Safety functional requirements for “Robot Fleets for Highly effective Agriculture and Forestry Management”

Pilar Barreiro*, Miguel Garrido*, Adolfo Moya*; Benoit Debilde, Patrick Balmer***, Jacob Carballido****, Constantino Valero*, Nicola Tomatis*** and Bart Missotten****

** LPF_TAGRALIA. Polytechnic University of Madrid (UPM), Avda. Complutense s/n, 28040 Madrid, Spain*

*** Case New Holland Belgium N.V. (CNH). Zedelgem, Belgium*

**** Bluebotics S.A. (BL.) Lausanne, Switzerland*

***** Soluciones Agrícolas de Precisión S.L. (SAP). Cordoba, Spain*

(e-mail: pilar.barreiro@upm.es).

Abstract: This paper summarizes the steps to be followed in order to achieve a safety verified design of RHEA robots units. It provides a detailed description of current international standards as well as scientific literature related to safety analysis and fault detection and isolation.

A large committee of partners has been involved in this paper, which may be considered as a technical committee for the revision of the progress of safety development throughout the progress of RHEA project.

Partners related to agricultural machinery, automation, and application development declare the interest of providing a stable framework for bringing the safety verification level required to be able to commercial unmanned vehicles such as those described in the RHEA fleet.

1. Introduction

This paper aims at establishing the safety specifications of RHEA robots based on current state of the art of safety standards and scientific knowledge.

The amount of authors reflects the wish of integrating a wide scope of points of views on the subject. These authors are committed to set-up a dedicated commission that will help the rest of partners on defining the safety functional requirements for each of those specialized units.

The paper is structured in a number of paragraphs dealing with the typification of actual hazards levels of operated machinery ; a review of the safety standard; the concept of life cycle assessment in the safety of agricultural machines; the assessment of risk; the concept of safety-related control systems for machines; hardware and software specifications; the recommendations towards the elimination of systematic faults and the definition of safety functions; available procedures for fault detection, isolation and prognosis; a review of the safety verification level when designing an agricultural machine; the concept of building blocks for intelligent mobile equipment and finally the steps to be accomplished for RHEA units.

2. Hazard levels in agricultural work

Agricultural machinery is involved in the majority of occupational accidents on farms, as proven by recent extensive scientific studies from the U.S. and Northern Europe (Bunn et al., 2008; Gerberich et al., 1998; Colémont and Van den Broucke, 2008; Thelin, 1998).

Although in absolute terms tractors are widely represented in these occurrences, large self-propelled harvesters are twice as hazardous as tractors. Most accidents occur in elevation or load transport work (21%), attachment and adjustment (20%), or when repairing (17%) machines. There are several variables that are associated to a high accident risk. Therefore, for example, working more than 40 hours a week multiplies this risk by three, as does the fact of the operator being married (risk multiplied by 2), or divorced (risk multiplied almost by 4).

Some factors that are associated to mortal accidents and which are not mutually exclusive are: 49% mechanical (seat belt not used, defective brakes or clutch), 52% type of tractor equipment (no rollover protection structure, use of rotary mowers or insufficient ballasting), or 55 % due to work location (slopes, muddy terrain). The risk of fatality is multiplied by 20 if the tractor rolls over. The lack of a rollover protection structure multiplies this risk by 11, while deficient maintenance multiplies it by almost 7, the same as for brake or clutch problems.

Some studies indicate that the user's perception of self-control is also a contributing factor in the risk of suffering an accident. It also appears that the number of accidents drops when the user has a positive and committed attitude towards the safety standards.

Generally speaking, reducing the presence of an operator without increasing risk would lead to an enormous decrease in accidents. Therefore, becoming autonomous may be more an advantage than a drawback in terms of safety. This argument was first held by Reid (2004a) and should be dearly considered when facing the analysis of safety in autonomous agricultural machinery.

3. Main safety standards for agricultural machinery

Making safe machines has become a top priority goal and in recent years, various standards have been published. It is important to review these standards. Figure 1 shows how the most relevant design and safety standards for general machinery are interlinked: ISO 12100 (safety of machinery, 2003), ISO 14121 (analysis and risk assessment, 2007), ISO 13849 (safety-related parts of control systems, 2003-2006), as well as for this specific field, ISO 25119: safe design for tractors and agricultural machinery(2009), although the general principles and safety requirements are set forth respectively in standards ISO 26322 (2010) and ISO 4254 (2008).

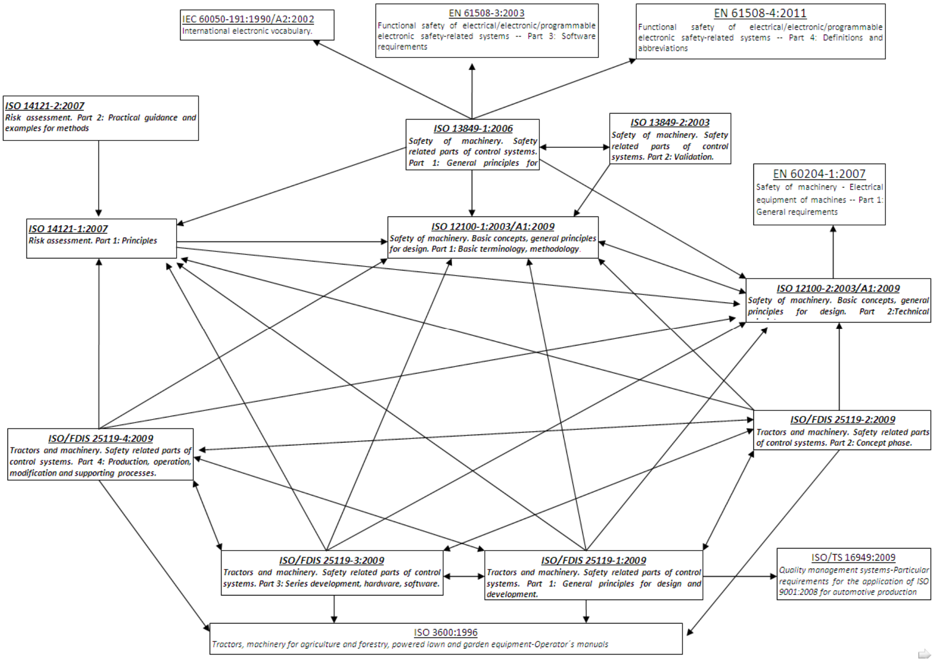

IEC 60050-191:1990/A2:2002
International electronic vocabulary.
EN 61508-3:2003
Functional safety of electrical/electronic/programmable electronic safety-related systems -- Part 3: Software requirements
EN 61508-4:2011
Functional safety of electrical/electronic/programmable electronic safety-related systems -- Part 4: Definitions and abbreviations
ISO 14121-2:2007
Risk assessment. Part 2: Practical guidance and examples for methods
ISO 13849-1:2006
Safety of machinery. Safety related parts of control systems. Part 1: General principles for
ISO 13849-2:2003
Safety of machinery. Safety related parts of control systems. Part 2: Validation.
EN 60204-1:2007
Safety of machinery - Electrical equipment of machines -- Part 1: General requirements
ISO 14121-1:2007
Risk assessment. Part 1: Principles
ISO 12100-1:2003/A1:2009
Safety of machinery. Basic concepts, general principles for design. Part 1: Basic terminology, methodology.
ISO 12100-2:2003/A1:2009
Safety of machinery. Basic concepts, general principles for design. Part 2:Technical
ISO/FDIS 25119-4:2009
Tractors and machinery. Safety related parts of control systems. Part 4: Production, operation, modification and supporting processes.
ISO/FDIS 25119-2:2009
Tractors and machinery. Safety related parts of control systems. Part 2: Concept phase.
ISO/FDIS 25119-3:2009
Tractors and machinery. Safety related parts of control systems. Part 3: Series development, hardware, software.
ISO/FDIS 25119-1:2009
Tractors and machinery. Safety related parts of control systems. Part 1: General principles for design and development.
ISO/TS 16949:2009
Quality management systems-Particular requirements for the application of ISO 9001:2008 for automotive production
ISO 3600:1996
Tractors, machinery for agriculture and forestry, powered lawn and garden equipment-Operator´s manuals

Fig.1. Interlinks between ISO standards related to the safety of machines.

This clearly shows the huge effort that has been made in the last five years towards enhancing safety conditions in the agricultural setting.

3.1 Life cycle analysis in the safety of agricultural machines

There are very close links between the various standards pertaining to safety. In general, the most recent ones tend to incorporate the content of the previous ones. For this reason, the first part of the design standard ISO 25119 offers a more global overview of the entire process in the form of a life cycle analysis, from conceptual development through to mass production or the alterations that are made after a machine enters the mass production stage (see Figure 2).

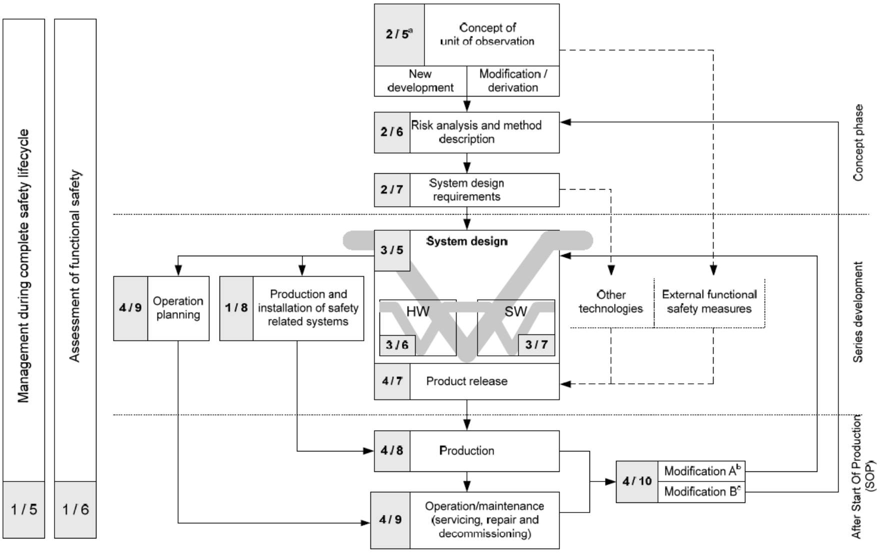

2 / 5a
Concept of unit of observation
New development
Modification / derivation
2 / 6
Risk analysis and method description
2 / 7
System design requirements
3 / 5
System design
HW
SW
3 / 6
3 / 7
4 / 7
Product release
Other technologies
External functional safety measures
4 / 9
Operation planning
1 / 8
Production and installation of safety related systems
4 / 8
Production
4 / 9
Operation/maintenance (servicing, repair and decommissioning)
4 / 10
Modification Ab
Modification Bc
Management during complete safety lifecycle
Assessment of functional safety
1 / 5
1 / 6
Concept phase
Series development
After Start Of Production (SOP)

Fig.2. Life cycle analysis in the safety of agricultural machines. (Source: ISO 25119-1)

Figure 2 indicates that when mass production commences, special attention will be paid to the system design, both hardware and software aspects, using the V-model (Fig. 3). The numbers shaded in grey (a/b) respectively encode the part of the ISO 25119 standard and the chapter in which they are contained.

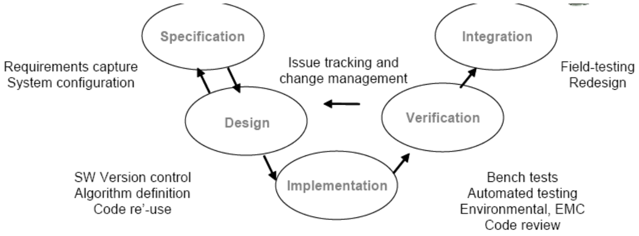


Fig. 3. V-model (Source: Lenz et al. 2007)

It is important to point out that wherever possible the new unit of observation (machine under study) should be defined as an alteration of some pre-existing system of the same or another manufacturing firm, so that it is possible to avail of the legacy of information available in terms of analysis and risk assessment, and the corrective measures associated thereto. It has also been proposed that insofar as possible, a parallel should be drawn between the hardware and software structure for assessment and pre-existing equipment, so that the required agricultural performance levels (AgPL) may be more easily allocatable.

3.2 Risk assessment

This section specifically refers to the ISO 14121 standard: Risk assessment. According to this standard, it is necessary to distinguish between analysis, which consists of determining the limits of the machine, hazard identification and quantitative risk estimation, and evaluation, which is the result of deciding on the need or otherwise to reduce risk by implementing design measures, incorporating protective elements or providing information to the person that may potentially be affected. Figure 5 sums up this process.

Defining the limits of the machine means considering the intended purpose and what kind of incorrect use may reasonably be foreseen, the operating modes (transport, work, maintenance), the level of training expected of users (operators, maintenance personnel, apprentices and members of the general public); as well as the space limitations to be taken into account for the breadth of movements (areas within scope) and the dimensional requirements for people.

In order to identify hazards, as sources of damage, i.e. physical injuries or harm to health, it is necessary to consider the operations and tasks that the machine performs, as well as those that are carried out by the people that interact with it, deciding which are hazardous situations and events, i.e. circumstances and events in which one or more people are exposed to one or more risks. The significance or severity of the damage should be defined: S0 (not significant or only requiring first-aid), S1 (slight to moderate with medical care and full recovery) , S2 (severe with lifelong side-effects but probable survival) and S3 (with side-effects in vital capacities, uncertain survival and/or severe disability); as should the likelihood of the damage occurring: E0 (improbable, maximum once in the machine's useful life, < 0.01%), (rare, annual maximum, 0.01%-0.1%), E2 (sometimes, less than on a monthly basis, 0.1-1%), E3 (frequent, more than once a month, 1-10%), and E4 (very frequent, in almost every operation, >10%) (see Figure 5).

The ISO 14121-1 standard is thorough in defining types of hazards: mechanical (associated to kinetic or potential energy, and the shape and structure of the elements), electric, thermal, noise-related, vibration-related, radiation-related, caused by materials or chemical substances, hazards associated to a failure to comply with the principles of ergonomics, or the setting in which the machine is used (dust or fog, humidity, mud, snow, etc.). The standard also provides several examples of tasks in relation to the stage in the life cycle of the machine, as well as hazardous situations, which are understood to mean situations that may give rise to damage.

Risk is defined as the combination of the likelihood of damage occurring and its severity and, as indicated previously, the concept of risk analysis contemplates specifying the limits of the machine, hazard identification and risk estimation.

In evaluating risk, the possibility of avoiding or controlling the damage should also be taken into consideration: C0 (easy to control), C1 (simple to control, over 99% of people would know how to control it in over 99% of circumstances), C2 (mostly controllable, over 90% of people would know how to control it in over 90% of circumstances) and C3 (not avoidable by average operator or typical personnel in vicinity) (see Figure 5).

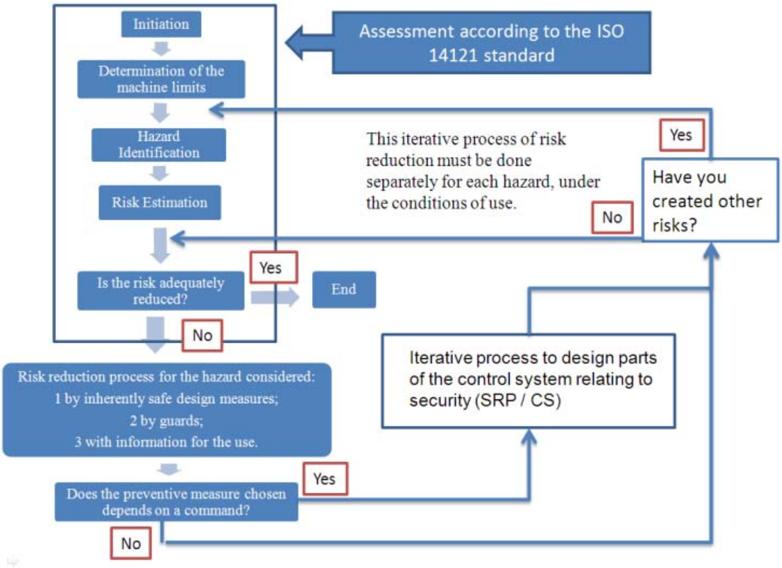
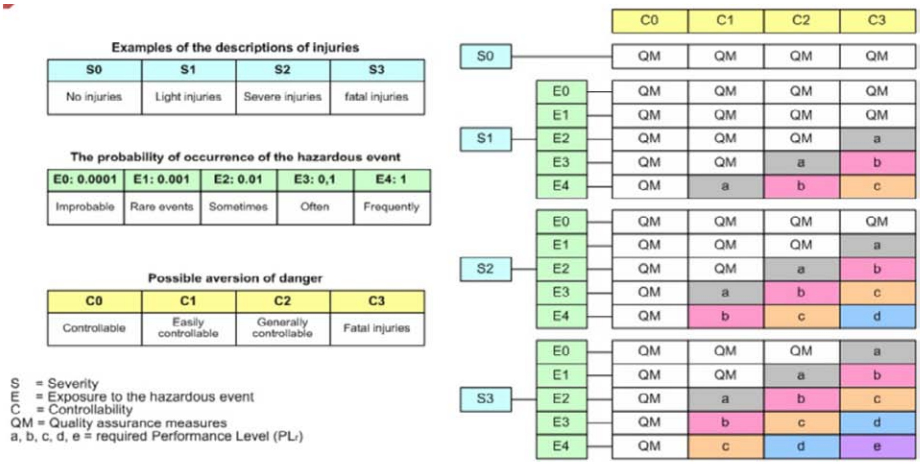

Initiation
Determination of the machine limits
Hazard Identification
Risk Estimation
Is the risk adequately reduced?
Yes
End
No
Assessment according to the ISO 14121 standard
This iterative process of risk reduction must be done separately for each hazard, under the conditions of use.
Yes
No
Have you created other risks?
Iterative process to design parts of the control system relating to security (SRP / CS)
Risk reduction process for the hazard considered:
1 by inherently safe design measures;
2 by guards;
3 with information for the use.
Does the preventive measure chosen depends on a command?
Yes
No

Fig.4. Flow diagram linked to assessing risk in agricultural machines. (Elaborated from ISO13849-1)

The ISO 25119-2 standard defines beyond which combination of severity and likelihood of damage, and control level it is indispensable to include a control system in addition to the inclusion of protection devices or merely informative aspects that are generally covered under the term QM, i.e. quality assurance measures pursuant to the ISO 9001:2000 standard (see Figure 5).

3.3 Safety-related control systems for machines

For cases in which the quality assurance measures do not suffice, it is indispensable to include risk reduction systems, the features of which should match the performance level. These systems are generally called SRP/CS, i.e. safety-related parts of the control system. The ISO 25119-2 standard provides five performance levels for agricultural equipment (AgPL) identified with the letters "a" to "e" for increasing levels of risk.



Examples of the descriptions of injuries

S0	S1	S2	S3
No injuries	Light injuries	Severe injuries	fatal injuries

The probability of occurrence of the hazardous event

E0: 0.0001	E1: 0.001	E2: 0.01	E3: 0,1	E4: 1
Improbable	Rare events	Sometimes	Often	Frequently

Possible aversion of danger

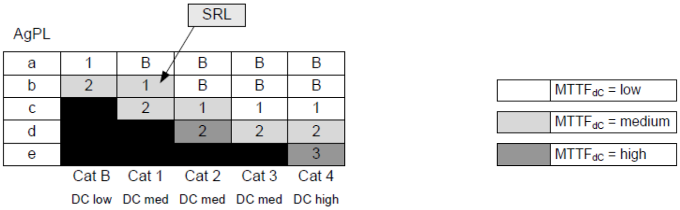
C0	C1	C2	C3
Controllable	Easily controllable	Generally controllable	Fatal injuries

S = Severity
E = Exposure to the hazardous event
C = Controllability
QM = Quality assurance measures
a, b, c, d, e = required Performance Level (PLr)

		C0	C1	C2	C3
S0		QM	QM	QM	QM
S1	E0	QM	QM	QM	QM
	E1	QM	QM	QM	QM
	E2	QM	QM	QM	a
	E3	QM	QM	a	b
	E4	QM	a	b	c
S2	E0	QM	QM	QM	QM
	E1	QM	QM	QM	a
	E2	QM	QM	a	b
	E3	QM	a	b	c
	E4	QM	b	c	d
S3	E0	QM	QM	QM	a
	E1	QM	QM	a	b
	E2	QM	a	b	c
	E3	QM	b	c	d
	E4	QM	c	d	e

Fig.5. Performance levels for agricultural equipment (AgPL) identified with the letters "a" to "e" for increasing levels of risk. (Source: Benneweis, 2006)

Attaining a particular AgPL depends on a number of factors, such as: the category associated to its hardware structure (B, 1, 2, 3 ó 4), the mean time to a dangerous fault (MTTFd), diagnostic coverage (DC) and common cause faults (CCF). The software readiness levels (SRL) are in turn dependent on the AgPL value that is required, the diagnostic coverage available: low (60 to 90%), medium (90 to 99%) or high (over 99%) and MMTfd: low (3 to 10 years), medium (10 to 30 years) or high (30 to 100 years). The ISO 25119-2 standard defines a simplified procedure for assessment, as shown in Figure 6.



SRL

AgPL	Cat B DC low	Cat 1 DC med	Cat 2 DC med	Cat 3 DC med	Cat 4 DC high
a	1	B	B	B	B
b	2	1	B	B	B
c		2	1	1	1
d			2	2	2
e					3

MTTF$_{dc}$ = low
MTTF$_{dc}$ = medium
MTTF$_{dc}$ = high

Fig.6. Performance levels and software readiness levels depending on hardware configuration (B, 1, 2, 3 and 4) and the diagnostic coverage level (fault detection capacity). (Source: ISO 25119-2)

3.4 Hardware configurations

According to the ISO 13849-1 and ISO 25119-2 standards, there are five typical hardware configurations (B, 1, 2, 3 and 4) in SRP/CS, which may be displayed in 3 different diagrams (see Figure 7). The first layout: inputs (I), logical processing (L), outputs (O) corresponds to the typical structures B and 1, with the difference that in the former, the diagnostic coverage is null and the MTTFd for each channel cannot be measured, whereas configuration 1 uses components of proven efficiency in safety-related operations and may require redundant inputs depending on the diagnostic coverage required (low or medium). The second layout, which corresponds to the type 2 architecture, includes as well as the above elements, other testing equipment (TE, typically man-machine interfaces) and the outputs of the testing equipment (OTE). Finally, architectures 3 and 4 are the third layout, with the difference that for the latter, the diagnostic coverage in monitoring (m) is higher than in architecture 3, and that redundant outputs may be necessary in order to maintain the safety functions.

Another relevant aspect of the standard is that it also defines how to calculate the performance level when there are several SRP/CS attached in series. Generally speaking, when there are more than 2 or 3 SRP/CS in series with the same minimum AgPL level, the global value drops by a level, e.g. from level AgPL d to AgPL c.

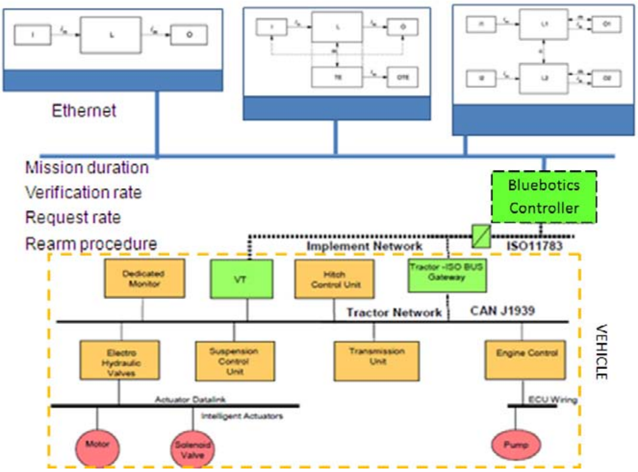


Fig.7. Predefined hardware configurations in the ISO 13849 and ISO 25119 standards. (Elaborated from Lenz et al. 2007)

Figure 7 shows a first approach towards the integration of several SRP/CS of varying hardware configurations that communicate with Bluebotics controller via Ethernet, while the latter interact with internal bus of the tractor via ISO11783 (ISOBUS). It is important to state that any hardware configuration should follow ASABE recommendations regarding environmental conditions (ASABE, 2008).

3.5 Software Specifications

In this sense, Hoffman (2006) provides probably the most complete review of actual complexity of software in tractors, given the great number of factors that affect the integrity of software in machines equipped with electronic systems, it is not possible to define an algorithm that will ascertain which techniques and measures are best suited to each application. On the other hand, when selecting methods and measures for defining software, it is important to bear in mind that as well as the manual code programming, model-based developments may employ automatic code generation tools. (Lutz, 1992)

The ISO 25119-3 standard (2009) devotes forty pages to the chapter on software in relation to the safety of agricultural machines and indicates that it is necessary to define the method to be employed in defining the safety requirements for the software: natural language, semi-formal methods (based on diagrams and figures, or animation-based analyses), formal methods (based on mathematical procedures), or methods that employ computer-assisted tools (in the form of databases that can be automatically inspected and examined to assess consistency and completeness).

In general, the standard provides that the software architecture should not be commenced until a sufficient degree of maturity has been attained in defining the safety requirements, employing top-down methods to evaluate the combination of events that may give rise to hazardous situations, and bottom-up methods to decide which components in the system would be damaged.

In developing the software, the first step will be to define the modules that will be related to safety and then define the rest of the functions. The programming language should be such as to enable easy code verification, validation and maintenance. In this regard, it is desirable to use automatic code translation tools, pre-existing libraries that have been extensively verified, code debugging systems and software version control tools. It is not clear if object-oriented languages are preferable to procedure-based languages.

The use of defensive programming methods is recommended, capable of producing programmes that can detect control flows or erroneous data, so that the system may react in a predetermined and acceptable manner. Some defensive programming techniques include: changing that variables are in range and analysing the credibility of their values, a priori checks on parameters and procedures before running them, and separating parameters according to whether they are read-only or read-write.

In general, the following criteria should be followed: the programme should be divided into small software modules, the modules should be composed using sequences and iterations, a limited number of paths should be maintained in the software, complex ramifications and unconditional leaps should be avoided, loops should be linked to input parameter values, and complex calculations should be avoided when making decisions on forks and loops. Lastly, they recommend that dynamic variables be limited so that the memory requirements and a priori directions are known a priori. The use of interruptions should also be limited, especially when using critical software, so that the maximum time for inhibiting safety functions is controlled at all times. The use of check-lists is recommended in order that the set of relevant issues are verified in each stage of the life cycle of the software.

3.6 Eliminating systematic faults and safety functions

There are a number of typical faults for which the ISO 25 119-2 (2009) standard provides certain recommendations: preventing the loss of electricity supply in electronic boxes, selecting manufacturing materials that are suitable for the setting in which they are to be used, correct component installation, compatibility, modularity of design, restricted use of common elements such as memories or electronic cards, separating safety-related and non-safety-related components in the control system, and checking design by employing assisted design systems for simulation and simulation programmes.

A number of typical safety functions are also defined by the ISO 25119-2 standard for consideration in design, i.e. 1) a lock to prevent switching on the system by accident, 2) the immediate halt function, 3) manual resetting, 4) automatic switching on and resetting after a fault, 5) response time (divided into detecting the fault, starting to take measures and managing to attain a safe operating mode), 6) safety-related parameters (position, speed, temperature, pressure), 7) external control functions (how to select external control, verify that switching the external control does not cause hazardous situations, and how to act in the event of loss of external control), 8) manual inhibition of safety functions (for example, for diagnostic purposes), and 9) the availability of alarms for the user.

3.7 Fault detection and diagnosis to improve safety

Once the safety functions have been defined, it is important to foresee available algorithms and procedures that are used in other fields of work such as spacecraft. In this sense NASA has show to be far ahead and the definitions provided are considered of major interest:

- Fault detection: addressing the occurrence of a miss function of any kind in a system, realizing that something is going wrong.
- Fault diagnosis: fault isolation, determining the cause of failure or what is particularly wrong in many cases as a source of common cause fault (CCF).
- Fault prognosis: detection the precursors of failure and predicting the remaining time before failure occurrence.

The procedures that can be used for any of the three tasks can be classified into model-based or data –driven (model-free) (Donca and Mihaila, 2010).

- Model-based fault diagnosis and prognosis: consisting either on qualitative or quantitative models that take advantage of fundamental knowledge of the problem.

- Data-driven fault diagnosis and prognosis: it is also referred as history-based knowledge. Methods available for Data-driven Fault Diagnosis and Prognosis combine: Data mining (also known as Knowledge Discovery in Databases KDD), Artificial Intelligence, Machine Learning and Statistics.

According to the nature of the information available we may define numerical and text data, and for the latter, further classification into structured (fit into narrow fields in databases) and unstructured text (nearer to natural language) is a relevant issue. In this context Text Mining refers to the tools that allow extracting knowledge from databases typical from customer (after-sales) services where unrestricted textual format for fault description is used (Harding et al., 2006; Hui and Jha, 2000).

There are several review papers and dedicated researches that make use of the three types of information for fault detection and diagnosis: Vibration signatures, CAN data and Warranty data.

For vibration signatures the following methods have been described and reviewed in the literature (2005 to 2010) (Schwabacher, 2005):

- Data-Driven Fault Detection: unsupervised anomalies detection algorithms (Orca, Grobot, DIAD), inversion induction monitoring System (data cluster into system modes), Neural Networks (NN) and envelope detection by means of hidden Markov models.
- Data-Driven Diagnosis: Feature extraction on data (Fast Fourier Transform in frequency domain, while signal energy and kurtosis in time domain), Support Vector Machines (SVM), wavelet transform and wavelet packet transform combined with SVM.
- Data-Driven Prognosis: NN, rule extractors, similarity based methods, autoregressive methods, fuzzy logic algorithms and Bayesian Belief NN.
- Model-based Diagnosis: hierarchical models with finite state machine.
- Model-based Prognosis: Kalman filters and stochastic differential equations.

For CAN data a very recent publication (Suwatthikula et al., 2011) proposes the use of Adaptive Neural Fuzzy Inference Systems (ANFIS) for the prediction of Network Health and fault diagnosis in CAN networks based on total differential resistance on the bus and the amount of error frames per second. It also enables to distinguish between internal (typically digital) and peripheral (mainly analogue) faults.

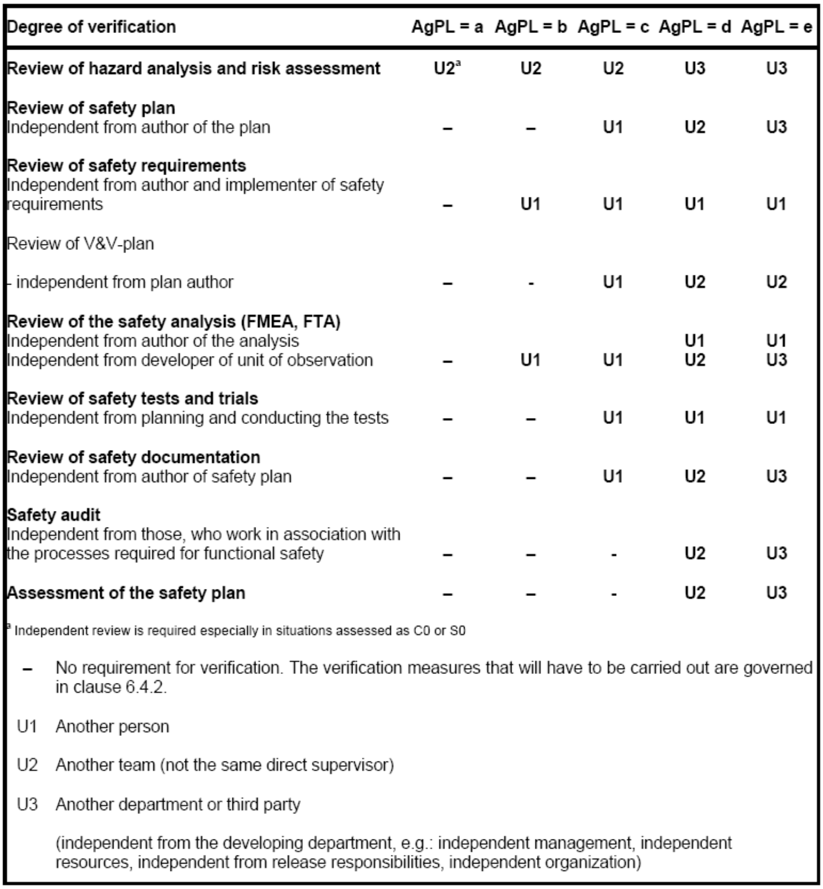
The characteristics of the ideal fault diagnosis system, as referred in 2010 by the only paper on FD in agricultural machinery (Craessaerts et al., 2010), include: 1)quick detection and isolation of faults, 2) robustness against noise and uncertainties, 3) novelty identification for unseen cases, 4) classification error estimate, 5) adaptability to time varying processes, 6) low modelling and low computational requirements, and 7) multiple fault identification (several at a time).

The incorporation of fault detection and diagnosis tools for autonomous machinery is to play an important role for safety purposes.

3.8 Safety verification level when designing an agricultural machine

In accordance with the ISO 25119-1 standard, one very important aspect when designing an agricultural machine is deciding on the safety verification level that may require the participation of persons not linked to design, teams of staff other than designers, or even different departments or consultancy firms, for the agricultural performance (AgPL) levels, which go from "a" to "e" in ascending order (see Table 1).

Table 1. Degree of verification (Source: ISO 25119-1)



Degree of verification	AgPL = a	AgPL = b	AgPL = c	AgPL = d	AgPL = e
Review of hazard analysis and risk assessment	U2[a]	U2	U2	U3	U3
Review of safety plan Independent from author of the plan	–	–	U1	U2	U3
Review of safety requirements Independent from author and implementer of safety requirements	–	U1	U1	U1	U1
Review of V&V-plan					
- independent from plan author	–	-	U1	U2	U2
Review of the safety analysis (FMEA, FTA) Independent from author of the analysis Independent from developer of unit of observation	–	U1	U1	U1 U2	U1 U3
Review of safety tests and trials Independent from planning and conducting the tests	–	–	U1	U1	U1
Review of safety documentation Independent from author of safety plan	–	–	U1	U2	U3
Safety audit Independent from those, who work in association with the processes required for functional safety	–	–	-	U2	U3
Assessment of the safety plan	–	–	-	U2	U3

[a] Independent review is required especially in situations assessed as C0 or S0

– No requirement for verification. The verification measures that will have to be carried out are governed in clause 6.4.2.

U1 Another person

U2 Another team (not the same direct supervisor)

U3 Another department or third party

(independent from the developing department, e.g.: independent management, independent resources, independent from release responsibilities, independent organization)

3.9 Building blocks for Intelligent Mobile Equipment (robots)

Some authors (Reid, 2004b) have defined unmanned vehicle not exactly in terms of safety requirements but as related to building blocks.

In this case the blocks are agents than can provide important complementary information to the safety function through the main controlled designed by Bluebotics.

The building blocks of intelligent mobile equipment proposed by Reid (2004b) are shown in Figure 8. The elements are defined in terms of Machine Control (X-by-Wire and Navigation), Machine Awareness (Localization and Perception), and Intelligence (Mission Planning and Intelligent Systems). Hereafter, it is useful to further define the blocks:

X-by-Wire: These are basic control of the actuation surfaces of a machine that include the steering, brakes, throttle and other functions. It also relates to the basic machine health and the interaction of these controlled components.

Navigation: Elements of Navigation relate to how the various control systems lead to machine mobility. Navigation is concerned with issues of path tracking accuracy and how machine functions respond in a mission.

Localization: Localization is the awareness of the posture of the intelligent vehicle relating to position and orientation in the open environment.

Perception: Perception is the awareness of the features of the local surroundings that can include obstacles and other environmental features. Perception is a key element of vehicle safeguarding in the sense that obstacle features are detected with perception sensors.

Mission Planning: Mission Planning systems allow the determination of the tasks and behaviors of an intelligent machine system in the operating environment. All of these functions are connected by an intelligent control system that can arbitrate what needs to happen under dynamically changing situation. Path planning is one of the key tasks that are controlled in mission planning. Mission planning tools like simulation are a key part of advanced system development.

Intelligent Systems: The semi-autonomous or autonomous vehicle is an intelligent system. It has an architecture that is both modular and scalable to allow it to be deployed for application.

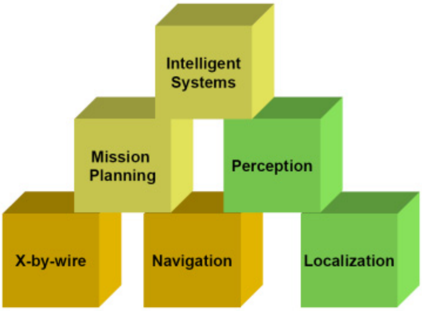


Fig.8. Building blocks for Intelligent Mobile Equipment (Source: Reid, 2004b)

4. Steps to be accomplished for "RHEA" robots

RHEA proposes the use of three robot fleets. The 3 ground mobile units will be based on small autonomous vehicles similar to New Holland tractor "Boomer 3050 CVT"– (4×4 wheel drive) powered by an engine (51 Hp) with a unit weight estimated in about 1.2 ton. The units will follow the rows at a speed of about 6km/h – with onboard equipment for navigation and application of treatments. The electronic equipment on-board the ground mobile units will be powered by a system based on solar panels and fuel cells.

Below are summarized the principal details of each ground mobile unit:

- **Sprayer Boom Vehicle in wheat:**

  This vehicle will be equipped with a spray boom (Fig.9) that will apply herbicide on wheat crops based on the information from the perception system on board the aerial units. The goal is to apply herbicide to at least 90% of the detected patches.

- **Physical weed control vehicle in maize:**

  This ground mobile unit will be equipped with end-effectors or tools, developed to destroy weeds in maize, which will be based on both thermal and mechanical devices (Fig.9). The goal is to destruct at least 90% of the detected weeds.

  The main idea is to equip the ground mobile unit with a 4.5 m hoe equipped with rigid or rotating tools for interrow cultivation and selective tools for in-row weed control. However, the best solution in this case could be the use of flaming, according to the high selectivity and the very low cost (in this respect, very simple, cheap, and easy to use and to adjust burners that are connected to very low LPG consumption will be developed).

- **Insecticide Application Vehicle in Olive:**

  The third vehicle will be equipped with a spray system to apply pesticide in olive trees (Fig.9). The goal is to apply the pesticide at least on 90% of the tree canopy.

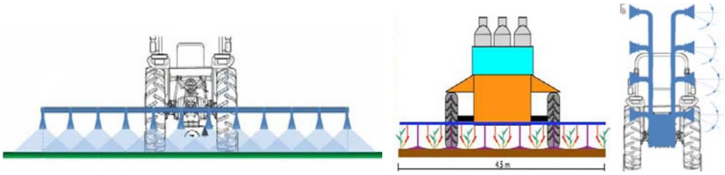


Fig.9. View of the different robot units (Sprayer boom, Physical control, and Insecticide unit).

According to the definitions and specifications provided in previous paragraphs, Figure 10 provides a first approach toward the safety control loop of the vehicle. It is important to indicate that since around 10 safety functions have been identified and more than 20 sensors will most probably be providing information, and therefore a safety logic unit should be used for the safety loop.

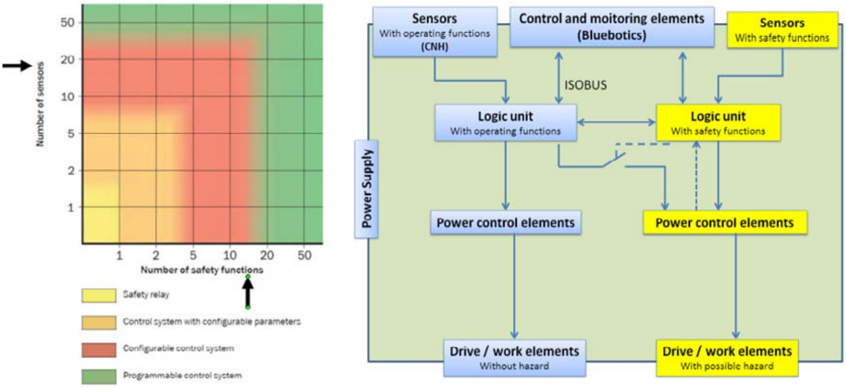


Fig. 10. Basic safety (Elaborated form: SICK Optic-Electronic, S.A.)

At this stage it is very important to clarify the tasks that should be considered in the particular case of RHEA for the risk assessment and therefore to define the performance level required for every SRP/CS.

Table 2 provides an example of tasks that take place during 3 diffrenets operating modes: labor, maintenance and transport, as defined by one of the end users in the RHEA project. This table should be considered by other partners in order to provide a similar approach for every of the three units. All partners should provide safety information concerning the most similar machine on equipment as stated at the beginning of the paper. Generally speaking, such manuals address the three operation modes and thus will be of highest relevance.

Table 2. Spraying tasks RHEA robot unit

Labor	Maintenance	Transport
Before	Mechanical	•Attachment •Checking Lighting System •Checking Elements That Could Shed Or Hang From The Machine
• Attachment (3 Points; PTO; Electric; Oil Hydraulic Jacks) • Filling With Water • Opening Bar and System Testing (Check Filters And Nozzles) • Addition Agrochemicals	• Cleaning, Check and Lubrication Of Moving Parts (Bar; Suspension System; Pump And PTO; Hydraulic Actuators)	
During	Hydraulic	
• Bars Opening and Closing • PTO Manipulation • Fill Water And Agrochemicals • Navigation	• Cleaning and Replacement (Filters, Nozzles, Pipes, Manometers)	
After	Electric	
• Cleaning (Clean Water Spray; Clean Filters) • Release (3 Points; PTO; Electic; Oil Hydraulic Jacks)	• Checking, Cleaning (Valves, Connection Boxes, Wiring, Other Sensors And Actuators)	

5. Conclusions

A dedicated review of safety standards and scientific state on this subject has been carried out in this work.

This paper aims at acting as the corner stone in the process of definition of safety specifications, functions and verification levels.

When all partners in the project agree and follow the recommendations described in the papers, the consortium should be confident in meeting a safety design at the end of the project.

A commission constituted by the authors of the paper together with the coordinator will be in charge of verifying the progress throughout the project stages.

Acknowledgement

The research leading to these results has received funding from the European Union's Seventh Framework Programme [FP7/2007-2013] under Grant Agreement nº 245986.

References

ASABE. 2008. Environmental considerations in development of mobile agricultural electrical/electronic components. ANSI/ASAE DEC 1990 (R2008)

Benneweis, R.K. (2006). Facilitating agriculture automation using standards. Club of Bologna. Proceedings, Volume nº17 – Bonn 3 sept. 2006.

Bunn, T.L., Slavova, S., Hall, L. (2008). Narrative text analysis of Kentucky tractor fatality reports. Accident Analysis and Prevention 40 (2008) 419-425.

Colémont, A., Van den Broucke, S. (2008). Measuring determinants of occupational health related behavior in flemish farmers: An application of the theory of planned behavior. Journal of Safety Research 39 (2008) 55-64.

Craessaerts, G., De Baerdemaeker, J. Saeys, W. (2010). Fault diagnostic systems for agricultural machinery. Biosystems Engineering 106 (1):26-36.

Donca, G., Mihaila., V.I. (2010). Aspects regarding data mining applied to fault detection. Annals of the Oradea University. Fascicle of Management and Technological Engineering, Volume IX (XIX), 2010.

Gerberich, S.G., Gibson, R.W., French, L.R., Lee, T-Y., Carr, W.P., Kochevar, L., Renier, C.M., Shutske, J. (1998). Machinery-related injuries: Regional rural injury study-I (RRIS-I). Accident Analysis and Prevention 30, No. 6 (1998) 793-804.

Harding, J.A., Shahbaz, M., Srinivas, S., Kusiak, A. (2006). Data Mining in Manufacturing: A Review. Journal of Manufacturing Science and Engineering 128, 969-976.

Hofmann, R. (2006). Software in Tractors: Aspects of Development, Maintenance and Support, Club of Bologna Proceedings, Volume nº17 – Bonn 3 sept. 2006.

Hui, S.C., Jha, G. (2000). Data mining for customer service support. Information & Management 38, 1-13.

ISO 11783: Tractors and machinery for agriculture and forestry -- Serial control and communications data network. Part 1: General specifications.

ISO 12100-1: Safety of machinery. Basic concepts, general principles for design. Part 1: Basic terminology, methodology.

ISO 13849-1: Safety of machinery. Safety-related parts of control systems. Part 1: General principles for design.

ISO 14121-1: Safety of machinery. Risk assessment. Part 1: Principles.

ISO 25119-1: Tractors and machinery for agriculture — Safety related parts of control systems — Part 1: General principles for design and development.

ISO 25119-2: Tractors and machinery for agriculture — Safety related parts of control systems — Part 2: Concept Phase.

ISO 25119-3: Tractors and machinery for agriculture and forestry — Safety related parts of control systems — Part 3: Series Development, Hardware, and Software.

ISO 26322-1: Tractors for agriculture and forestry — Safety — Part 1: Standard tractors.

ISO 4254-1: Agricultural machinery. Safety. Part 1: General requirements.

Lenz, J., Landman, R., Mishra, A. (2007). Customized Software in Distributed Embedded Systems: ISOBUS and the Coming Revolution in Agriculture. Agricultural Engineering International: the CIGR Ejournal. Manuscript ATOE 07 007. Vol. IX. July, 2007.

Lutz, R.R. (1992). Analyzing software requirements errors in safety-critical, embedded systems. Iowa State University of Science and Technology. Departament of Computer Science. Tech Report: TR 92-27. Submission date: August 27, 1992.

Reid, J. F. (2004b). Mobile intelligent equipment for off-road environments. Written for presentation at the Automation Tehcnologiy for Off-Road Equipment at 7-8 October 2004 Conference (Kyoto, Japan). ASAE Publication Number: 701P1004.

Reid, W.S. (2004a). Safety in perspective, for autonomous off road equipment (AORE). Written for presentation at the 2004 ASAE/CSAE Annual International Meeting. Paper number: 041151.

Schwabacher, M.A. (2005). A Survey of Data-Driven Prognostics. Infotech@Aerospace. AIAA 2005-7002. 26 - 29 September 2005, Arlington, Virginia.

Suwatthikula, J., McMurranb, R., Jonesa, R.P. (2011). In-vehicle network level fault diagnostics using fuzzy inference systems. Applied Soft Computing 11 (2011) 3709–3719.

Thelin, A. (1998). Rollover Fatalities-Nordic Perspectives. Journal of Agricultural Safety and Health 4(3): 157-160.