task controller and file server. Virtual terminal is a standardized interface that a tractor or implement ECU can use remotely using standardized messages in ISOBUS network. Task controller is an ECU that schedules implement functions via ISOBUS according to instructions given to task controller. A file server is an ECU that provides data storage for other ECUs to use via ISOBUS network. Architecture of ISOBUS network is shown in Figure 9 and in Figure 10.



Key

1	tractor	9	tractor network	17	task controller
2	engine	10	implement network	18	ECU
3	transmission	11	terminator	19	lighting controller
4	brakes	12	implement bus breakaway connector	20	rear-mounted or towed implement
5	hitch controller	13	diagnostic connector	21	ISO 11783 or other network
6	network interconnect unit	14	bus extension connector	22	front- or side-mounted implement
7	tractor ECU	15	virtual terminal	23	other standard's network
8	power input	16	management computer gateway		

NOTE Smaller numbers indicate parts on the interconnect units and tractor ECU.

Figure 2 —Typical tractor/implement network physical connection structure

Figure 9 ISOBUS network physical layout /20/

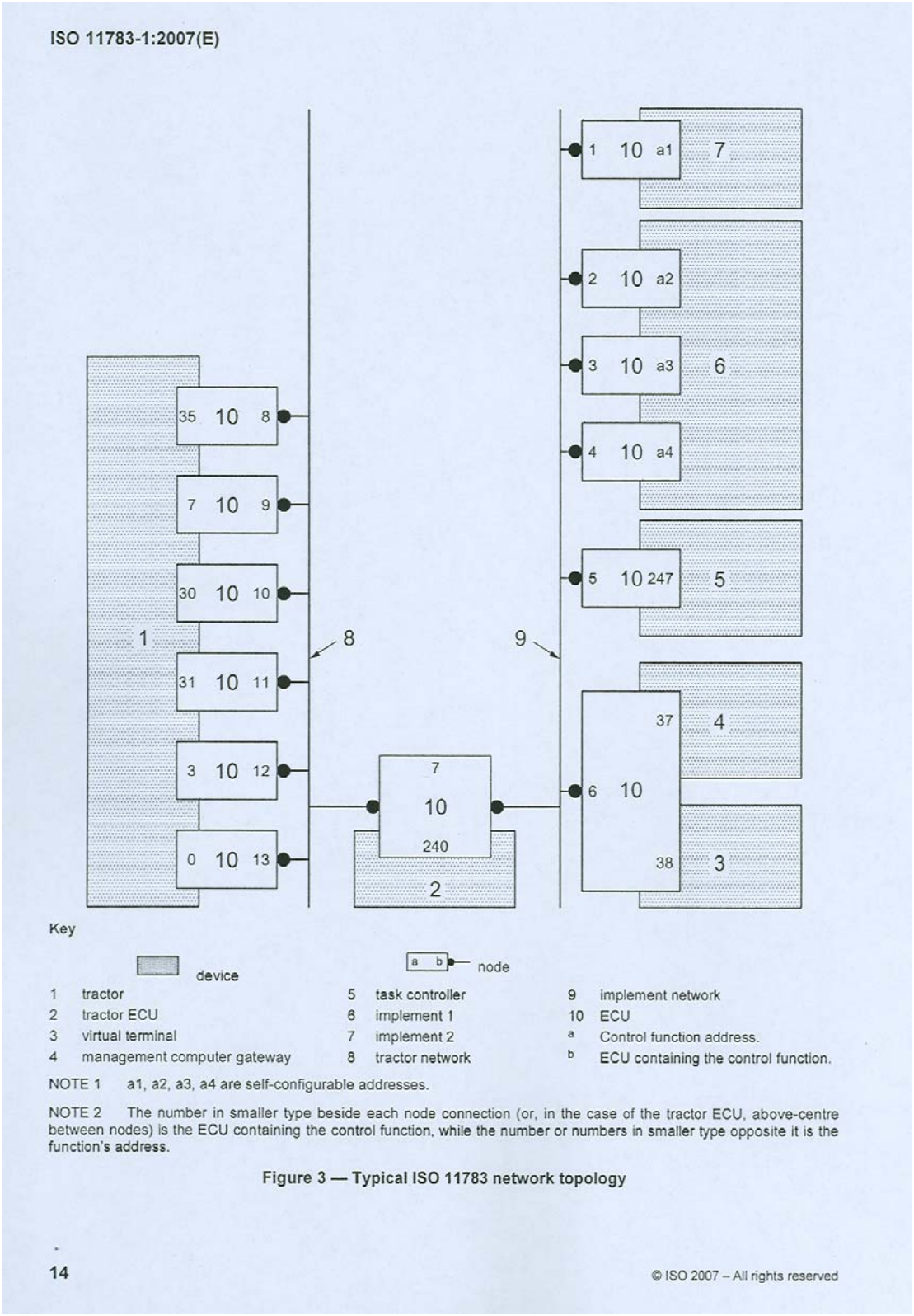


Figure 10 ISOBUS network topology /20/

Tractor ECU is a special ECU that acts as a bridge between ISOBUS network and tractor's internal bus. In ISO 11783-9 standard properties of tractor ECU are specified. In this standard division to different tractor-implement classes is made. These classes specify which information tractor ECU sends to ISOBUS network. Number of these classes is usually added to the end of ISOBUS name like ISOBUS class 3 or ISOBUS 3.

Defined command parameters in ISOBUS 3 are rear hitch position, rear power take of commands for output shaft speed and engagement and auxiliary valves command. Class 3 is of special interest, because in class 3 equipment, the tractor may accept control commands from ISOBUS network. This means that tractor's rear implement may control its own functions independently or task controller may control the rear implement independently. This creates new possibilities for automating field working in farming. Previously each automated implement needed its own controller in the tractor cabin, and it needed operator to adjust auxiliary hydraulic valves or to have its own valve set in the implement. Now the implement may use tractor's VT as its user interface or directly command functions it needs. It is stated in the standard that tractor ECU may deny these control requests from the ISOBUS and negative-acknowledge them.

ISO 11783-9 also specifies these commands for front-mounted implements when letter F is added to class description to indicate support for front-mounted tractor-implement interface. Letter N is added to the class description if navigational messages from GPS or DGPS are provided.

In ISO 11783-9 an implement commanded tractor control option is given. This means that the tractor may accept also other commands from ISOBUS network. This gives the option to control for example tractor's speed, engine torque or hydraulic flow. It is stated in the standard that the tractor shall determine the constraints of each control mode and acknowledge the commands only as appropriate. This gives even greater possibilities for automation of work in field. The implement or the TC could now work autonomously under operator supervision, as they could now control all necessary functions of themselves and those of the tractor. This also gives glimpses of possibility of removing the operator from the tractor in the long run. Commonly accepted development path to completely autonomous remotely supervised agricultural machinery in the industry has been development of driver aids to auto guidance and automated implements to fully autonomous tractors. This view is also presented in/53/ and /32/

ISO 17783-9 also defines a safe-mode operation. It states that upon loss of power or communication with the tractor, the implement shall assume a condition of fail-safe operation, and that irregularities in power supply or control logic failures shall not lead to a dangerous situation. The standard emphasises following:

- The implement shall not start unexpectedly.
- The implement shall not be prevented from stopping if the command has already been given.
- No part of the implement or piece held by it shall fall or be ejected.
- Automatic or manual stopping of any moving parts shall not be unimpeded.
- The protection devices shall remain fully effective.
- Remote controlled implements shall be designed and constructed to stop automatically in the event of the driver losing control.
- The operator shall have the ability to override implement controlled systems.

In Table 5 defences to communication threats listed in chapter 4.4 and their availability in ISOBUS are listed. In Table 5 ISOBUS' defences to communications threats listed in chapter 4.4 are listed.

Table 5 Communication defences available for ISOBUS

Defence	Availability in ISOBUS
Redundancy/Replication	In physical layer Two signal lines with inverted signals Provides defence against EMI and cable faults
Sequence number	No
Timestamp	No
Time out	for some messages
Source and destination identifiers	Yes
Feedback/acknowledgement	Yes Acknowledgement in data link layer Feedback in application layer for some messages
Identification procedure	Address claim when the bus is initialised and when a node first time connects to the bus
CRC	Yes 15 bit CRC in data link layer
Cryptographic techniques	No
Membership control	For some nodes
Atomic broadcast	Yes
Time triggered architecture	No
Bus guardian	No but error counters in transceivers
Message prioritisation	Yes Pre set priorities in standard
Inhibit times	Yes for some messages
Identifier's Hamming distance	No

Table 6 Defences against communication threats available in ISOBUS

Threat	Defence available in ISOBUS
Repetition	No
Deletion	Time out for some messages Feedback for some messages Acknowledgement
Insertion	Source and destination identifiers Acknowledgement CRC Feedback for some messages
Incorrect sequence	No
Corruption	Feedback/acknowledgement CRC Redundancy/Replication
Late	Time out for some messages Feedback for some messages Message prioritisation (fixed)
Early	No
Excessive jitter	Message prioritisation
Masquerade	Feedback for some messages Identification procedure CRC Membership control
Inconsistency	Membership control Atomic broadcast

From the Table 5 and Table 6 we can see that there are several defences available in ISOBUS and that the available defences vary a little depending on the type of the message. The problem with ISOBUS and safety critical messaging is that all messages are specified in the standard and the standard is lacking definitions for safety critical messages. Now all safety critical messages are sent as regular messages, whose access to bus can not be guaranteed in specified time and the receiving node can negative acknowledge those messages. The predefined messages also make it impossible to add additional safety features to messages. Also the access times of messages can not be guaranteed. The bus system is open and there can be many different nodes connected to it. Therefore the bus traffic is difficult to forecast. Therefore some sort of bus traffic monitoring would be needed to detect times when the access times of safety related messages grow too long.

Because there is no way to tell whether the message received from the bus is safety-critical or not, nodes in the bus can override or cancel the safety function intended by the other node. If there would be a way to distinguish safety-critical messages it would be possible to lock requested resource to preferred state, which is crucial in implementing safety-related functions.

The hazards of concern related to autonomous operation of the machine seem to be related to movement of machine. The commands that are used in ISOBUS systems to drive or steer the tractor-implement combination or used in controlling of tractors implement hydraulics, PTO or three-point hitch have specified transmission rates and time-outs. So it is possible to detect a failure in the commanding system if that failure

leads to termination of communications. Erroneous behaviour of the commanding module can not be detected. The standard ISO 11783 also lacks of the definition what is to be done after a time out occurs.

The ISOBUS standard is a communication standard. It, however, does specify some features of some nodes or ECUs. To crate a safe combination of machinery where different parts are made by different manufacturers, we need to know what functions are available at all times and what are their consequences.

One problem is Bus' fail-silent property. If a node fails it will not send anything to bus but remains silent. This is to allow normal communication with normally functioning nodes. To create a safe system, the system needs to know when its safety systems fail and prevent then any hazardous action. This requirement is presented in standards as diagnostic coverage of a safety related system.

In the tractor used in MTT's and TKK's Agrix project one hydraulic valve connected to ISOBUS was especially prone to crashing, and the only way of noticing this, was the operator noticing that functions controlled by that valve were stopped. Had this valve had been used to implement a safety-related function the system would have needed to detect this failure of the valve. Because the ISOBUS is a fail-silent system the ECU responsible for implementing that safety function would have needed to make regular status queries to the valve to find out its state. Other possibility would be that each node would transmit a heartbeat message about its state.

It is very difficult for tractor manufacturer to estimate what kind of implements will be connected to the tractor. So it could be claimed that the safety, safe functioning and the safety-functions of the implement are the responsibility of the implement manufacturer. On the other hand, the implement needs to use the resources of the tractor to function. Therefore the implement manufacturer needs to know what kinds of functions are guaranteed by the tractor. These functions would need to be specified in a standard or in an industrial agreement. The author takes no view on whether these functions need to be specified in ISO 11783. Other solution for this problem would be that the implement would itself have the means to control the resources and implement the functions it needs. This would radically change the structure of the tractor and the implements. If all implements would have their own hydraulic valve packs and couplers, gears and clutches for PTO-shaft and controls for any other possible power sources and their use, the implement could perform all its functions independently and all safety issues would be left for implement manufacturer to worry about. This would, of course, mean that such valve pack that exists in today's tractors for implement would need to be replaced with just an outlet for hydraulics. This would also mean that direct or direct manual control of the implement from the tractor cabin will become impossible. This might create new problems for the system. Another drawback of this solution is that the implements will become heavier, more complex and more expensive, increasing the overall cost of the machine system where one tractor is used with multiple implements.

Both white channel and black channel approaches are problematic for ISOBUS. White channel approach would require the whole bus system to be specified to some safety criterion. This would include both the hardware components and the methods for communicating as well as the used software. The physical components might be specified to some SIL and the physical transmission media as well as transceivers and other communication hardware could be duplicated if analysed to be necessary. Also, the software used in communication hardware would be specified to acquire some desired SIL. Communications would also need to be monitored to guarantee access of safety

critical messages to the bus in specified time and to monitor the availability of communications i.e. whether all nodes are in the bus and whether the bus is functioning properly. There might be a need to re-define the physical layer of the bus system and specify the useable parts to gain a SIL level for the bus system. The idea of ISOBUS being based on CAN bus is that CAN bus components could be used to create an ISOBUS network or device. Putting heavy restrictions for components to use might cause the loss of usability of major part of CAN modules. In ISOBUS environment a special class of safety-critical messages could be specified, and for these messages access to bus would be guaranteed and functions to be performed on arrival of these messages would be specified and guaranteed. Implementing such functions would require changes to the standard. This would mean that major changes are needed in the message layer of the system. New class for safety critical messages is needed or some other way to indicate a safety critical message. In ISOBUS all communication messages are standardised so adding new features to the message frame would cause all communications to be re-designed to take new safety features into account. Creating new class and identifier for safety critical messages might be less of work. In application level we would need to specify what kinds of functions we have for safety-use and guarantee the execution of these functions. Also the possibility to cancel or override these functions needs to be prevented. In application layer we also need to monitor the availability of the safety functions and signal their failure.

The black channel approach is also problematic in ISOBUS environment. In this approach we need to build additional safety features to the message frame, which could be used to monitor the availability and execution of the safety-function. In ISOBUS the message frame is already specified fully so adding extra features to the frame would require major changes to the standard. There would also, as with the white channel approach, be need to indicate the safety criticality of the message. In black channel as well in white channel we need to specify the safety-functions and to guarantee their execution and to monitor the safety function and to indicate its failure. These would also need to be specified and added to a standard whether to ISOBUS standard or some other standard specifying safety and functions of agricultural machinery.

2.3.3 Fault tolerance in CAN based buss

CAN is a fail-silent system. If one node fails or its transmitter’s error counters reach their maximum limit the node goes silent. It will not disturb functioning of the rest of the bus system but other nodes may not be aware of the failure of the other nodes. This may be beneficial in some cases, but when safety critical system is implemented and higher levels of safety integrity is required, it is required that system will monitor its own functioning and detect its own failures and this can not be achieved with CAN based bus system as such. Additional monitoring of the nodes is needed.

CAN buses can tolerate many failures at its physical layer, which are also specified in CAN specification. These faults include disconnection of communication wires or shortcuts in communication wires to ground or to power supply line. CAN modules should be able to detect these faults. In some cases CAN nodes may continue communications with reduced noise ratio. /10/ However these functions are not available in hi-speed CAN buses, like in ISOBUS bus.

2.3.4 Safety oriented bus

There exist several bus systems where safety features are taken into account. Some of these bus systems are designed to transfer information between safety-devices for example from safety-switch to safety-logic and from there to safety-relay. These systems are used to create complex safety systems where there are several safety related components and where several different combinations of safety-device inputs can lead to many different safety-functions. Some bus systems are also useable for regular communications as well as for safety-related communications. There are many approaches to create a so called safety-bus. Some systems use a safety functions built on top of an existing bus system, some others are built for safety and handle safety issues right from their architectural level and from methods of communication. Benefit from the use of these bus systems is that safety aspects of the bus system and its components are already considered to some level and the system developer only needs to consider safety at the application level./16/

FlexRay™

FlexRay is a bus system under development. It is being developed by FlexRay consortium. In this consortium major automotive manufacturers, like BMW, Daimler, General Motors and Volkswagen and component suppliers like Freescale semiconductors and Robert Bosch develop fault-tolerant deterministic and high capacity bus for automotive use. This bus is intended for use in automotive control applications like x-by-wire/51/ . This is a bus system in development but it is presented here as an example of a bus system where the safety aspects have been taken into consideration right from the start of the development and where the communication threats are dealt with system architecture rather than adding additional safety layers on top of the system./16/ /9/

The FlexRay will have both time-triggered and event-triggered transmissions in use. Time triggering will make the bus deterministic and failure of one node is recognised quickly. Global time provided by a bus master will be used to synchronise transmissions. The bus will have error management and signalling capabilities. All erroneous and missing transmissions will be signalled to host. It will have a bus guardian in a data link layer. It will support many bus topologies and redundant channels. /51/ The error management shall follow the “never-give-up” principle, which means that a node and the system will attempt to operate until some critical error state is reached./9/

3 Tractor ECU in autonomous operations or under autonomous implement command

Tractor ECU, or T-ECU, is an ECU, defined in the ISOBUS standard's part nine. It is an ECU that acts as a gateway between tractor's functions and ISOBUS network, so it is the tractors ISOBUS interface. In the ISO 11783-9 standard is defined so called "implement commanded tractor control option". In this control mode the tractor's resources such as steering, velocity, hydraulic functions, PTO, or the three point hitch may be commanded by an external device.

ISOBUS standard states that when under commands from ISOBUS T-ECU acknowledges commands only when appropriate and that T-ECU should define the constraints to those commands./25/ This means that envelope of safe operations is defined and only commands within that envelope are accepted. However defining acceptable commands for some commands is easier than for some other. For example defining acceptable range for engine speed torque or hydraulic pressure is quite simple, but for example maximum vehicle speed or rate of turn is more complex for it requires information about possible implements, vehicles centre of gravity and environmental conditions such as slippage or slope of field to name a few. These operations can however be determined using worst scenario design method. However, if we add navigational functions, should T-ECU have information about tractor-implement-structure and pose and map and location information and how reliable this data is.

As T-ECU acts as a gateway between tractor's functions and ISOBUS network it would be possible to build some kind of a safety-layer or safety manager as proposed in /33/ . However, building very exact safety-functions is quite difficult or impossible because it is not known what kind of implements will be connected to the tractor. What could be built instead is the monitoring of ISOBUS network's functionality. The ISOBUS standard lacks the definitions what to do if a network fault or error occurs. It is stated in the standard that if the communications are lost the implement shall assume a safe mode of operation. The standard does not state what is done in case of lesser faults as message time-outs.

The ISOBUS standard specifies a transmission rates for messages that are used to control different tractor-resources as well as for some other types of messages. These messages can be used as a heartbeat messages for these functions. The problem is that access to bus may cause extra delay for message as access to the bus is not guaranteed. This delay can however be estimated /10/ . The more serious problem is that it is not defined in the ISOBUS standard what to do after a time-out has taken place, and can the operation continue, if the connection is re-established after a time-out. Also, it is not defined in the standard, what to do, if we, for some reason, get conflicting messages or one resource is attempted to be controlled by two different nodes.

When considering safety issues with autonomous functions performed via ISOBUS, one must remember that operator is still present in the tractor. This means that the operator can act as a backup system, if he has possibility to take over the controls. Then the controls must be easy to take over and the operator must be aware of the state the control system is in.

According to ISOBUS standard the implement shall be designed so that it shall fall to safe mode if communications with tractor is lost or power is lost.

3.1 Software safety

Developing control software for autonomous machinery is often considered most difficult and complex task on development of autonomous machinery. Extra difficulty and uncertainty is added when some level of safety is required from this software

Storey defines validation as the process of confirming that the specification of a phase, or of the complete system, is appropriate and is consistent with the customer requirements, /12/ and verification as the process of determining whether the output of a lifecycle phase fulfils the requirements specified by the previous phase./12/ By lifecycle phase we mean here the phase in product development's V-model. Using these definitions we can conclude that if we have a valid specification and we verify that we have a product that fulfils its specification we have a valid product. The problem is that we do not have a clear way to do the validation process. There is no external reference point to which we could refer. And software systems are also very complex so that they are difficult to test. Also the hardware is often so complex, that even testing it is too complex process to perform and manage.

The standards give guidelines how to manage, plan and develop software, but they do not give any fixed way to test validity of the system. IEC 61508, EN 62061 and ISO/DIS 25119 all give some guidance to developing safety related software and especially to how to realise this software. IEC 61508-1 focuses especially on creating specification for safety related software.

Now we could claim that if the software's specifications are valid, then all we have to do to show that our software is safe is to verify that it fulfils our specification.

The development process according to IEC 61508, illustrated in Figure 2, begins by defining and analysing the system. After the definition and analysis phase safety related functions should be specified and allocated. After the allocation phase, according to IEC 61508 for software, we should create software safety requirements specification, which is made of safety functions requirements specification and safety integrity requirements specification. The safety functions requirements specification would include definition of the functionality of the software and the safety integrity requirements specification would define the required SIL for each function. The SIL will then set some limitations for design and implementation of the software, for example what kinds of development tools can be used or what development methods are available. Having proper and valid specification at this phase is very important, for it is the specification to which the software is then verified and according to which it is designed. The problems concerning specifications are handled later in this chapter.

When we have a proper specification design and development of the software can begin. At the same time with the design and development of the software, a validation or verification plan is to be made for the software. In this plan we need to define how to verify that our software fulfils the safety requirements specification. Also, at the same time with the software/hardware realisation phase, a verification plan for the overall system is made.

All A- and B-type standards and some C-type standards presented in this text do not state explicitly what is safe and what is not. The case is the same here. These standards set

requirements and give instructions on how the software should be created or how it should be validated. Necessary safety is defined and realised by the creator of the machinery and software. These standards define a process where safety is built during the process. They require developers to define and analyse their object of development and to identify possible hazards and to react to them. Requirements for safety have to be defined by the developers with the help of systematic analysis of the system. If the definition of the system is made properly and risks of the system are identified and analysed properly, then it should be possible to make a valid safety requirements specification and from this specification it should be possible to create a verification plan. If, for example, it is noted that poor memory handling by the software may cause risks, then to validation plan is to be added testing of memory handling, and for software requirements is to be added requirement for proper memory handling. The creation of safety requirements specification and verification plan may also reveal weakness of the development team and help in getting external help. If for some part of the system some expertise is needed then that expertise needs to be acquired.

As it is now clear, key to creation of safe software is a valid specification for software. Creating a proper and valid specification is well recognised problem in product development and especially in software development. Reason why problems with specification of software are so well-known is that many developers use external services to produce software. I.e. they buy software from some supplier. This is the case especially with small and medium size businesses, which may not have the resources needed or knowledge to produce the software by themselves. This leads to a situation where the developer may have no natural knowledge about the system, to which the software is being developed, or about the requirements that this system sets. To a person familiar with these systems requirements may be so obvious that these requirements are not even mentioned anywhere.

There are two approaches to these problems. One in which the specification is made so precise that very little if any knowledge about the system is needed by the ones implementing the system. The other is that the ones developing the software have sufficient natural knowledge about the system so that even little looser specifications are sufficient. Both of these approaches require good exchange of information and good communication between the purchaser and the supplier.

The IEC standard 61508 also emphasises good communication. It requires that persons responsible for certain aspects are defined and that their responsibilities are also defined. The standard also requires good documentation of the process and decisions made. When persons responsible for certain matters are defined and the level of documentation is set, then communication between different parties becomes easier as there is some information to exchange and it is clear from who this information can be acquired.

Good communication requires that the developer of software is well integrated into the development process, so that he knows what is expected from the software, from its functionality and from its safety integrity. The developer must know if the software piece under development is safety-related, and what that means. As the specification is as important as it is, sufficient time should be reserved for creating it, and all relevant parties should participate in creation of this specification.

One more important aspect in proper specification is that it is unambiguous and understandable. The specification may contain all relevant requirements, but if they are stated unclearly or there are conflicts in requirements these requirements may not be fulfilled in the realisation of that specification.

One interesting solution for specification problem is the use of formal methods. These are methods where the specification is expressed in formal language. These methods are still rarely used, because they require lot's of resources and training. A few examples exist in use of formal methods for example in some nuclear power plants. /12/ Formal methods are discussed shortly later in this text.

The IEC 65108-3, EN 62061 and ISO 25119-3 all discuss the development of software. There is difference in the approach and depth between these standards, but all have common basic ideas. The first one is organised and planned development process. The second one is analysing and defining the problem in a systematic way. Both IEC 65108 and ISO 25119 define clear input and output data for each steps of the development process. Both set requirements for the output data and also for the process used to produce that data.

The software development process described in IEC 61508 is illustrated in Figure 3 E/E/PE and software safety lifecycles according to IEC 61508 and the process described in ISO 25199 is illustrated in Figure 4. In both standards the development of software is related to the development of hardware and to the development of the whole control system and ,moreover, to the development of the whole system.

The ISO 25119 lists different methods and techniques for each phase of the development process and it lists which methods should be used in different requirement levels. The IEC 61508 requires that each phase of the development process is verified for validation of the process. Annex A of IEC 61508-3 has a guide for selecting suitable tools and measures for that verification process for different safety integrity levels.

When developing safe systems also the tools used should be analysed. This applies also for software development. Standards like EN 62061 IEC 65108 and ISO 52119 require that also software development tools must be taken into account. This requires that safety of compilers IDE tools and analysis tools is to be considered. This would also require that operating system on which software is run is to be analysed. However analysing compilers or let alone modern operating systems to highest integrity level are impossible because of the shear complexity of these systems. Operating system's memory handling or compilers' compiling errors can be a source of unexpected and undetected systematic common-cause errors. However as these tools are very complex, very thorough analysis of such components is very difficult and required only at the highest SIL levels. In the lower levels considerations of properties and possible risks of used tools is enough. Use of right tools for right purpose is of course required. Use of well tried and widely used compilers and tools is encouraged, because it can be assumed that most errors from these systems are detected and removed. Also standards encourage use of well tried tools. For operating system use of simple runtime kernel can be considered or providing software isolation by the means provided by programming language. In more complex systems use of cyclic execution scheme could solve problems of task scheduler /12/

3.1.1 Low level safety architecture

Low level safety architecture is a strategy to manage complex systems from the safety point of view. When system is designed, the system should be partitioned to smaller, more manageable, pieces. These partitions can then be arranged according to the level of operations they perform. When arranged in this way system forms a pyramid-like structure where simple low level functions, such as reading sensor data and commanding actuators are at the bottom, above them there are for example simple control loops and bus communication. At top are more complex and global functions such as AI, task

managing or SLAM. It is preferable to perform safety functions at the lower levels of architecture, for it is preferable to have simple systems that are easier to manage and analyse. If an important safety function requiring high SIL is implemented in for example complex AI system, the whole AI system should be developed and analysed for that integrity level, and not only that all systems that this system is dependant on need to be built to high SIL. So if we for example have a safety switch which should prevent some functions to be performed. it would be easier if we would have a simple system that would just prevent certain actuator from working if that safety switch is in some certain position and just inform modules at the higher levels that this function can not be performed. In this case the higher levels still need to react to that situation, but they do not need to be developed to meet as high requirements as the would, if the safety function would be performed in them. Also, if we would like to create some sort of safety-manager or safety-layer set-up, it would be sensible to place it in lower levels of system architecture. /12/ Partitioning system and designing system architecture should be done at the same time when allocating safety functions when following the design process defined in IEC 65108 and EN 62061.

Sufficient isolation between software modules is needed if some software modules, running on a same platform with safety related modules, are to be excluded from safety analysis. ISO 25119-3 annex B provides example methods for proving independence and isolation of software modules.

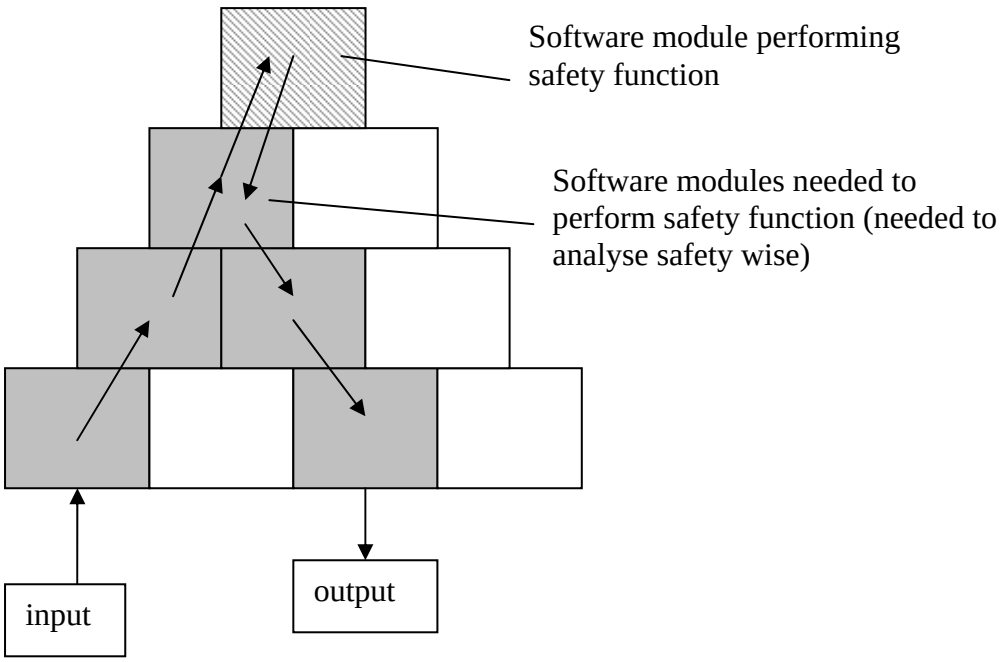


Figure 11 Software partitioned so, that safety function performed at high level

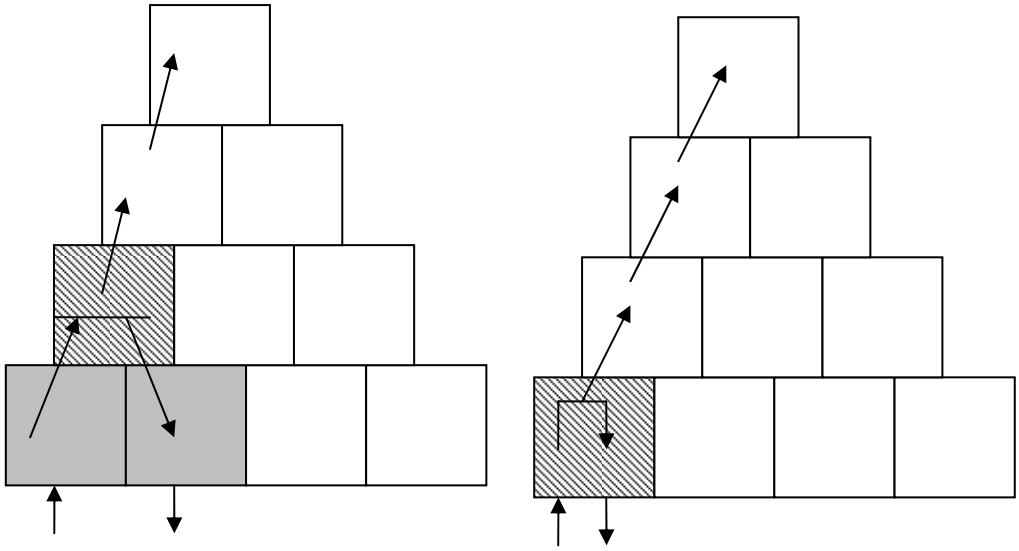


Figure 12 Software partitioned so, that safety functions performed at low level

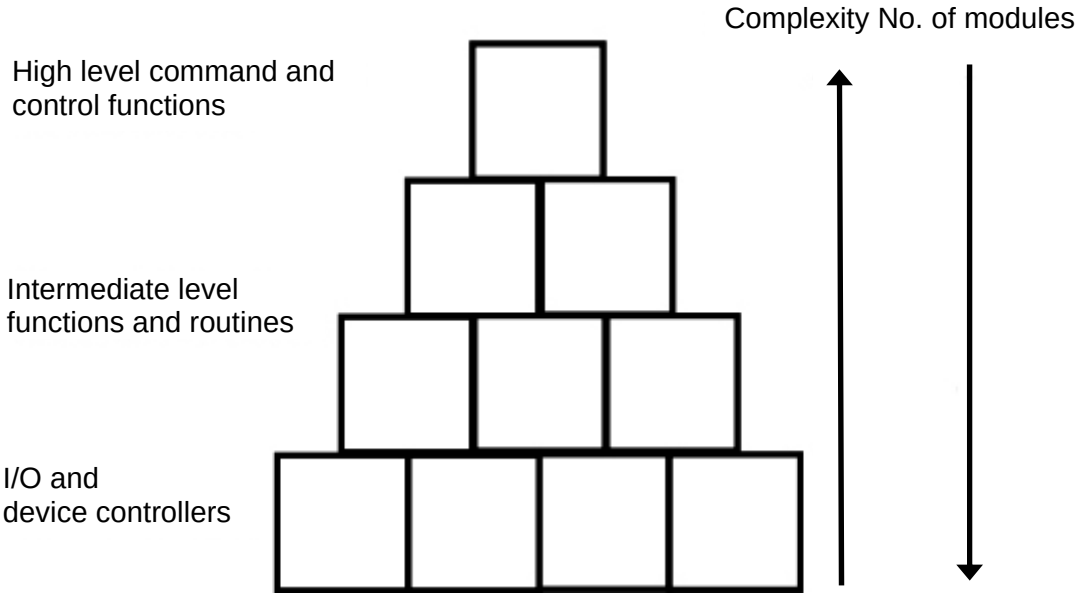


Figure 13 Software modules and their complexity

3.1.2 Formal methods

Faults in software are always systematic and are due to faulty coding or logical errors. Errors in coding can be removed by inspecting the code or analysing its functioning. Coding errors are often errors like errors in memory handling or in declarations of variables. Errors in coding can be eliminated during development. There are many automated inspection software to seek these errors, most already integrated into software development environment. Errors in program logic are more difficult. These errors lead program to function in a wrong way but do not show up in inspection. Some logical errors come from program developer's own mistakes, but most originate from poor or faulty software specification. Software is developed according to its specification and also tested against that specification. Specifications are often given in natural language, such as English or Finish. Problem with natural languages is that they are not unambiguous.

Some expressions can be understood differently in different situations. Phrase “here’s a man eating lion” is an example that quite clearly demonstrates problems with natural languages. In a globalised world situations are even more complicated because workers may come from different countries and cultures and may not understand language used in work place as well as their co-workers and this adds risk of misunderstanding. Use of so called formal languages and methods reduces or eliminates problems originating from poor specification. It does not remove problems caused by faulty specification but reduces risk of such faults and makes it easier to detect such faults. Formal languages aim to describe functioning and specification of program in unambiguous formal way. These languages use mathematical language and make it possible to make checks on specification, create programs correctly, test and validate programs. Using formal languages also opens possibilities for automate these tasks. If we have formal mathematical description from the functioning of program the actual code could be created automatically, and so reducing the risk for coding errors. However formal methods are still under development and development tools are not widely available. Use of formal methods also is quite complicated and much training is needed if one wishes to start using them. Examples of formal specification languages are OBJ, Vienna Development Method (VDM) and Z notation.

3.1.3 Software testing

Software is tested to verify its correct functioning. When non-critical software is developed it is usually only tested to see that it functions correctly in its intended and expected use. Safety critical software however is expected to function and perform the right function even in improbable an unexpected conditions. Therefore exhausting testing where the software is given all possible inputs and all outputs produced by software are evaluated. However, as programs grow more complex and perform more complex functions and have more inputs and outputs, this exhaustive testing soon becomes impossible to perform /12/ . In exhaustive testing many of the input configurations are redundant and lead to execution of the same branch in software structure. Selecting cases that are more of an interest might reduce the number of test cases to a manageable level. Often just selecting cases of interest does not reduce the number of test cases to a manageable level. Therefore other methods of software testing are needed.

Software testing and analysis can be divided into two groups: static and dynamic. Static analysis is analysing code at source level without compiling or running the code. In static analysis code is not actually run therefore this test method is called analysis instead of test. The analysis of software architecture and design as well as its dataflow analysis is also counted in static analysis. In dynamic testing and analysis the code is compiled and run against dynamic test environment. Dynamic testing is more complex task than static analysis for it needs the test environment and often additional code has to be injected to the piece of software under test, to monitor its functions and state and to alter execution of the software according to test plan. Of course tools are also needed in static analysis, but in dynamic testing environment needs to be customised for the tested software/49/ . When testing highly critical piece of software, some questions arise, such as how will the injected code effect on behaviour of the software/12/ .

The standards demand some certain type of testing for software. In ISO 25119 testing methods that are recommended for some requirement level should be carried out and if they are not carried out the reason for doing so should be justified and documented. Also IEC 61508 has similar type of list or table of testing. The standards also demand that both design and testing are planned carefully and executed according to the plan. For

validation and acceptance of software for use, it is required that the piece of software passes the tests planned for it and that other requirements laid out in standards, such as planning, documentation and realisation methods, are fulfilled. Nordtest developed a proposal for Nordtest method to validate software according to IEC 61508 (Nordtest technical report 459). This test is a checklist that verifies that all requirements set by IEC 61508 are fulfilled. For testing and validation it only verifies that testing and verification plans were made properly, that the tests were carried out and documented properly and whether the pieces of software passed those tests. It does not question what the tests were, but were they planned properly. Proper planning, of course, requires the use of correct and suitable testing methods.

Swedish SP Technical Research Institute of Sweden also listed and presented different verification and validation test methods for different phases of development of safety related systems, in their report "Methods for Verification and Validation of Safety" by Strandén et.al (2007). Many methods listed in this report can be applied to software and are also presented in IEC 61508 and ISO 25119.

3.2 Hard- and Software Redundancy

For safety-critical systems some level of redundancy is needed. By redundancy we mean that there are multiple ways for performing some function and these ways are redundant to each other. With redundancy we allow machine to function safely even if one or more of its safety-related systems fails. Redundancy increases system's reliability and fault tolerance. System's safety increases through that increase in system reliability.

There are several ways to increase redundancy in system. Storey /12/ lists four forms of redundancy: hardware redundancy, software redundancy, information redundancy and temporal redundancy. Hardware and software redundancy is defined as use of additional hardware or software to that what would be necessary to implement required function in the absence of faults, with the aim of detecting or tolerating faults. Information redundancy is defined as use of additional information that what would be necessary to implement required function in the absence of faults, with the aim of detecting or tolerating faults. Uses of parity bits or checksums are forms of information redundancy. Temporal redundancy is defined as use of additional time that what would be necessary to implement required function in the absence of faults, with the aim of detecting or tolerating faults. Temporal redundancy is a good defence against transient faults. Transient faults are faults that manifest themselves temporarily and disappear, but the error caused by them may remain in the system. Information and temporal redundancy may be implemented using hardware or software techniques.

Hardware redundancy can be ether static or dynamic. By static we mean that there are several systems performing the same task and their outputs are combined through some voting or combining element so that if some system fails others still functioning properly can perform the task. Static redundancy masks the fault. That is it conceals fault so that its effects do not interfere with other systems. An example of static redundancy is triple modular redundancy, where three modules perform the same function and their outputs are combined in a voting element so that two-out-of-three result is the one that is passed forward./12/

By dynamic hardware redundancy we mean systems that are actively detecting faults and errors. These systems have modules that monitor the function of the system and when a

fault is detected they react to it. The reaction can vary greatly, form disconnecting the output to signalling failure and switching to spare system. These systems do not mask the fault but try to contain the fault and to reconfigure the system and/or signal the failure./12/

Statically redundant systems are often expensive to manufacture due to use of larger numbers of components. To build a system, that would statically tolerate one fault, three systems would need to be built./12/

Even if systems are built to be redundant they can still suffer from common-cause failures or common-mode failures. Many redundant systems have shared resources such as common input point, power supply or voting element, and a fault in such shared resource will cause whole system to fail. Also, if redundant systems are built using same components or design they may have common systematic failures, which could cause all redundant systems to fail simultaneously. Defences for these types of faults are minimal use of shared resources and design diversity. Design diversity means that we use different kinds of designs to perform same function in a redundant system. This reduces the risk for similar kinds of systematic faults existing in systems. However, use of diverse design does not guarantee freedom from such faults./12/

Often it is practical to build so called hybrid systems, where both methods static and dynamic are in use. For example building triple modular system and adding some diagnostic function to voting mechanism.

Means for software redundancy are somewhat similar to those in hardware. When a hardware block containing software is duplicated to gain more fault tolerance, this duplication provides no extra protection for faults originating from software used in both blocks. Because software faults are always systematic both pieces of software fail similarly, therefore, if we wish to have similar masking capabilities for software faults, we need to use different kinds of software pieces. This method is called N-version programming. N-version programming is problematic because it is expensive and time consuming to produce multiple versions of programs and running multiple versions requires more computing power and memory. Also the voting system needed may be quite complex. N-version programming is mostly used in the most critical solutions such as avionics. N-version programming does not remove problems caused by faulty or poor specification of software, for all pieces of software are made according to that specification and tested against it. Good and unambiguous specification is one of the most critical requirements when producing safe software./12/

Software can also monitor its own functioning or functioning of some other software module. It can perform tests to results of different software functions and determine whether those results are acceptable and software functioning properly. If fault is detected, secondary module can take over or some sort of failure or recovery sequence be started. Problem is that when a fault is detected the software may already have damaged the system, for example by writing faulty values to memory. Therefore some sort of recovery point is needed before software function is run. Again this kind of defensive method requires more computing power and may make already complex software even more complicated. /12/

The standards IEC 61508 and EN 62061 stipulate, that possibility for common-cause failure is to be analysed. In IEC 61508 section 7.6.2.7 it is said that possibility to common-cause failure is to be considered. Safety related systems can be considered independent from each other if they are functionally diverse, based on diverse

technologies, do not share common parts, services or support systems, do not share common operational, maintenance or test procedures and are physically separated in such way that foreseeable failures do not affect redundant safety-related systems and external risk reduction facilities. As it can be seen in mobile work machinery, building completely independent redundant is quite impossible, for the need for example of shared power supply and communication bus. In EN 62061 section 6.7.8.1 requires that possibility of common-cause failure is to be examined. Annex F in EN 62061 helps in determining the risk for common cause failure.

Both standards require some level of redundancy for system to have higher safety integrity levels. In EN 62061 table 5 is shown that system with zero fault tolerance needs safe failure fraction of over 90% to claim higher SIL than 1. Diagnostic coverage, which is a quantity used in EN 62061 to describe performance of system's diagnostics functions, is a factor when determining safe failure fraction and thus effects the highest possible SIL. Diagnostic coverage is also a factor when estimating system's meantime to failure according to EN 62061 and IEC 61508.

These architectural constraints have been under criticism for example by Lundteigen /31/ because they favour systems with high safe failure fractions over systems with high reliability, and it is also possible to manipulate SFF to favour less reliable systems with high diagnostic coverage. However these constraints force designers to add some level of redundancy to their system when high safety integrity is required. Often it is quite expensive to add additional systems to already complex and expensive safety system, but these constraints make it impossible for manufacturer to claim that adding such system would not be sensible due to its high cost.

3.2.1 Architectural constraints

The standards IEC 61508, EN 62061, EN 13849 and ISO 25119 present architectural constraints to safety related systems. The architecture of the system has an effect on how high SIL or PL level system can claim.

There are 5 classes for systems. System's architecture, its diagnostic coverage and meantime to failure are specified fore each class. Classes are illustrated in figures from Figure 14 to Figure 16.

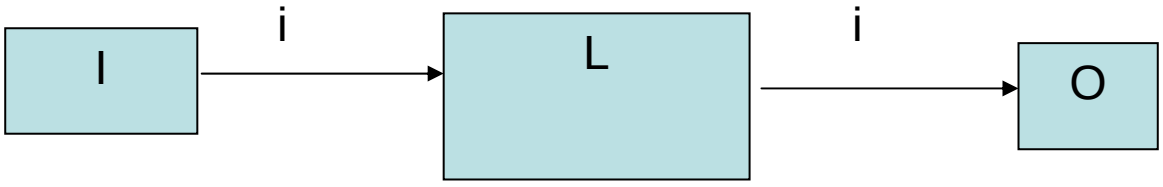


Figure 14 B and 1 system

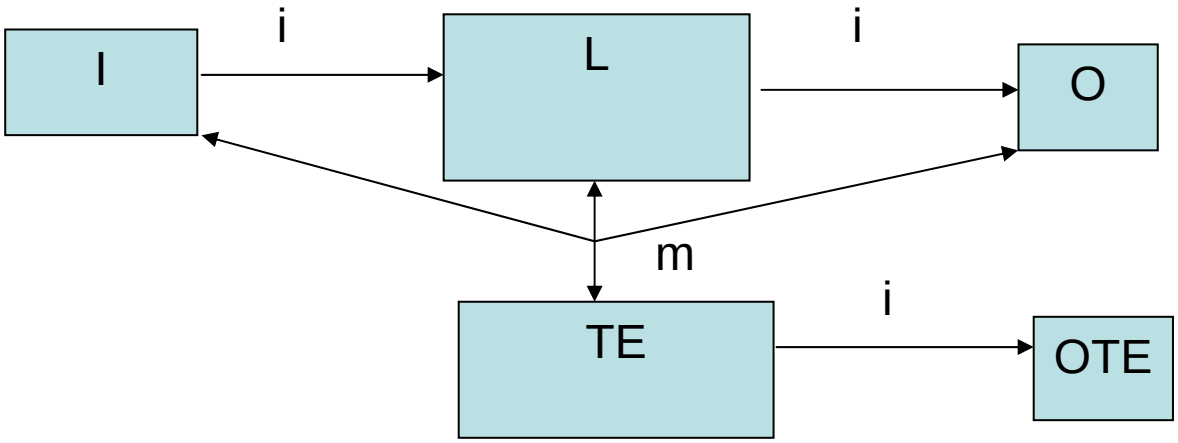


Figure 15 class 2 system

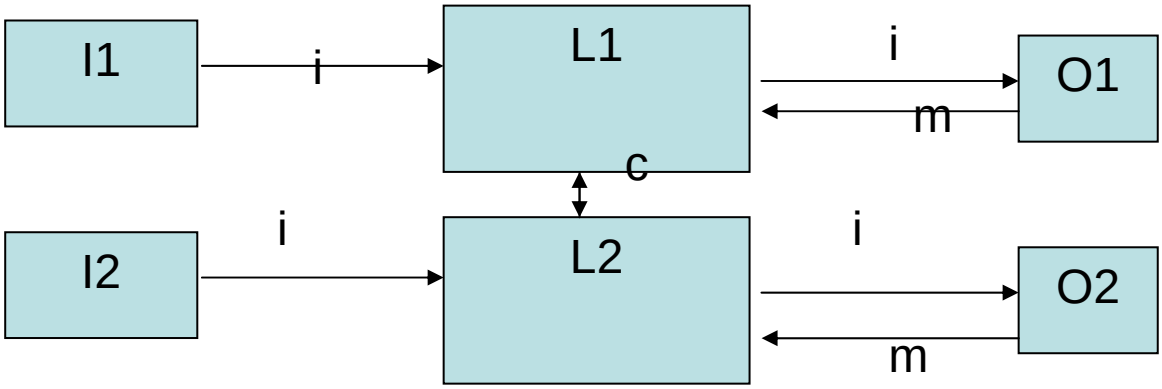


Figure 16 class 3 and 4 system

The following notation is used in Figure 14, Figure 15 and Figure 16:
I = input device
L = logic
O = output device
TE = test equipment
OTE = output of TE
i = interconnecting means
m = monitoring
c = cross monitoring

Class B and 1 systems differ from each other in requirements of DC, MTTF and in quality of used components and techniques. In class 2 system additional testing equipment is added to monitor the functioning of the system. The testing equipment has its own output to indicate failure of the system and to take the necessary precautions to maintain the safety of the system. In class 3 and 4 systems the system is duplicated and the duplicated systems monitor each others functioning. They also monitor their outputs to monitor their own functioning. Classes 3 and 4 differ from each other so that class 4 system has higher requirements for DC and MTTF and in class 4 system accumulation of undetected errors is to be taken into account. In class 2, 3 and 4 possibility of common cause failure is to be taken into account. In tables from Table 7 to Table 9 presented the effect of system class in different standards.

The constraints add redundancy and failure detection to system at the higher levels of safety integrity or performance. A system functioning in a high safety integrity level must be reliable and the system's failures are to be detectable, so that we know when the safe operation is compromised.

Table 7 Relationship between AgPL, system categories and software requirements in ISO 25119

AgPl	Software Requirement Level MTTF					
a	1 Low	B Low	B Low	B Low	B Low	
b	2 Med	1 Med	B Low	B Low	B Low	
c		2 Med	1 Med	1 Low	1 Low	
d				2 Med	2 Med	
e					3 Hi	
	B DC low	1 DC med	2 DC med	3 DC med	4 DC hi	system category (class in EN 13849)

Table 8 Maximum SIL claim for a system containing a subsystem with given SFF according to EN 62061

	Hardware failure tolerance		
Safe failure fraction	0	1	2
<60%	-	SIL 1	SIL 2
60% - < 90%	SIL 1	SIL 2	SIL 3
90% - < 99%	SIL 2	SIL 3	SIL 3
>99%	SIL 3	SIL 3	SIL 3

Table 9 SIL claim limit's relationship to system categories according to EN 62061

Category (EN 13849)	HW fault tolerance	Safe Failure Fraction	Maximum SIL claim limit
1	0	<60%	-
2	0	60 - 90%	SIL 1
3	1	< 60%	SIL 1
		60% - 90%	SIL 2
4	>1	60% - 90%	SIL 3
	1	>90%	SIL 3

There are also other requirements for the system than these presented here, but architectural constraints are one major constraint, when designing a safety-related system.

3.3 Discussion

As it can be seen from the material presented above, safety is a wide and complex issue. The law, viewing just from the machine directive's point of view, is satisfied when machine is safe, and this is shown and proven. The machine directive acknowledges that it is not possible to build completely safe machine. However completely safe machine should be the objective in design. When a machine is safe enough is defined by comparing the machine under inspection to the state of the art. The state of the art is defined by the standards and especially by harmonized standards. One is not obliged to follow these standards, but as the level of technology and the state of the art is defined by them, producing anything less safe than defined by the standards is not really an acceptable deed.

As standards develop so develops the state of the art. One could claim that standards are poor measurement for the state of the art, as they develop slowly and usually drag behind of what could really be done and what is out there at the field. However standards are a commonly accepted reference point of what has been agreed and compromised by a large group of experts. It is well documented and defined so that it can be used as a reference point even in a legal matter. One can not take something that is constantly changing and from where there is many very different versions available, like products in open markets, or something that is not yet completely ready, like things that are done for research purpose. But it should be noted that the state of art is not fixed and that it develops over time. As technology develops and new things come available the level of safety will increase.

One of the most important or the most important phase of developing safe machinery and systems is the risk or hazard analysis. Risk is a product of probability of harmful event and the level of harm. A hazard can only cause harm when human and a hazard exist at the same time and at the same place. Also risk can only exist when these two assumptions are true. /1/ /2/ These are the principles of safety theory. So, to eliminate the risk we simply have to make sure that these two conditions are not true. We can do this by separating human and the hazard or completely removing the other.

Risk analysis is important, because if a risk is not identified, it can not be removed./1/ /5/ Risk analysis also reveals how to get rid of the risk. It is required that the machine is safe throughout its lifecycle from commissioning to de-commissioning and in all its modes of operation, even in faulty ones. Therefore it is important that the analysis is systematic, covers all phases of the lifecycle and all modes of operation. To find the faulty modes of operation, or states and possible risks they pose, tools are needed. One can find all faulty modes of a machine without tools, but this can be very laborious effort, especially when machines become more complex. Also, if proper tools are not used, it is difficult to show and prove, that all faulty modes have been examined, and that all risks are dealt with. The legislation requires that all risks are dealt with or at least there has been the best possible effort to identify and reduce them and proving this without the use of suitable tools is a difficult task.

Risk analysis is also important for it is used to determine the requirements for safety systems. It is interesting to notice that even as the risk analysis is as important as it is, many results of that analysis are based on qualitative methods and engineering judgement. When estimating and evaluating a risk, it is often impossible to use quantitative analysis for there is not enough numerical information available or that data is so unreliable that the quantitative analysis would give no better or accurate results than using qualitative method. Especially at the start of the development process making

accurate analysis is very difficult for there might not be enough information available about the system under development. It is therefore important that the analysis is revised as the system concept and design develops. I personally prefer using qualitative methods that give clearly qualitative results such as risk graph or risk matrix presented in ISO/TR 14121-2. Using quantitative methods is usually laborious, and the source data might be unreliable. Problem with unreliable source data and quantitative method is that the result may be as well unreliable, but the method gives false image of accuracy of the result. Also, using qualitative methods that give results with image of accuracy is something that I would not recommend. In both cases we might get a result of 76 in a scale of one to one hundred. Now how this risk of 76 differs from risk of 75 or 80? Giving an exact result, like 76, gives an image of accurate analysis process, when it necessarily is not. If we use methods that are based on estimations on inaccurate source data then it would be better if we would acknowledge that in our results too, for example by stating that the risk is "high" instead of saying that the risk is 76%. The impact of data uncertainty in determining SIL was also discussed in /34/ .

When considering functional safety and its requirements, it is interesting to notice that the standards regarding functional safety, give quite strict requirements and limits for systems and these requirements are based on a risk analysis which can be based on rather uncertain information.

Because the risk analysis is so important it is necessary and has long reaching effects in the process of making things safe, it is important that it is done properly with enough time and resources and with proper amount of preparation work done.

3.3.1 Safety as a part of development process

The view in the standards examined is that safety is a process. It is not something you add to your product to make it safe, but a way of developing your product so that it becomes safe.

The model of safety process presented in standards IEC 61508 EN 26021 and ISO 25119 can be integrated to the V-model of product development. This way the safety aspect becomes part of the product development instead of something that is added to the product.

There are two aspects in safety and especially in functional safety. One is the functionality i.e. what is done to achieve safety or what is the function. The other is the integrity of that function i.e. how reliable that function is to perform as intended every time it is needed. The process like approach to safety makes it easier to define the functionality of the safety function and also increases the integrity of the function as the function is well defined and understood. Of course the actual development of the safety function also needs to have a well defined development process to achieve the required integrity. Process approach to safety also makes it easier to develop inherently safe devices as the safety of the device and its functions are constantly evaluated throughout the development process. Also the requirement that the machinery is safe throughout its lifecycle is easier to fulfil, as the safety aspect is kept in mind when planning for installation and de-commissioning activities for the machinery.

Main requirements for safety process are that the process is continuous throughout the development of the machine and during its life cycle and that the process evolves so that right tools are used at the right time in the process. Even when the product is released to the market the safety process should continue, for repairs, modification and retrofits of the machine and if undetected hazards are revealed in use they should be reacted to.

Safety analysis should be also adjusted to suitable scope, preliminary estimates of the possible hazards in the early phases, analysis of system failures during the system phase and effects of component failures at the component phase of the development phase, and so on. Thorough safety concept for development of machines is presented in /7/ .

Embedding safety process as a part of the development and other processes within the company may seem like a complicated task, but I believe once the tools and methods have been introduced the safety will become a natural part of these processes and that in the long run it will be beneficial. I believe, that starting to see safety as a process and the attempt to achieve safety through process will force the manufacturers, to take the whole development process into control and will lead to better products as the increased safety often means also increased reliability, quality and usability as well as other RAMS values.

3.3.2 Functional safety in ISOBUS network

It is quite clear that ISOBUS was not designed for safety. However as a CAN-based bus it has quite a few defence mechanisms aimed for high data reliability. I would say that this bus system is not usable for safety critical functions where the risk is high. The main problems for safety related to ISOBUS systems are presented in

Table 10 We can use the ISOBUS network as it is now, if our risk analysis shows that the level of risk that the safety integrity or performance level requirement is so low that ISOBUS would be usable as such or we react to the shortcomings and properties of ISOBUS with other alternative methods.

Table 10 Main problems for safety in ISOBUS network

Fail Silent. A node fails to silent state, sot it is possible that a failure of a node is not detected by other nodes
Execution of a function is not guaranteed.
Safety-critical messages can not be identified and special requirements of safety functions' are not specified. (for example guaranteed execution of a function and locking the machine to desired state access time to the bus ect.)
Lack of definitions for actions in error situations

The other option is, to specify the ISOBUS network attain some performance level or some safety integrity level, as a system. This would require changes and additions to current standard. To my understanding this kind of work is in progress within the ISOBUS community. The white channel approach would be problematic as it would require all the components in the system to be specified to some level and then usability of standard CAN bus components might not be possible. The black channel approach however might be possible, as regular components might be used, but the standard itself would need changes.

My suggestion for improvement of ISOBUS would be that the bus would be duplicated and that safety critical messages would be specified and there would be a way to identify those messages from the bus. Also, we would need to guarantee the access of safety critical messages to the bus. It should also be defined what to do when those messages are received, not received or received with an error. Also, it should be defined, what is to be done, in case of bus failures.

4 Case study

4.1 Introduction to first case study

In this case study we perform safety analysis to a seeding machine. The seeding machine is Maestro 3000 by Junkkari which was modified to be ISOBUS class 3 compliant in MTT's and TKK's FARMIX project. Seeding machine can adjust its working depth and seed and fertilizer flow automatically, it also operates its driveline markers automatically and adjust its lateral location when operated in a slope. These functions can also be remotely operated from a virtual terminal via ISOBUS bus. In this assembly one virtual terminal is located in the cabin of the used tractor. The Tractor used to pull this seeding machine is ISOBUS class 3 compliant prototype tractor by Valtra. The tractor's implement hydraulics can be operated by the implement via ISOBUS. The combination is presented in Figure 17. In a future AGROMASSI project further autonomy will be added to this combination. Tractor is to be changed to a fully ISOBUS class 3 compliant one, a task controller will be added to the ISOBUS bus and the seeding machine will be controlling speed of the tractor, lift itself up during the turnings and to some extent also steer the tractor. Full specification of functions performed by the seeding machine will be ready in early 2010, which is slightly after this study should be finished.

In this study we perform safety analysis according to ISO 12100 standard using tools provided by ISO 14121 standard. We give priority to use part of the product life cycle and to risks related to automation and autonomy of the machine.

Figure 17 The tractor-seed drill combination

The purposes of this study are to walkthrough the safety process and describe and analyse it. One purpose is also to gather information and requirements of safety for further development of the system in AGROMASSI project, and to document the process and safety issues in ISOBUS class3 machinery for ISOturva project.

4.2 Methods

The safety process according to ISO 12100 standard begins by risk assessment. Standard ISO 14121 provides tools and method for performing this risk assessment so that it fulfils requirements presented in ISO 12100.

Risk assessment according to standard ISO 14121 begins with definition of machines limits. Then risks are to be identified, estimated and evaluated. These four parts are also called risk analysis. To risk assessment we also include assessment whether the risk is small enough or has been reduced enough.

ISO 14121 suggests working in group when performing risk assessment /2/ . We decided to organise workshops where different phases of the process were performed, and we also evaluated the work done so far and methods used. Feedback from workshops was used to evaluate the process and also to guide it. Work group, that attended these workshops, comprised of persons who are familiar with the operation of the machine, have been developing or building the machine, are familiar with safety issues and persons who are somewhat familiar with safety process, legislation and standards regarding this type of machinery. This is also the recommended line-up for work groups in section 4.2.2 of ISO 14121-2. In larger projects composition in the group must vary according to the task at hand, and in larger projects it will be necessary to partition the tasks so that not all risks are tried to be identified at one instance.

In first phase of the risk assessment limits of the machine are to be defined. This means that all phases of the machine's lifecycle are to be defined as well as its functions, performance values and human interaction during those phases. Purpose of this phase is to define the machine and region of interest for assessment. In other words: to make a definition of the scope of assessment. Other purpose of this phase is to give good understanding of the machine, its functions and properties for persons assessing it.

Section 5 of ISO 14121-1 requires that limits of use, space time, and other relevant aspects are to be defined. ISO 14121-2 section 5.2 presents' two methods for determining limits of the machine: machine-based and task-based. Machine-based approach is defined as "Describing machine in terms of distinct parts, mechanisms or functions based on its construction and operation." /5/ Task-based approach is defined as: "By considering all persons who interact with the machinery in a given environment, the use of the machinery can be described in terms of the tasks associated with the intended use and the foreseeable misuse of the machinery."/5/ Use of one method does not exclude the use of the other. The method selected for this case was the task-based method. At the start of the process it seemed that this method would require less technical knowledge about the system, that definitions this way could be quicker to make and that it would require less analysis in the later phases.

After limits are defined and identified, hazards can be identified. ISO 14121-1 section 6 requires systematic approach to identify all reasonably foreseeable hazards, hazardous situations and/or events during all phases of product lifecycle./5/ Only after hazards are identified can actions be taken to remove them. For this reason this is the most important

phase of risk assessment and in safety process. All hazards should be listed regardless of their severity or possibility, for significance is estimated later in the process. Listing all imaginable hazards also makes it possible to later show the process of risk assessment for inspection. ISO 14121-2 section 5.3 states that there are many methods for identifying hazards. These methods can be classified as top-down or bottom-up methods. A fault tree is an example of top-down method. In fault tree analysis an identified harm is selected as a top event and then causes leading to top event are examined using logical operations like AND and OR to find the events that lead to possible harm. The failure modes and effects analysis is an example of bottom-up method. In this method we select a possible failure as a top event and then examine using logical operations AND and OR to find out how this fault could lead to harm. In ISO 14121-2 annex A hazards are identified by using forms. ISO 14121-1 annex A has lists of hazards, their sources and their possible consequences. In this case study, found hazards are listed in a form that is an adaptation from form used in ISO 14121-2 annex A (table A.2 in ISO 14121-1). Principles of few popular hazard analyses are presented in Table 11.

Table 11 Principles of some risk analysis methods /54/ /5/

Name of method	For analysis of	Principles of use
HAZOP Hazards and operability	For processes. To discover effects of varying process parameters to process	each parameter is varied according to list of guide words (such as more less none….) and effects of such variations are documented
FTA Fault tree analysis	To find causes for selected failures and hazards	The hazard under inspection is selected as the top event and events leading to that event are mapped in a graphical presentation using logical operators
Event tree analysis	To find consequences of a failure	The possible consequences of a failure and possible path to a hazardous situation is mapped in a graphical presentation using logical operators
Check lists	To check that commonly known hazards and situations are taken into account or that set requirements are fulfilled.	The results of a development phase are compared to the check list
FMEA Failure modes and effects	to find possibly hazardous combinations of failures	Different failure modes of component are combined with failure modes of another component in the system using logical operations and their effects are evaluated

Initially we identify hazard in an open discussion in a group using task-based approach. In this approach the actions of the user and others are being observed and possible hazards identified as the user goes through the normal tasks involving the use of the machine.

After listing the hazards, more general forms of hazards were identified. From a hazard list generated more general hazard cases were identified. Few general hazards were chosen for further analysis.

We used fault tree analysis to these general hazards to gain more knowledge of these hazards. The decision to use fault tree analysis is based on ease of the use this method. It

is easy to learn and require very little, if at all, training. It also produces clear and understandable graphical result and is easy to develop in a group. Information from these analyses can also be used in later phases when estimating and evaluating the risks.

Identified risks are estimated and evaluated using risk matrix method presented in annex A of ISO 14121-2. Same method is used in IEC 61508 and in EN 62061 to determine required SIL for control system. In this method each risk is given grades in four fields: severity, frequency, probability and avoidance. Severity is a factor in matrix in its own, and grades in frequency, probability and avoidance are summed to form the other factor in this matrix. The used matrix is shown in Table 12 and values for frequency, probability and avoidance are given in Table 13. Risks for estimation were chosen by the author and selections were approved in the workgroup. Risks selected for estimation were graded in the workgroup.

Also other estimation and evaluation methods were performed to compare methods. These other methods are a risk graph method from ISO 14121-2 and EN 13849 and matrix-graph hybrid from ISO 25119 draft.

Table 13 Risk estimation parameters from ISO 14121-2. This method was chosen for it is clearly qualitative in its nature. No exact values are used to describe any aspect of the risk. The result of this estimation method is not clearly visible when grading is done, so estimation can be more honest than when using for example risk graphs where seeing the results may have an effect on grading. A qualitative method is desired at this phase as there is not enough information to perform quantitative estimation. If such estimation was made, the initial values would have to be based on so called engineering judgement which are no better in quality than qualitative estimates.

Table 12 Risk matrix used in risk evaluation. A hybrid of table A3 in ISO TR 12141-2 and table A6 in EN 62061

Severity (Se)	Class (Cl)				
	3-4 remote	5-7 unlikely	8-10 possible	11-13 likely	14-15 very likely
4 catastrophic	low 3	low 3	medium 2	high 1	high 1
3 serious	negligible 4	low 3	medium 2	high 1	high 1
2 moderate	negligible 4	negligible 4	low 3	medium 2	high 1
1 minor	negligible 4	negligible 4	negligible 4	low 3	medium 2

Risks for estimation were chosen by the author and selections were approved in the workgroup. Risks selected for estimation were graded in the workgroup.

Also other estimation and evaluation methods were performed to compare methods. These other methods are a risk graph method from ISO 14121-2 and EN 13849 and matrix-graph hybrid from ISO 25119 draft.

Table 13 Risk estimation parameters from ISO 14121-2

Frequency	2 Interval between exposure > 1a	3 Interval between exposure >2 weeks	4 Interval between exposure > 1d	5 Interval between exposure > 1h	6 Interval between exposure < 1h
Probability	1 Negligible	2 Rarely	3 Possible	4 Likely	5 Very high
Avoidance	1 Likely	3 Possible	5 Impossible		

4.3 Results

Definition of the machine and its limits was done in a group using task-based method. The tasks and actions performed during those tasks and the state of the tractors and implements systems were gathered into a form. In addition to this form there was seed drill's user manual and a set of photographs at the group's disposal and many members of the group had used or had been involved in the development of the machine combination. The description table is attached to appendix IV.

Hazards were identified using task-based approach described in section 4.2 and in ISO 14121. Results were gathered to a form that is an adaptation of a form model in ISO 14121. Form is attached to appendix II.

Four more general types of automation related hazards were identified. These are:

- Impact from the implement due to unexpected movement.
- Impact from falling driveline marker.
- Bystander being run over by the machine.
- Machine falling over in field/road.
- Machine falling from field/road

A fault tree analysis was performed for these hazards; fault trees generated are attached to appendix I.

The risk of being hit by falling driveline marker was selected as an example risk for this case. In this accident scenario the operator is about to refill the seed or fertiliser container in the seed drill. He, for some reason, leaves the seed drill in automated state and lifts the machine up. The automation system now thinks that the operator is doing a turn and waits for a signal from the seed drill position sensor to begin a new run. As the operator fills the containers, the weight of the drill increases and it may lower seed drill's position just enough to trigger the automation to think that a new run has begun and it lowers a driveline marker. The FTA found this risk by first asking: what are possible reasons, which could cause the driveline marker to come down?". One answer was that control system gives the command to lower a driveline marker. Then a question was asked "what causes the control system to lower a driveline marker?" and so on. A driveline marker is highlighted in Figure 18.

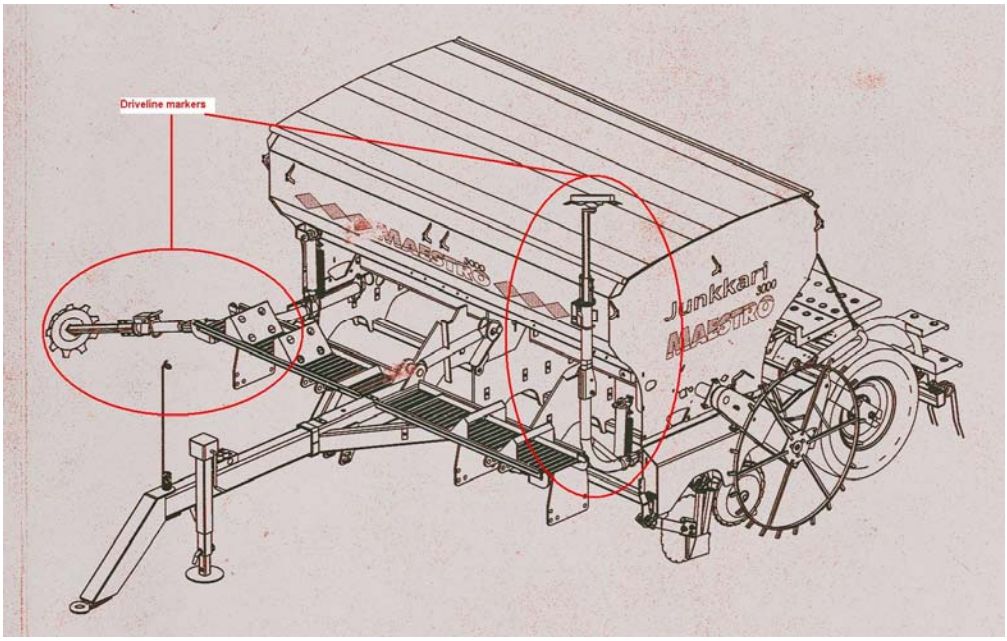


Figure 18 The seed drill and its driveline markers

Risk of being hit by a falling driveline marker was selected for estimation and evaluation. The workgroup used the result of the fault tree analysis and hazard list to estimate the risk.

In risk matrix method the risk is ranked in four categories:

- Severity (Se)
- Frequency (Fr)
- Probability (Pr)
- Avoidance (Av)

A grade is given in each category. Grades and their definitions are from ISO 12141-2 and are presented in tables.

Grades given for this risk by the workgroup are as follows

- Severity 4 (death)
- Frequency 5 (approx once every 2½hours of work)
- Probability 3 (possible)
- Avoidance 5 (impossible)

The Class of the risk is calculated as /5/

$$Cl = Fr + \Pr + Av \qquad (1)$$

And the result is 13 which corresponds to “likely” (A.3) or “probable” (A.4). Class and severity placed in the risk-matrix gives result of category one in a scale of one to four, one being the most severe or “high”. This brings us to a conclusion that the risk is intolerable by any standard and needs to be reduced.

Three solutions to reduce or remove the risk associated with the driveline markers were presented in the workshops. The first solution was to remove the driveline markers. Second solution was to add a safety-device to monitor the operation area of the driveline marker and to block the operation of the driveline marker either by using a separate

locking device or via software. The third solution was to define the state of the machine when the driveline marker is allowed to operate. It was analysed that the hazard only presented itself when the tractor and the seed drill was not on normal work operation, but was standing still and people needed to work around or walk by the machine. Therefore, if we define the states where the driveline marker may operate, we could lock the driveline marker in all other states either by locking device or locking via software. These solutions are illustrated in Figure 19 and in Figure 20 and they are our safety concepts for solving this hazard.

Removing the driveline markers would be the best solution for it would remove the risk completely and would be the inherently safe solution. Removing the driveline marker would be possible, as with the help of automation and driver assistance systems, it would be possible to work in field as efficiently as with the traditional mechanical driveline markers. However, as it will be necessary to couple the seed drill to tractors without such assistance systems and as with this particular machine ,the driveline marks were to be used in other research projects and for the sake of exercise it was decided that it is not possible to remove the driveline markers and other options were to be considered.

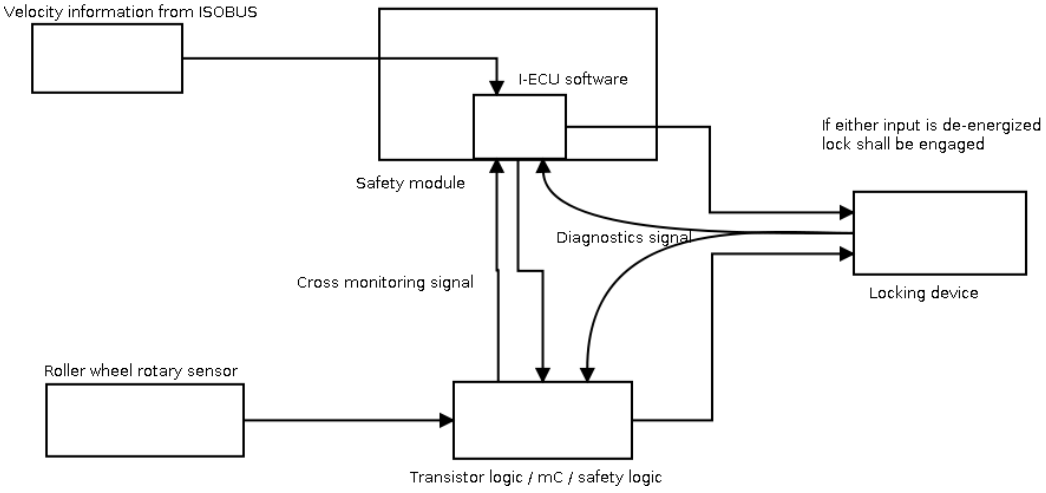


Figure 19 A SRS preventing the movement of driveline markers with a locking device

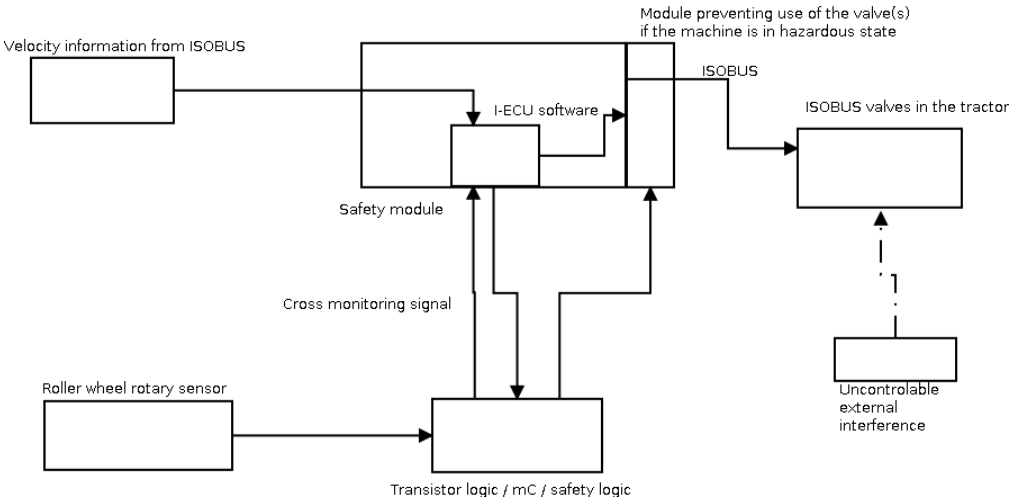


Figure 20 A SRS preventing the movement of the driveline marker with a software lock

The second and the third solution need to be implemented in the control system of the seed drill. To develop such system a requirement must be set for this system.

In IEC 61508 the safety integrity level is determined using a risk matrix similar to the one used previously when estimating and evaluating the risk. The result using parameters defined earlier is SIL 3. In EN 13849 requirement of performance level is defined using risk graph, similar to the one used earlier in estimation and evaluation of the risk. The result using the same parameters defined earlier gives a result of PL d. The graph-matrix hybrid in ISO/DIS 25119 draft provides as well AgPL of d.

Safety integrity requirements defined would set following requirements for the system. A duplicated system with cross monitoring is required. Other requirements for the system according to ISO/DIS 25119 would be MTTF_dC of “medium” DC of “medium” and Software Requirement Level of 2, or better. From the Table 14 we can see the required levels of probability of dangerous failure per hour for continuous mode of operation or the average probability of failure to perform on demand for low demand mode of operation, set in IEC 61508. Our safety-system works in low demand mode, but the system may have components that have to function in continuous mode, like the sensing devices, that monitor either the state of the machine or the operation area of the driveline marker.

Table 14 SRS performance requirements according to IEC 61508

SIL	Low demand mode of operation	Continuous or high demand mode of operation
1	$\geq 10^{-2}\ to < 10^{-1}$	$\geq 10^{-6}\ to < 10^{-5}$
2	$\geq 10^{-3}\ to < 10^{-2}$	$\geq 10^{-7}\ to < 10^{-6}$
3	$\geq 10^{-4}\ to < 10^{-3}$	$\geq 10^{-8}\ to < 10^{-7}$

From Table 7, Table 8 and Table 9 we see, that according to IEC 61508, our system must have safe failure fraction of over 99% with hardware tolerance of zero, SFF of over 90% with hardware failure tolerance of 1 and SFF of over 60% wit hardware tolerance of 2. Corresponding requirements when comparing to system categories specified in EN 13849 are SFF of over 90%with category 4 system with hardware failure tolerance of 1 or SFF of over 60% with hardware failure tolerance of over 1 and with category 4 system. From category requirements in EN 13849 we get requirements for DC and MTTF_dC, and for category 4 system they are DC high and MTTF_dC high. The requirements set by EN 13849 for PL 4 system are however slightly looser. EN 13849 requires category 3 system with DC medium and MTTF_dC medium or category 3 system with DC low and MTTF_dC high or category 2 system with DC medium and MTTF_dC high.

4.4 Discussion

Identifying the limits of the machine was a difficult part in this process. The definition what we mean by the limits of the machine is a bit obscure. Also inexperience with the safety analysis process makes it more difficult to know what is relevant information for the future process. In this part one must also state much of obvious information which for some participants might be so obvious that stating that information might seem unreasonable. But if we define one goal of this part of the process is to give all participants of the safety analysis process, and also for person reviewing the process afterwards, a common view and understanding of the machine under observation, then it

is necessary to state all relevant matters even if they seem unnecessary for a person with experience of that machine. In this phase it might be a good idea to gather a good information package of the machine to which the actors in the safety analysis process can refer to during their work. This information package can then be included in the technical file required by the machine directive.

Identifying hazards is stated to be the most important part of the process in many instances in this text. We went through this phase using task-based approach. In this process we walked through the tasks that operator must take when operating the machine. The first observation was that we did not discuss much about the use of the machine in the phase of identifying limits of the machine, but focused a bit more on the technical details of the machine. The second observation was that we tend to evaluate the hazards and filter out the more minor risks or try to find solutions for them already in this phase. It is important to list all hazards that are found, even if they seem to be really minor. In the later phases it can be then stated that the risks are negligible. An identification process, where even the minor risks are identified, is a sign of a systematic and thorough approach. It is also possible, that some hazards, that seem to be negligible, are actually something that requires more attention. Also, finding many minor hazards in some function of the machine, might be a sign that there is something wrong with the design of that function. The information about the minor hazards is also valuable information in future development as points of improvement. We made a conscious decision not to list minor hazards caused by mechanical and structural components, such as getting minor cuts and bruises from sharp edges when doing service work and minor hazards from low voltage electrical system. We wanted to focus on the risks caused by or related to the automation and there would have been too many minor hazards of those types.

Identifying hazards was done in one three-hour workshop session and it turned out that this was too short of a session. This kind of machine has many phases in its cycle of use, from connecting and coupling of the machine to calibration, setting, transfer, filling to use in field. We also intentionally left out other phases of the lifecycle such as installation, commission and de-commission, for right now we have interest in the risks during the use of the machine. As this is an important phase of the safety process it is important that enough time is reserved for this phase of the process. Personally I would recommend that the identification of the hazards would continue trough the whole lifecycle of the product.

Approximately 50 hazards were identified in the workshop. It is clear that large number of hazards will be identified. Therefore, there is a need for a system to store and to collect identified hazards. For simpler products and smaller projects set of forms or spreadsheets might be enough, but when machines and projects become more and more complex, some sort of database setting is necessary. A well organised database will also be a valuable source of information in future development projects. This database would also serve as a part of the technical file required.

The result list of identified hazards was compared to the list of possible hazard sources listed in table A.1 of ISO 14121-1. From this comparison it was clear that there would be a large amount of possible minor hazards that were neglected from the identification process.

From the hazard list it is possible to find common types of hazards and common sources of hazards. Eliminating this common source will eliminate a huge amount of hazards and, therefore, making a proper identification of hazards where even the minor hazards are identified is beneficial. Identified common types of hazards were:

- Impact from the implement due to unexpected movement.
- Impact from falling driveline marker.
- Bystander being run over by the machine.
- Machine falling from field/road.
- Machine falling over in field/road

It was noted that unexpected movement could also cause many minor harms.

It was noted soon that when using chosen approach, fault tree analysis, to identify hazards as planned originally was not applicable. This was because the task-based approach gives quite detailed accident scenario and this approach also gives a lot of risk scenarios which might be just slight variations of each other. So using analysis or identification method that goes quickly into detail is more useful on more general hazards. Fault tree analysis was applied to identified common type hazards. It was noted that the analysis went quickly to technical details of the machine and its systems, so information about machine's systems is needed to do this analysis. In this case not much information was available. So in early phases of development it is not beneficial to go too much in detail in the first steps of development, but to continue analysis later when more information becomes available. From the analysis it is possible to get requirements for development and the analysis reveals points in system where special attention is needed. The analysis also clarifies the risk. It reveals different factors in the risk and their relations to each other. This analysis also reveals quickly solutions for identified problems. As with the identification process I would recommend continuation in this analysis process, in which this analysis would be updated as development progresses and more information becomes available.

D. Seward et al mentioned in their paper Safety analysis of autonomous excavator functionality similarly that FTA goes quickly into detail and this should be avoided if we wish to gain general information and requirements for the system development./33/ They also concluded that, if we wish to gain general or generic information from the risk scenario, we should also select the top event to be as general as possible to avoid narrowing our scope of inspection. Overall FTA was experienced in a work group as useful and informative tool.

We evaluated the risk of being hit by falling driveline marker in a work group using risk matrix presented in ISO/TR 14121-2. The FTA was found to be a useful aid when determining the parameters for the matrix. The risk matrix was very quick to use once the parameters were determined, finding credible parameters might how ever be quite difficult especially if the system is very complex and many uncertain factors need to be considered. Data uncertainty is one recognised problem in risk analysis. This problem is for example addressed by Wang et al /34/

Other evaluation methods were found to give similar results and to use similar parameters. One interesting point that was discovered was that these evaluation methods are quite stiff. For the evaluation result to change one or more of the parameters need to change quite dramatically. It can be noted that the parameters are also selected so that the right methods for risk reduction are favoured. Reducing severity of the harm reduces the evaluation result quickly and this favours inherently safe design and improving avoidability reduces evaluation result just slightly. Other example of the stiffness is that when the same risk was re-evaluated after implementing the safety system. All parameters stayed the same except the probability (Pr) of the risk which was reduced

from the original 3 to lowest 1. So the class is reduces from 13 to 11 and the result of evaluation will still give the risk level of “high”.

The result of the evaluation was quite a surprise for the work group as without the evaluation method the risk was estimated to be much smaller. Also engineering judgement is needed when the effectiveness of risk reduction is considered.

The two safety concepts given are examples of possible systems to reduce the risk. How these systems would be implemented is not considered, but they demonstrate the requirements that are required from the system and problems that need to be solved to implement the system. The examples take different approaches to demonstrate possible solutions to the problem and to show what kind of problems there are in different approaches. The solution for implementation might just as well be a hybrid between the given examples. The solution based on a locking device can be implemented independently from the tractor so that no resource is needed from the tractor or so that the safety function performed if a fault occurs in required resource. On the down side system based on a locking device needs the physical locking device which adds to the component and assembly costs of the implement. The software lock approach, on the other hand, does not necessarily need any new components, but it needs to use the ISOBUS network and tractor resources and therefore we would need some kinds of guarantees that we can perform the required function. Now there exists a possibility that for example a message requesting that function is for some reason is not received or for some reason some other node in the network overrides the requested function. Also, there is no redundancy in the ISOBUS system as it is requested by the architectural constraints. The probability for failure to happen in ISOBUS system is very low, but in safety and especially in cases, where the failure of safety would lead to serious injuries or loss of life the requirements are set to be very strict and therefore all possible failures are to be considered. The ISOBUS network can be used if the function can be guaranteed and the loss of that function can be detected.

As we first tried to acquire some kind of definition of the level of safety for our existing machine, we realized that it is very difficult or even impossible to apply IEC 61508, EN 62061 or ISO/DIS 25119 to existing design, especially if there is no rigorous documentation of the development process available. This is because these standards do not regerd safety as something that the machine has, but as something that is designed and built into the machine.

5 Discussion and conclusions

The key to design of safe machinery is in the process of the design and the management of the design process and safety. We begin by identifying the possible hazards and then we analyse and evaluate them. From our evaluation we then decide whether the risks related to identified hazards need to be reduced. Then, with the help of our analysis we create a plan to reduce that risk if necessary. First mean of risk reduction is inherently safe design, which is elimination of the hazard or reducing its risk. Second mean is the use of protective measures, which is preventing humans from being in a hazardous area at the time, when the hazard occurs. The last mean is instructional and organisational means, which do not reduce the actual risk, but it is hoped that increased information will add the awareness of people around the machine and help them avoid hazardous situation. The plan for risk reduction is to be re-analysed to be sure that no new risks are created. These are also requirements of the machine directive and ISO 12100 standard.

Once we have created a plan for safety, we need to make sure that this plan is implemented properly in design and realization of the machine. To do this, several different standards are available. When the plan involves the use of a (electronic) control system there are three standards available (EN 13849 EN 62061 IEC 61508) and for agriculture the ones mentioned above and a fourth one (ISO/DIS 25119). From these standards we can choose the one that fits best our development process and to the needs of our application.

In functional safety there are two aspects. First aspect is the function itself. What does a safety function or system do? What is the risk scenario, what is the equipment where this function is used? How does our function reduce the risk and how much? These define the functionality part of the system and they are to be defined by the manufacturer himself, with the help of hazard identification and analysis. The second aspect is the integrity of the function. From the hazard analysis we get a requirement for integrity of this function. That integrity requirement of the function then gives us the requirements for technical aspects of the system and not just the technical aspects but also requirements for the development of the system. These requirements are set in the standards.

For the development to be smooth and effective I believe that the process for safety has to be continuous and iterative. It should run parallel with the development process and evolve as the development and the process evolves.

In agricultural tractor-implement combinations the implements use tractor’s resources or functions to operate. The ISOBUS network allows implements to use tractor’s resources independently and allow highly automated and autonomous functions. From the safety and functional safety point of view I see three main problems in such systems.

The first problem is design of safe machinery and ECUs. The tractors and the implements need to be designed to be safe. The safety can be achieved using the safety process described in ISO 12100 or some other similar kind of method. For functional safety we can use some suitable standard. The implements need to use resources of the tractor to perform functions and when a function is needed they need to use the ISOBUS network. This leads us to the second problem.

The second problem is the use of ISOBUS network in safety-related communications. Is it feasible to utilize ISOBUS network in safety functions. This is more of a technical problem. My view is that it can not be used as such, but with improvements it could be used. There is work in progress in ISOBUS consortium to develop a system which could be used to in safety-related communications.

The third problem is a larger one that lies at the system level. I call it the *problem of division of responsibilities*. Can we trust the functions of the other machine? The ISOBUS standard lacks any definition for integrity of requested functions or guarantees for that function to be performed. What is the responsibility of the tractor to perform requested function, and what is the responsibility of implement to send safe functions? This is a larger problem, that will need further inspection and discussion within the industry. I am not sure whether these are questions to be answered in the ISOBUS standard. The standards for the connection and interface between the tractor and implement are rather old and it might be a good idea to review this connection and bring it to a new level, where high level of automation is taken into account. This would include the coupling, positioning, power transfer, power control, data communications, functions and other resources needed in use of tractor-implement combinations. My suggestion to the division of responsibilities problem is that we would define a set of functions for the tractor, which would be guaranteed to be performed with certain integrity. These functions could then be used as a part of a safety function. Now the design of the safety function is left to the responsibility of the implement manufacturer.

Higher level of automation is needed in this world to produce more food to the needing people, efficiently, affordably and sustainably. However the new highly automated farming machinery can not be any less safe than the ones that are in use now. The safety is a complex matter, but there are tools to manage it and methods to create safe machinery. The lack of safety or the lack of development is not acceptable with excuses that this safety-thing would be expensive or difficult.

6 References

/1/ SFS-EN ISO 12100-1:2003 Koneturvallisuus. Perusteet ja yleiset suunnitteluperiaatteet. Osa 1: Peruskäsitteet ja menetelmät. Suomen standardoimisliitto SFS 2003 (Safety of machinery. Basic concepts, general principles for design. Part 1: Basic terminology, methodology)

/2/ SFS-EN ISO 12100-2:2003 Koneturvallisuus Perusteet ja yleiset suunnitteluperiaatteet. Osa 2: Tekniset periaatteet Suomen standardoimisliitto SFS 2003 Safety of machinery. Basic concepts, general principles for design. Part 2: Technical principles)

/3/ SFS-IEC 61508-1 Sähköisten/elektronisten/ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus. Osa1: Yleiset vaatimukset. Suomen standardoimisliitto SFS 2000 (Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 1: General requirements)

/4/ SFS-EN 62061 Koneturvallisuus. Turvallisuuteen liittyvien sähköisten, elektronisten ja ohjelmoitavien elektronisten ohjausjärjestelmien toiminnallinen turvallisuus. Suomen standardoimisliitto SFS 2005 (Safety of machinery. Functional safety of safety-related electrical, electronic and programmable electronic control systems)

/5/ SFS-EN ISO 14121-1:fi Koneturvallisuus. Riskin arviointi. Osa 1: Periaatteet. Suomen standardoimisliitto SFS 2009 (Safety of machinery. Risk assessment. Part 1: Principles)

/5/ ISO/TR 14121-2:fi Koneturvallisuus. Riskin arviointi. Osa 2: Käytännön opastusta ja esimerkkejä menetelmistä. Suomen standardoimisliitto SFS 2009 (Safety of machinery. Risk assessment. Part 2: Practical guidance and examples of methods)

/6/ Marita Hietikko, Timo Malm & Jarmo Alanen. Koneiden ohjausjärjestelmien toiminnallinen turvallisuus. Ohjeita ja työkaluja standardien mukaisen turvallisuusprosessin luomiseen [Functional safety of machine control systems. Instructions and tools for the creation of standard safety process]. Espoo 2009. VTT Tiedotteita . Research Notes 2485. 75 s. + liitt. 14 s. ISBN 978-951-38-7298-4 (URL: http://www.vtt.fi/publications/index.jsp)

/7/ Tiusanen, Risto, Hietikko, Marita, Alanen, Jarmo, Pátkai, Nina & Venho, Outi. System Safety Concept for Machinery Systems [Järjestelmäturvallisuuskonsepti työkonejärjestelmien riskien hallintaan]. Espoo 2008. VTT Tiedotteita . Research Notes 2437. 53 p. ISBN 978-951-38-7215-1 (URL: http://www.vtt.fi/publications/index.jsp)

/8/ Alanen, Jarmo, Haataja, Kari, Laurila, Otto, Peltola, Jukka & Aho, Isto. Diagnostics of mobile work machines. Espoo 2006. VTT Tiedotteita . Research Notes 2343. 122 p. ISBN 951.38.6799.4 (URL: http://www.vtt.fi/publications/index.jsp)

/9/ Alanen, Jarmo, Hietikko Marita & Malm, Timo. Safety of digital communications in machines. Espoo. VTT Tiedotteita – Research Notes 2265. 93p + app 1p. ISBN 951-38-6503-7

/10/ Hietikko, Marita, Alanen, Jarmo & Tiusanen, Risto. Työkoneiden ja automaation CAN-väyläsovellusten turvallisuus [The Security of CAN bus applications in working machines and automation]. Espoo 1996, Valtion teknillinen tutkimuskeskus, VTT Tiedotteita – Meddelanden – Research notes 1745. 100s. +liit. 1s. ISBN 951-38-4900-7

/11/ Safety and reliability. Technology theme . Final report. Ed. by Veikko Rouhiainen. Espoo 2006. VTT Publications 592. 142 p. + app. 27 p. ISBN 951.38.6697.1 (URL: http://www.vtt.fi/publications/index.jsp)

/12/ Storey Neil. Safety-Cirtical Computer Systems. Addison Wesley Longman 1996 ISBN 0-201-42787-7

/13/ Jacobson Jan, Johansson Lars-Åke, Lundin Magnus. Safety of Distributed Machine Control Systems. Swedish National Testing and Research Institute SP-Rapport 1996:23. 1996 ISBM 91-7848-628-9

/14/ Jacobson Jan, Johansson Lars-Åke, Lundin Magnus, Larsson Hanna. Safety of Distributed Machine Control Systems, Validation Methods Swedish National Testing and Research Institute SP-Rapport 1998:24. 1998 ISBN 91-7848-730-7

/15/ Viljanen Aarre. Koneiden turvallisuussuunnittelun perusteet standardissa EN ISO 12100 – Miten EN 292 muuttui ja standardin kansainvälistymisen seuraukset. Tekninen Tiedotus 5/2004 Teknologia teollisuus ry ISBN 951-817-843-7

/16/ Sundquist Matti (ed.) Teollisuusautomaation tiedonsiirtoliikenne Turvaväylät. Inspecta Koulutus oy 2008 ISBN 978-951-98254-3-4

/17/ ISO11783-1:2007 Tractors and machinery for agriculture and forestry- Serial control and communications data network – Part1: General standard for mobile data communication. Suomen Standardoimisliitto SFS 2007

/18/ ISO11783-2:2007 Tractors and machinery for agriculture and forestry- Serial control and communications data network – Part2: Physical layer. Suomen Standardoimisliitto SFS 2007

/19/ ISO11783-3:2007 Tractors and machinery for agriculture and forestry- Serial control and communications data network – Part3: Data link layer. Suomen Standardoimisliitto SFS 2007

/20/ ISO11783-4:2007 Tractors and machinery for agriculture and forestry- Serial control and communications data network – Part4: Network layer. Suomen Standardoimisliitto SFS 2007

/21/ ISO11783-5:2007 Tractors and machinery for agriculture and forestry- Serial control and communications data network – Part5: Network management. Suomen Standardoimisliitto SFS 2007

/22/ ISO11783-6:2007 Tractors and machinery for agriculture and forestry- Serial control and communications data network – Part6: Virtual terminal. Suomen Standardoimisliitto SFS 2007

/23/ ISO11783-7:2007 Tractors and machinery for agriculture and forestry- Serial control and communications data network – Part7: Implement messages application layer. Suomen Standardoimisliitto SFS 2007

/24/ ISO11783-8:2007 Tractors and machinery for agriculture and forestry- Serial control and communications data network – Part8: Power train messages. Suomen Standardoimisliitto SFS 2007

/25/ ISO11783-9:2007 Tractors and machinery for agriculture and forestry- Serial control and communications data network – Part9: Tractor ECU. Suomen Standardoimisliitto SFS 2007

/26/ ISO11783-10:2007 Tractors and machinery for agriculture and forestry- Serial control and communications data network – Part10: Task controller and management information system data interchange. Suomen Standardoimisliitto SFS 2007

/27/ ISO11783-11:2007 Tractors and machinery for agriculture and forestry- Serial control and communications data network – Part11: Mobile data element dictionary. Suomen Standardoimisliitto SFS 2007

/28/ ISO11783-12:2007 Tractors and machinery for agriculture and forestry- Serial control and communications data network – Part12: Diagnostics services. Suomen Standardoimisliitto SFS 2007

/29/ ISO11783-13:2007 Tractors and machinery for agriculture and forestry- Serial control and communications data network – Part13: File server. Suomen Standardoimisliitto SFS 2007

/30/ Robyn R. Lutz. Software Engineering for Safety: A Roadmap. Finkelstein (ed.) The Future of Software engineering. ACM Press 200 ISBN 1-58113-253-0

/31/ Lundteigen, Rausand. Architectural constraints in IEC 61508: Do they have the intended effect? Reliability Engineering and System Safety 94. 2009

/32/ Ehrl, Auernhammer. X-By-Wire via ISOBUS Communication Network. Agricultural Engineering International: the CIGR Ejournal. Manuscript ATOE 07 002. Vol. IX. July, 2007

/33/ Seward, Pace, Morrey, Sommerville. Safety analysis of autonomous excavator functionality. Reliability Engineering and System Safety 70. 2000

/34/ Wang, West, Mannan. The impact of data uncertainty in determining safety integrity level. Process Safety and Environmental Protection 82. 2004

/35/ Möller, Hansson. Principles of engineering safety: Risk and uncertainty reduction Reliability Engineering and System Safety 93 2008

/36/ Valtioneuvoston asetus koneiden turvallisuudesta 12.6.2008/400

/37/ Laki eräiden teknisten laitteiden vaatimuksenmukaisuudesta 26.11.2004/1016

/38/ Laki kulutustavaroiden ja kuluttajapalvelusten turvallisuudesta 30.1.2004/75

/39/ EUROOPAN PARLAMENTIN JA NEUVOSTON DIREKTIIVI 2006/42/EY, annettu 17 päivänä toukokuuta 2006, koneista ja direktiivin 95/16/EY muuttamisesta (uudelleenlaadittu)
(ETA:n kannalta merkityksellinen teksti) EC directive 2006/42/EC

/40/ EUROOPAN PARLAMENTIN JA NEUVOSTON DIREKTIIVI 2003/37/EY, annettu 26 päivänä toukokuuta 2003, maatalous- tai metsätraktoreiden, niiden perävaunujen ja vedettävienvaihdettavissa olevien koneiden ja näihin ajoneuvoihin tarkoitettujen järjestelmien, osien ja erillisten teknisten yksiköiden tyyppihyväksynnästä sekä direktiivin 74/150/ETY kumoamisesta (ETA:n kannalta merkityksellinen teksti) EC directive 2003/37/EC

/41/ ISO/DIS 10975 Tractors and machinery for agriculture – Auto-guidance systems – Safety requirements. Draft standard 2008

/44/ ISO/DIS 25119-1 Tractors and machinery for agriculture and forestry – Safety-related parts of control systems – Part1: General principles for design and development. Draft standard 2008

/45/ ISO/DIS 25119-2 Tractors and machinery for agriculture and forestry – Safety-related parts of control systems – Part2: Concept phase Draft standard 2008

/46/ ISO/DIS 25119-3 Tractors and machinery for agriculture and forestry – Safety-related parts of control systems – Part3: Series development, hardware and software Draft standard 2008

/47/ ISO/DIS 25119-4 Tractors and machinery for agriculture and forestry – Safety-related parts of control systems – Part4: Production, operation, modification and supporting processes Draft standard 2008

/48/ Komission lausunto, annettu 27 päivänä toukokuuta 2008, Euroopan parlamentin ja neuvoston direktiivin 98/37/EY 7 artiklan soveltamisesta Suomen viranomaisten toteuttamaan HARVERI-merkistä pienharvesteria koskevaan kieltotoimenpiteeseen MD-2007-144

/49/ Hedley D. The testing of real-time embedded software by dynamic analysis techniques. Daniels B.K.(ed.) Safety of Computer Control Systems 1990

(SAFECOMP'90) Safety, Security and Raliability Related Computers for the 1990s Proceedings of the IFAC/EWICS/SARS Symposium Gatwic, UK, 30 October – 2 November 1990. IFAC Symposia Series 1990 Number 17 ISBN 0-08-040953-9

/50/ Valtioneuvoston päätös N:o 856. työssä käytettävien koneiden ja muiden työvälineiden hankinnasta, turvallisesta käytöstä ja tarkastamisesta. Annettu Helsingissä 25 päivänä marraskuuta 1998

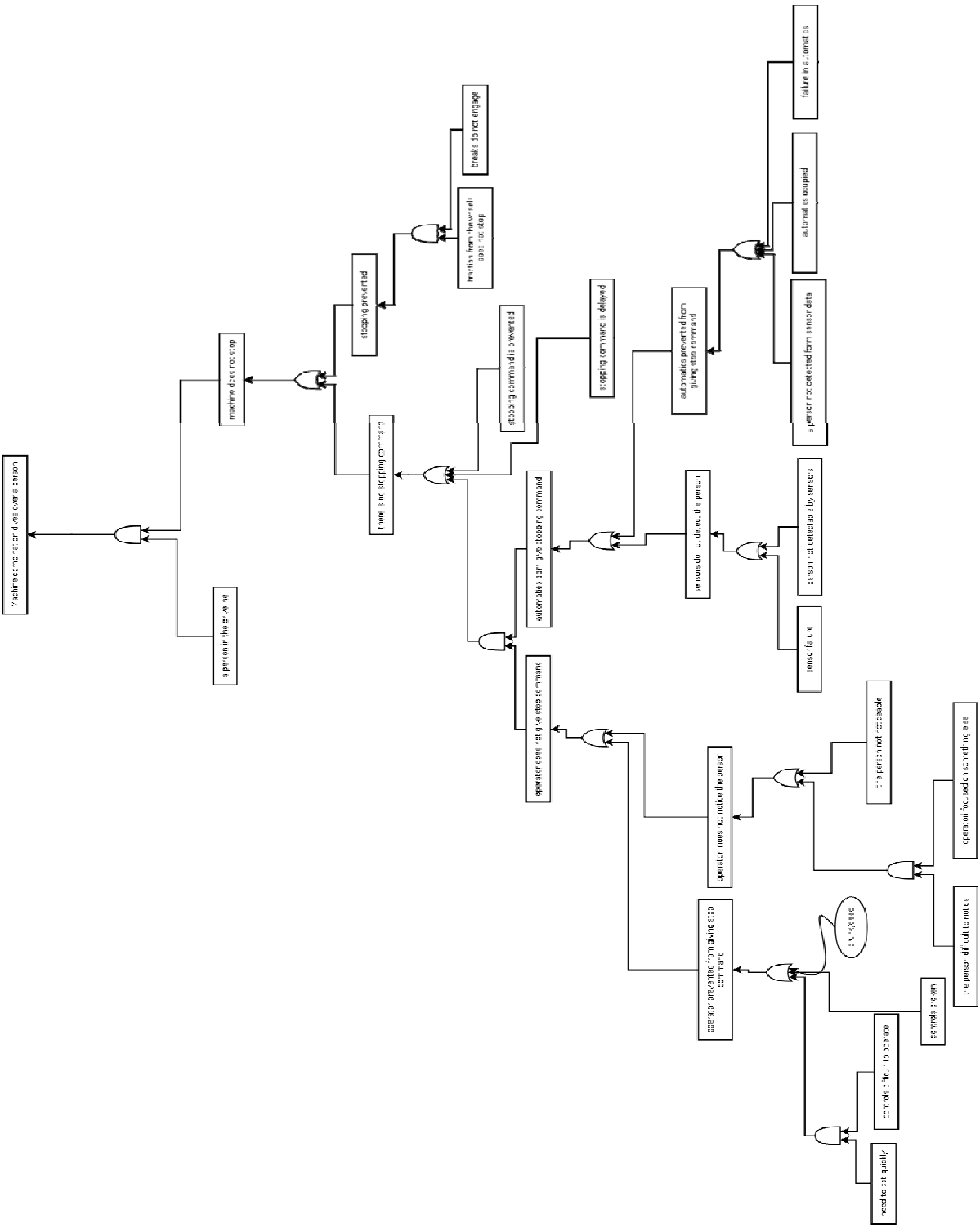
/51/ Web page www.flexray.com visited 20.11.2009

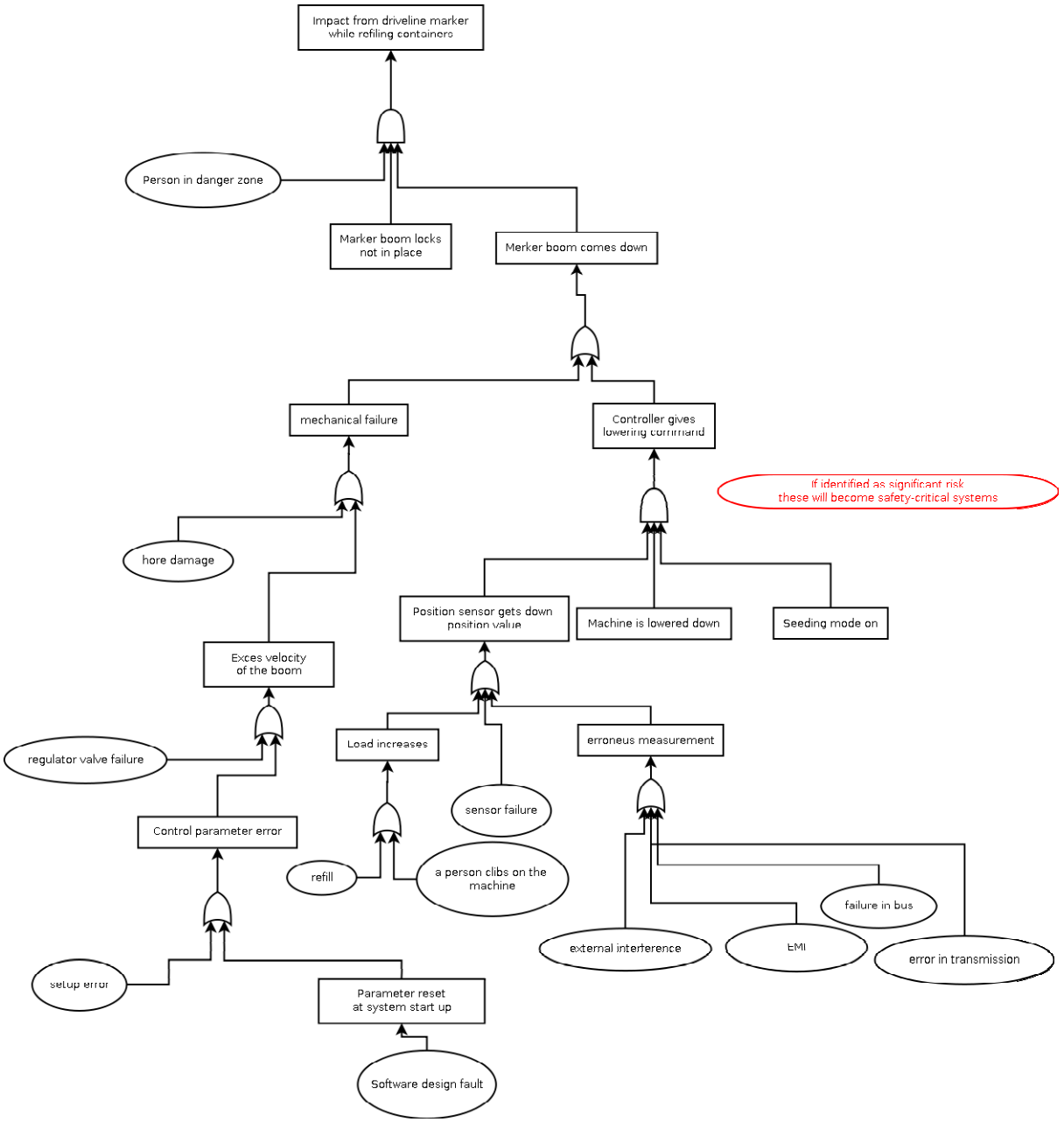
/52/ Leen, G.; Heffernan, D Expanding Automotive Electronic Systems IEEE Computer, Volume: 35 Issue: 1, January 2002,

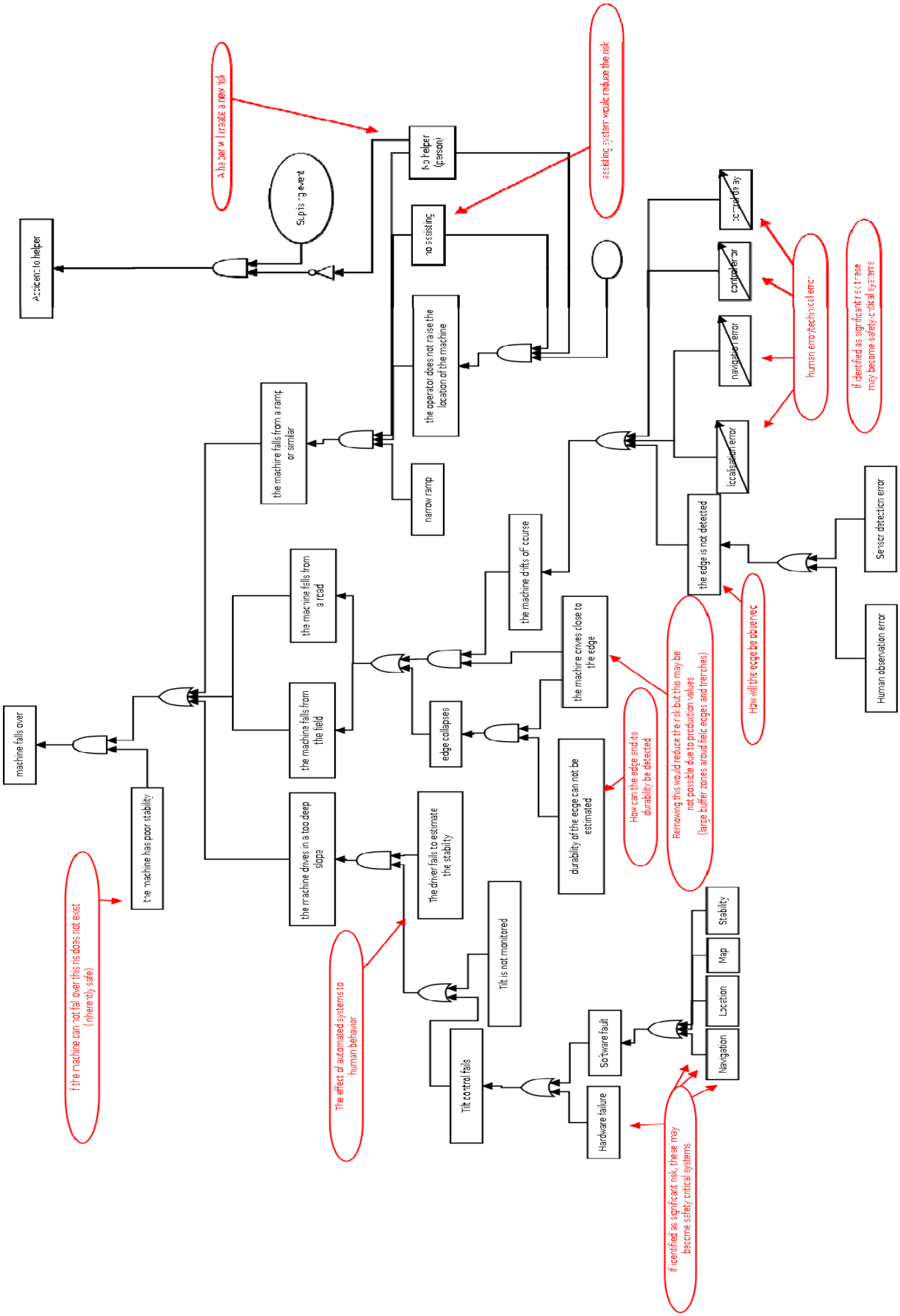
/53/ Blacmore, B Simon, Griepentrog, Hans Werner Autonomous Vehicles and Robotics Section 4.3 in Chapter 4 of CIGR Handbook of Agricultural Engineering Volume VI Information Tecnology. 2006

/54/ Web page http://www.vtt.fi/proj/riskianalyysit/ visited 21.2.2010

Appendix I




Impact from driveline marker while refiling containers
Person in danger zone
Marker boom locks not in place
Merker boom comes down
mechanical failure
Controller gives lowering command
If identified as significant risk these will become safety-critical systems
hore damage
Position sensor gets down position value
Machine is lowered down
Seeding mode on
Exces velocity of the boom
Load increases
erroneus measurement
regulator valve failure
sensor failure
Control parameter error
refill
a person clibs on the machine
failure in bus
external interference
EMI
error in transmission
setup error
Parameter reset at system start up
Software design fault


machine falls over
the machine has poor stability
the machine falls from a ramp or similar
the machine falls from a road
the machine falls from the field
the machine drives in a too deep slope
edge collapses
the machine drives close to the edge
the machine drifts of course
the edge is not detected
durability of the edge can not be estimated
The driver fails to estimate the stability
Tilt is not monitored
Tilt control fails
Hardware failure
Software fault
Navigation
Location
Map
Stability
localisation error
navigation error
controller
Sensor detection error
Human observation error
narrow ramp
the operator does not raise the location of the machine
no assisting
K9 helper (person)
Accident to helper
Slipping event
A helper will create a new risk
assisting system would reduce the risk
human error/technical error
If identified as significant risk these may become safety-critical systems
How will the edge be observed
Removing this would reduce the risk but this may be not possible due to production values (large buffer zones aroud field edges and trenches)
How can the edge and its durability be detected
The effect of automated systems to human behavior
If the machine can not fall over this risk does not exist (inherently safe)

Appendix II

Index	Hazard zone	Task	Hazard type	Hazard	Hazard scenario
1	side of the machine and driller adjustment zone	lifting the machine	crushing / cutting	crushing of a limb in between machine parts	a bystander adjusting /cleaning /exploring the machine
2	driller adjustment zone	calibration /rotation test			unexpcted movement of the machine while the operator adjusts bottom plates
3	rotation test site				a limb being caught to feeder axles
4	driller adjustment zone	not defined			a limb being caught in between the feeder axles
5		adjustement of the drillers			unexpected movement of the machine while the operator is adjusting the drillers
6		cleaning of the drillers			unexpected movement of the machine while the operator is cleaning the drillers
7	side of the machine	seeding depth check			unexpected movement of the machine while the operator is inspecting the seeding depth
8		lowering of the machine		crushing of a limb in between the machine and ground	a bystander under the machine
9	rotation test site	calibration /rotation test			unexpected movement of the machine while the operator is standing by the machine
10	driller adjustment zone	adjustement of the drillers			unexpected movement of the machine while the operator adjusts the drillers
11		cleaning of the drillers			unexpected movement of the machine while the operator cleans the drillers

12	side of the machine	seeding depth check			unexpected movement of the machine while the operator inspects seeding depth
13	side of the machine and the boom	not defined	impact	Impact from the machine frame or the boom	unexpected movement of the machine while the operator or a bystander works around the machine
14	driveline marker movement zone	preparing the machine	impact, falling object	impact from falling driveline marker	unexpected falling of the driveline marker
15		drive			
16		refill			
17		calibration /rotation test			
18		headline drive			unexpected falling of a driveline marker or a bystander in movement zone of the driveline marker
19		headline turn			
20		strip-drive			
21	container refill zone	refill	impact, crushing, falling object	being hit by falling objects	falling sack or its contents
22	road	drive	collision	collission with the machine	a road user collides with laterally displaced machine
23					collission to lowered driveline marker
24	field	headline drive		collission between the machine and an obstacle	the machine including the tractor collides with an obstacle
25		strip-drive			
26		headline turn			
27					the machine and the tractor fall from the field
28		headline drive			
29		drive			lowered driveline marker colides with an obstacle

30	road		crushing / cutting	beeing driven over by the machine or the tractor	the tractor or the machine runs over somebody
31	field	headline drive			
32		headline turn			
33		strip-drive			
34		headline drive	falling	the machine or the tractor falls over	the combination drives in too deep of a slope
35		headline turn			
36		strip-drive			
37		headline drive			the combination falls from the field
38		headline turn			
39		strip-drive			
40	road	drive			the combination falls form the road
41	field	headline drive	falling crushing	beeing run over by the machine	the operator or a pasanger falls from the tractor
42		headline turn			
43		strip-drive			
44	road	drive			
45	field	headline drive			a passanger falls from the machine
46		headline turn			
47		strip-drive			
48	road	drive			
49	coupling zone	coupling	crushing, impact	impact to or crushing of limbs or fingers	a finger or a limb gets caught between the couplings or gets hit by the couplings
50			noise	ear damge	exposure to noise
51	vincinity of the machine	field work	dust	inhailing dust	exposure to dust rising from the field or from the containers
52		drive	ejects	impact from an object ejected by the machine	the machine is driven on road while on lowered position
53	container refill zone	refill	slipping, falling	falling from the machine	loss of balance while workong on the planes of the machine
54		cleaning of the container			

Appendix III

1.2. CONTROL SYSTEMS

1.2.1. Safety and reliability of control systems

Control systems must be designed and constructed in such a way as to prevent hazardous situations from arising. Above all, they must be designed and constructed in such a way that:

- they can withstand the intended operating stresses and external influences,

- a fault in the hardware or the software of the control system does not lead to hazardous situations,

- errors in the control system logic do not lead to hazardous situations,

- reasonably foreseeable human error during operation does not lead to hazardous situations.

Particular attention must be given to the following points:

- the machinery must not start unexpectedly,

- the parameters of the machinery must not change in an uncontrolled way, where such change may lead to hazardous situations,

- the machinery must not be prevented from stopping if the stop command has already been given,

- no moving part of the machinery or piece held by the machinery must fall or be ejected,

- automatic or manual stopping of the moving parts, whatever they may be, must be unimpeded,

- the protective devices must remain fully effective or give a stop command,

- the safety-related parts of the control system must apply in a coherent way to the whole of an assembly of machinery and/or partly completed machinery.

For cable-less control, an automatic stop must be activated when correct control signals are not received, including loss of communication.

1.2.2. Control devices

Control devices must be:

- clearly visible and identifiable, using pictograms where appropriate,

- positioned in such a way as to be safely operated without hesitation or loss of time and without ambiguity,

- designed in such a way that the movement of the control device is consistent with its effect,

- located outside the danger zones, except where necessary for certain control devices such as an emergency stop or a teach pendant,

- positioned in such a way that their operation cannot cause additional risk,

- designed or protected in such a way that the desired effect, where a hazard is involved, can only be achieved by a deliberate action,

- made in such a way as to withstand foreseeable forces; particular attention must be paid to emergency stop devices liable to be subjected to considerable forces.

Where a control device is designed and constructed to perform several different actions, namely where there is no one-to-one correspondence, the action to be performed must be clearly displayed and subject to confirmation, where necessary.

Control devices must be so arranged that their layout, travel and resistance to operation are compatible with the action to be performed, taking account of ergonomic principles.

Machinery must be fitted with indicators as required for safe operation. The operator must be able to read them from the control position.

From each control position, the operator must be able to ensure that no-one is in the danger zones, or the control system must be designed and constructed in such a way that starting is prevented while someone is in the danger zone.

If neither of these possibilities is applicable, before the machinery starts, an acoustic and/or visual warning signal must be given. The exposed persons must have time to leave the danger zone or prevent the machinery starting up.

If necessary, means must be provided to ensure that the machinery can be controlled only from control positions located in one or more predetermined zones or locations.

Where there is more than one control position, the control system must be designed in such a way that the use of one of them precludes the use of the others, except for stop controls and emergency stops.

When machinery has two or more operating positions, each position must be provided with all the required control devices without the operators hindering or putting each other into a hazardous situation.

1.2.3. Starting

It must be possible to start machinery only by voluntary actuation of a control device provided for the purpose.

The same requirement applies:

- when restarting the machinery after a stoppage, whatever the cause,

- when effecting a significant change in the operating conditions.

However, the restarting of the machinery or a change in operating conditions may be effected by voluntary actuation of a device other than the control device provided for the purpose, on condition that this does not lead to a hazardous situation.

For machinery functioning in automatic mode, the starting of the machinery, restarting after a stoppage, or a change in operating conditions may be possible without intervention, provided this does not lead to a hazardous situation.

Where machinery has several starting control devices and the operators can therefore put each other in danger, additional devices must be fitted to rule out such risks.

If safety requires that starting and/or stopping must be performed in a specific sequence, there must be devices which ensure that these operations are performed in the correct order.

1.2.4. Stopping

1.2.4.1. Normal stop

Machinery must be fitted with a control device whereby the machinery can be brought safely to a complete stop.

Each workstation must be fitted with a control device to stop some or all of the functions of the machinery, depending on the existing hazards, so that the machinery is rendered safe.

The machinery's stop control must have priority over the start controls.

Once the machinery or its hazardous functions have stopped, the energy supply to the actuators concerned must be cut off.

1.2.4.2. Operational stop

Where, for operational reasons, a stop control that does not cut off the energy supply to the actuators is required, the stop condition must be monitored and maintained.

1.2.4.3. Emergency stop

Machinery must be fitted with one or more emergency stop devices to enable actual or impending danger to be averted.

The following exceptions apply:

- machinery in which an emergency stop device would not lessen the risk, either because it would not reduce the stopping time or because it would not enable the special measures required to deal with the risk to be taken,

- portable hand-held and/or hand-guided machinery.

The device must:

- have clearly identifiable, clearly visible and quickly accessible control devices,

- stop the hazardous process as quickly as possible, without creating additional risks,

- where necessary, trigger or permit the triggering of certain safeguard movements.

Once active operation of the emergency stop device has ceased following a stop command, that command must be sustained by engagement of the emergency stop device until that engagement is specifically overridden; it must not be possible to engage the device without triggering a stop command; it must be possible to disengage the device only by an appropriate operation, and disengaging the device must not restart the machinery but only permit restarting.

The emergency stop function must be available and operational at all times, regardless of the operating mode.

Emergency stop devices must be a back-up to other safeguarding measures and not a substitute for them.

1.2.4.4. Assembly of machinery

In the case of machinery or parts of machinery designed to work together, the machinery must be designed and constructed in such a way that the stop controls, including the emergency stop devices, can stop not only the machinery itself but also all related equipment, if its continued operation may be dangerous.

1.2.5. Selection of control or operating modes

The control or operating mode selected must override all other control or operating modes, with the exception of the emergency stop.

If machinery has been designed and constructed to allow its use in several control or operating modes requiring different protective measures and/or work procedures, it must be fitted with a mode selector which can be locked in each position. Each position of the selector must be clearly identifiable and must correspond to a single operating or control mode.

The selector may be replaced by another selection method which restricts the use of certain functions of the machinery to certain categories of operator.

If, for certain operations, the machinery must be able to operate with a guard displaced or removed and/or a protective device disabled, the control or operating mode selector must simultaneously:

- disable all other control or operating modes,

- permit operation of hazardous functions only by control devices requiring sustained action,

- permit the operation of hazardous functions only in reduced risk conditions while preventing hazards from linked sequences,

- prevent any operation of hazardous functions by voluntary or involuntary action on the machine's sensors.

If these four conditions cannot be fulfilled simultaneously, the control or operating mode selector must activate other protective measures designed and constructed to ensure a safe intervention zone.

In addition, the operator must be able to control operation of the parts he is working on from the adjustment point.

1.2.6. Failure of the power supply

The interruption, the re-establishment after an interruption or the fluctuation in whatever manner of the power supply to the machinery must not lead to dangerous situations.

Particular attention must be given to the following points:

- the machinery must not start unexpectedly,

- the parameters of the machinery must not change in an uncontrolled way when such change can lead to hazardous situations,

- the machinery must not be prevented from stopping if the command has already been given,

- no moving part of the machinery or piece held by the machinery must fall or be ejected,

- automatic or manual stopping of the moving parts, whatever they may be, must be unimpeded,

- the protective devices must remain fully effective or give a stop command.

Appendix IV

Task	sub task	machine pose	supports and safeguards	driveline markers	automatics	false state in automatics possible	engine	operator
coupling	preparations	up	driveline marker lock, standing support, service support	up	off		off	machine setting
		up	driveline marker lock, standing support	up	off		off	machine setting
	coupling to hitch	up	driveline marker lock, standing support, service support	up	off		on	coupling zone
		down	driveline marker lock, standing support	up	off		on	coupling zone
	attaching connectors	up	driveline marker lock, standing support, service support	up	off		off	coupling zone
		down	driveline marker lock, standing support	up	off		off	coupling zone
transfer from shelter	lifting the machine	up	driveline marker lock, (service support)	up	manual	x	on	cockpit
drive		up	driveline marker lock, service support	up	drive	x	on	cockpit
refill for rotation test calibration	service support removal	up	driveline marker lock, service support	up	manual	x	off	refill zone
	lowering the machine	down	driveline marker lock	up	manual		on	cockpit
	refilling from a sack	down	driveline marker lock	up	manual	x	off	refill zone
	lifting the machine	up	driveline marker lock	up	manual		on	cockpit
rotation test calibration	plate adjustment	up	driveline marker lock, service support	up	manual	x	off	refill zone
	calibration state (VT)	up	driveline marker lock, service support	up	manual		on	cockpit
	rotation test	up	driveline marker lock, service support	up	manual		on	side of the machine
driller adjustement		up	driveline marker lock, service support	up	manual	x	off	refill zone
drive		up	driveline marker lock, service support	up	drive	x	on	cockpit
Preparations for fieldwork	removal of supports	down	driveline marker lock, service support	up	manual	x	off	refill zone
	lowering the machine	down	driveline marker lock	up	manual		on	cockpit
	refilling from a sack	down	driveline marker lock	up	manual	x	off	refill zone
	lifting the machine	up	driveline marker lock	up	manual		on	cockpit
	driveline marker bc removal			up	manual	x	off	machine setting
field work 1 st stage	headline round	down		down	auto	x	on	cockpit
	working depth inspection	both		?	?	x	?	machine setting
	headline turns	both		?	auto/manual	x	on	cockpit
field work	strip drive	down		down	auto	x	on	cockpit
	headline turns	both		?	auto/manual	x	on	cockpit

Task	sub task	machine pose	supports and safeguards	driveline markers	automatics	false state in automatics possible	engine	operator
coupling	preparations	up	driveline marker lock, standing support, service support	up	off		off	machine setting
		up	driveline marker lock, standing support	up	off		off	machine setting
	coupling to hitch	up	driveline marker lock, standing support, service support	up	off		on	coupling zone
		down	driveline marker lock, standing support	up	off		on	coupling zone
	attaching connectors	up	driveline marker lock, standing support, service support	up	off		off	coupling zone
		down	driveline marker lock, standing support	up	off		off	coupling zone
transfer from shelter	lifting the machine	up	driveline marker lock, (service support)	up	manual	x	on	cockpit
drive		up	driveline marker lock, service support	up	drive	x	on	cockpit
refill for rotation test calibration	service support removal	up	driveline marker lock, service support	up	manual	x	off	refill zone
	lovering the machine	down	driveline marker lock	up	manual		on	cockpit
	refilling from a sack	down	driveline marker lock	up	manual	x	off	refill zone
	lifting the machine	up	driveline marker lock	up	manual		on	cockpit
rotation test calbration	plate adjustment	up	driveline marker lock, service support	up	manual	x	off	refill zone
	calibration state (VT)	up	driveline marker lock, service support	up	manual		on	cockpit
	rotation test	up	driveline marker lock, service support	up	manual		on	side of the machine
driller adjustement		up	driveline marker lock, service support	up	manual	x	off	refill zone
drive		up	driveline marker lock, service support	up	drive	x	on	cockpit
Preparations for field work	removal of supports	down	driveline marker lock, service support	up	manual	x	off	refill zone
	lovering the machine	down	driveline marker lock	up	manual		on	cockpit
	refilling from a sack	down	driveline marker lock	up	manual	x	off	refill zone
	lifting the machine	up	driveline marker lock	up	manual		on	cockpit

	driveline marker loc romoval			up	manual	x	off	machine setting
field work 1st stage	headline round	down		down	auto	x	on	cockpit
	working depth inspection	both		?	?	x	?	machine setting
	headline turns	both		?	auto/manual	x	on	cockpit
field work	strip drive	down		down	auto	x	on	cockpit
	headline turns	both		?	auto/manual	x	on	cockpit

MTT TEKEE TIETEESTÄ ELINVOIMAA

MTT RAPORTTI 6

www.mtt.fi/julkaisut

MTT Raportti -verkkojulkaisusarjassa julkaistaan maatalous- ja elintarviketutkimusta sekä maatalouden ympäristötutkimusta käsitteleviä tutkimusraportteja. Lukijoille tarjotaan tietoa MTT:n kaikilta tutkimusaloilta eli biologiasta, teknologiasta ja taloudesta.

MTT, 31600 Jokioinen.
Puh. (03) 4188 2327, sähköposti julkaisut@mtt.fi