Università degli Studi di Ferrara

DOTTORATO DI RICERCA IN
"SCIENZE DELL'INGEGNERIA"

CICLO XXVIII

COORDINATORE Prof. Stefano Trillo

Scalable Safety-Oriented Architectures for Mechatronic Components and Systems in Agricultural and Heavy-Duty Machines

Settore Scientifico Disciplinare ING-INF/01

Dottorando	**Tutore**
Dott. Ferraresi Carlo	Prof. Ruggeri Massimiliano
_______________________	_______________________
(firma)	*(firma)*

Anni 2013/2015

Index

Preface

The growing importance of electronics systems, in conjunction with the new regulatory framework for agricultural and heavy-duty industry compartments, calls for new architectural paradigms for the design of systems and components. The widely adoption of X-by-wire systems and mechatronic components, introduces a new set of issues related to the functional safety of those systems, which have traditionally relied on hydraulic or mechanical solutions.

The international community has recognized these problematics and a particular effort has been put on the implementation of new standards and regulations specific for the functional safety.

In particular, the Machine Directive 2006/42/EC addresses the electronic control systems in machinery. One of the main point of the directive is that manufacturers are responsible for the safety of their products and they must make a risk assessment to identify and reduce every unnecessary risk. For each industry compartments, a specific standard has been created that gives the requirements and the guidelines that manufacturers must follow for the development.

The adoption of new regulations for the ag-mobile and heavy-duty industry compartments, mandatory for new designs since 2016, is a challenging task since the great machines diversification in terms of functionalities makes it difficult to adopt reusable solutions for the machine design. Therefore, it can lead to a high expenses increase because the development costs are usually distributed on small series. Moreover these machines operate in many different environments so the hazards analysis is rather time consuming and represent a big part of the development project. Many approaches have been developed to cope with these problematics but they are mostly oriented to automotive systems rather than for ag-mobile or heavy-duty vehicles. Therefore, it is important to develop new scalable architectures and components compliant with the specific standards, which can be easily customized for different applications.

This thesis deals with the identification of such architectures and it is the result of a three years research conducted at the IMAMOTER-CNR, Institute for Agricultural and Earth-Moving Machinery. IMAMOTER is a research center focused on different aspects of agricultural machinery, construction equipment and, in general, heavy-duty vehicles. The research staff of the Institute is composed by a group of engineers with diverse specialization and is a national and European excellence for what concerns the hydraulic and electronic control of the hydraulic components, namely mechatronics related to electrohydraulic applications.

In particular the attention has been focused to the analysis of the safety requirements defined by the standards, in order to identify the common principles that can be exploited for the definition of a reference architecture. The key idea of the proposed work is to reduce the software safety requirements, in order to ease the customization of the system for different applications, reducing at the same time, the effort of software certification, which is considered prohibitive for many small and medium sized companies.

The effectiveness of the architecture has been proved realizing an advanced machine controller for agricultural machines that integrates in a single device several safety-relevant functionalities. The activity has been also recognized by FEDERUNACOMA, the Italian Agricultural Machinery Manufacturers Federation, as a reference design for the development of electronic control system compliant with the recently introduced regulations.

The thesis is structured as follows. In Chapter 1 it will be introduced the functional safety basic concepts, with reference to different standards.

Chapter 2 will focus on the architecture design, which is the main result of this thesis. It will be also described an implementation of the proposed architecture for the realization of an advanced machine controller for agricultural machines.

In chapters 3 it will be described the methodologies and development process, carried out during a technology transfer activity, inherent a steer-by-wire system of an innovative 6 wheeled self-propelled agricultural machine.

Finally, Chapter 4 will describe the design of a mechatronic component that represents an innovative solution for the realization of novel electro-hydraulic architectures for heavy-duty machinery. If used singularly, the component is a robust fail silent device that can additionally be used in a stacked configuration. Thus, it realizes a physical matrix that interconnects pumps and actuators in order to provide failure operational features. The work is an extension of the displacement control systems developed at MAHA research center of Purdue University.

Acronyms

E/E/PE: Electrical/Electronic/Programmable Electronic

SIL: Safety Integrity Level

PL: Performance Level

AgPL: Agricultural Performance Level

FMEA: Failure Modes and Effects Analysis

FTA: Fault Tree Analysis

MD: Machine Directive 2006/42/EC

MCS: Machine Control Systems

SRL: Software Requirement Level

MTTF: Mean Time To Failure

DC: Diagnostic Coverage

CCF: Common Cause Failures

TE: Test Equipment

OTE: Output Test Equipment

PTO: Power Take-Off

QM: Quality measures

CC: Cruise Control

MMC: Main Microcontroller

SMC: Safety Microcontroller

SME: Small and Medium Enterprises

LS: Load Sensing

PSM: Pump Switching Matrix

1. Introduction

1.1. What is the "Functional Safety"?

The functional safety, as defined in [1] is "*the part of the overall safety that depends on a system or equipment operating correctly in response to its inputs*" or "*the freedom from unacceptable risk of physical injury or damage*". The functional safety addresses the *Electrical, Electronic, Programmable Electronic* (E/E/PE) parts of a safety-relevant system. Nowadays, with the technology advancements and the integration of E/E/PE systems in many mechanical and hydraulic applications, this might be considered a misconception since the functional safety can also be extended to every system that deals with safety.

The key concepts of functional safety are strictly related to the dependability of a system. According to [2] [3], the objectives of functional safety are:

- the quantification of every potential risks in terms of severity, probability, controllability for every system functionality;
- the identification of safety mitigation which can reduce those risks to tolerable levels, reducing its negative impact in case of failure;
- the validation of the functional safety measures implemented by the system.

When the context of the system changes, the safety properties also change, including those attributes, checks and mechanisms designed to mitigate the risks associated with the system. Therefore, a safety system should be designed to detect hazardous conditions and to switch the machine in a safe condition, e.g. safe stopping, in order to prevent further risks or damages.

1.2. Safety Function and Safety Channel

The safety analysis starts from the evaluation of the safety relevant functions of a system. A *safety function* is the function implemented by E/E/PE system which is intended to achieve or maintain a safe state for the equipment under control, in respect of a specific hazardous event [1].

For each safety function it can be identified a related *safety channel*, which is composed by the components and subsystems which achieve that function. In its simplest form, a channel is composed by an input or a sensor, a logical block, i.e. a microcontroller and an output stage, i.e. an actuator. (figure 1.1)

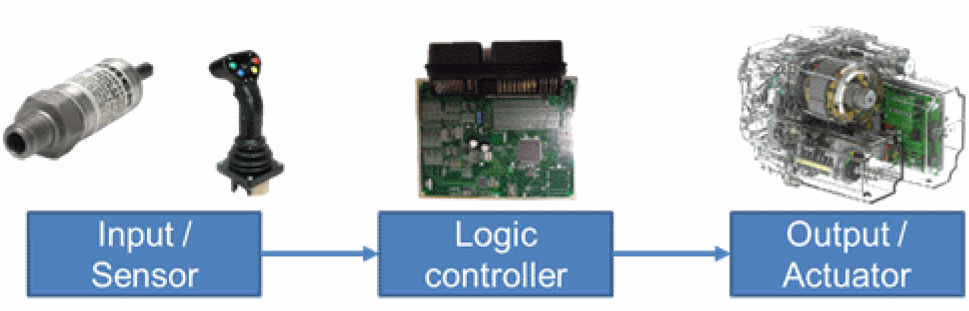


FIGURE 1.1: SAFETY CHANNEL EXAMPLE

The channel architecture affects the dependability of the related safety function. To avoid or minimize a system failure, the general approach is to minimize the risks. This can be achieved by reducing the occurrence probability of the failure cases acting either on the operating time of the safety channel or the failure rate. An alternative approach for risk minimization is to implement an improved control such as a safe shutdown or providing a fault-tolerant system.

The channel architectures can be classified from the point of view of the operation guaranteed in faulty conditions [4]:

- Fail Silent;
- Failure Operational;
- Fault Tolerant

The first class is the simplest to be designed and the related systems are the simplest to be controlled: in case of fault occurrence a safe state is reached and all operations are stopped; normally load lifting and earth moving movements are fail silent functions.

The second class is more complicated, because, in case of fault, an alternative function, that could also be undersized with respect to the main function, shall be provided; sometimes transmissions, more often brakes, throttles are classified failure operational functions.

The third class of machine functions, Fault tolerant functions, are normally available in avionic or military applications and are related to fully redundant systems, in which the systems, even faulty, are able to perform the main function without any limitation, except from the safety level.

The measure of safety performance of a channel defines the *safety integrity level* (SIL) [5] of the E/E/PE system. The higher the level of safety integrity, the lower the likelihood of dangerous failure [2]. The SIL also defines the tolerable risks related to a safety function and consequently the architectural requirement of the channel.

1.3. Risk Assessment

The main purpose of an E/E/PE safety-related system is to prevent and/or mitigate hazardous events introduced by an equipment under control before it may cause damage to people or properties.

With *risk* is intended the probability of hazard occurrence, according to [2] , risks are consequence of failures. The failures are classified in:

- Random failures, which are due to environmental conditions such as corrosion, thermal stressing and wear-out of components.

- Systematic failures: these failure are produced by human error during the system development and operation.

From a practical point of view, the achievement of a zero-risk system is not achievable. As a matter of fact, the recognition of every failure mode cannot be realistically performed in a complex system.

Therefore, objective of functional safety is to ensure that the residual risk, the probability of a hazardous event occurring even with the safety functions in place, is less than or equal to the tolerable risk. The tolerable risk level is defined on the basis of the occurrence of a hazard and to its own degree of severity, it a directly related to the SIL of the system.

Without a precise identification of hazards and failure modes very little can be accomplished to improve the overall safety of a system. Identified hazards, failure modes, and lessons learned become the basis for the identification and implementation of safety requirements within the design of the system.

According to [3] and [6], the hazard analysis is the study of the chains of cause and effect between the identified hazards and the hazardous events to which they might lead. The analysis is intended to determine causes and consequences, so that the risk attached to each hazard can be derived. There are several methodologies used for a hazard analysis, an exhaustive list can be found in [7]. In the next paragraphs will be exposed two of the most important techniques.

1.3.1. FMEA

The *Failure Modes and Effects Analysis* (FMEA) is a methodology for analyzing potential reliability problems at the beginning of the development process. The FMEA process is described by several standards [8] [9] and it consists of the following tasks:

1. Potential failure modes identification. It is not possible to anticipate every mode that a component etc. might fail, but as many modes as possible are identified;
2. Determination of the consequences of the failure;
3. Evaluation of the actions to mitigate the risks

A traditional FMEA uses potential failure modes as the basis of analysis. Therefore, human errors and especially those that do not produce equipment failure are often overlooked. Since the failure mode are analyzed one by one, the combinations of failure modes might be neglected. Environmental conditions, external impacts and other such factors are analyzed in FMEA only to the extent that they produce equipment failures.

1.3.2. FTA

The *Fault Tree Analysis* (FTA) is a graphical method that directly focuses on the modes of failures rather than focusing on the single system or component. [10] It is based on analyzing failures and causes that lead to know hazardous events in a top-down manner. The selected event becomes the root of a reversed tree-diagram, where each node is composed by the sub-events that lead to the parent node. Those sub-events are connected to the parent node with symbols which represent the Boolean logic operators. The diagram ends when the lowest event cannot be further divided into sub-events.

It is important to understand that a fault tree is not a model of all possible system failures or all possible causes for system failure. A fault tree is tailored to its top event that corresponds to some particular system failure mode, and the fault tree thus includes only those faults that contribute to this top event. Moreover, these faults are not exhaustive—they cover only the faults that are assessed to be realistic by the analyst. [11].

1.4. Functional Safety Standards

In recent years, the legislation concerning the functional safety has changed rapidly, trying to keep pace with the technology advancements. In particular, the regulatory framework for automotive, agricultural and heavy-duty vehicles has been completely revisited since the pervasive adoption of E/E/PE systems in these compartments and the migration from mechanical and hydraulic systems to mechatronic solutions.

The international standards are governed by two organizations: *International Organization for Standardization* (ISO) and *International Electrotechnical Commission* (IEC). In many countries, the regional regulations have been harmonized with the international standards produced by ISO and IEC, moving towards a global adoption of those standards [12]. Those harmonized standards are created and recast periodically to ensure they remain applicable and current as time and innovation continue to impact the machinery industry. This process, along with the collaborative efforts of the standards committees, helps ensure that the latest ideas and technology are represented within the resulting standards.

Therefore, the regulatory framework can be considered as a complex relationship between international standards and their accurate knowledge is a mandatory requirement to design architectures and systems that can be used in real world applications. In figure 1.3 is shown a simplified overview of the standards related to the functional safety of mobile machinery.

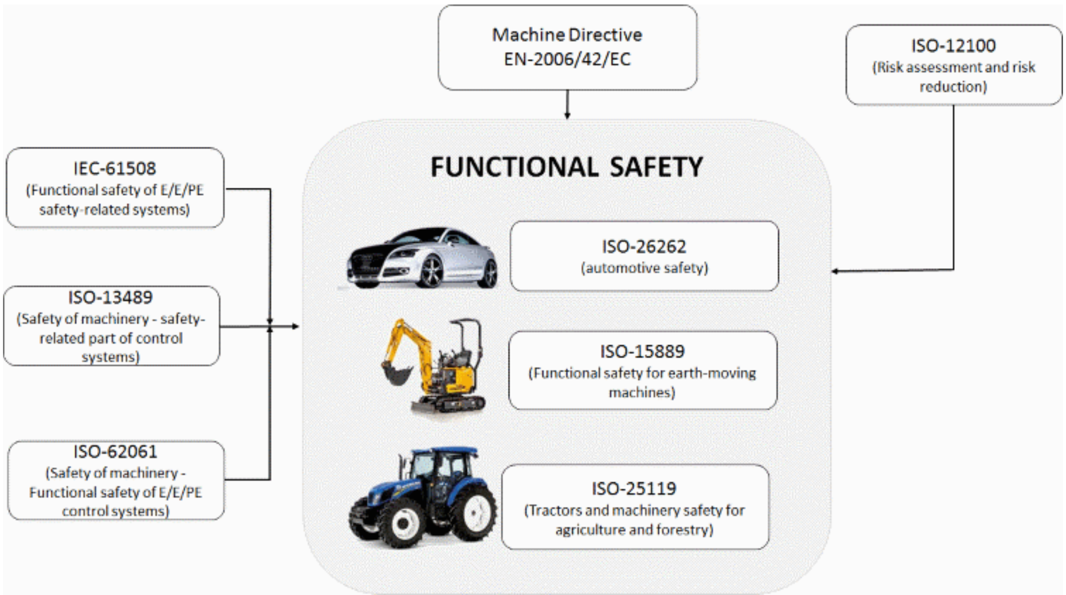

Machine Directive
EN-2006/42/EC
ISO-12100
(Risk assessment and risk reduction)
FUNCTIONAL SAFETY
IEC-61508
(Functional safety of E/E/PE safety-related systems)
ISO-13489
(Safety of machinery - safety-related part of control systems)
ISO-62061
(Safety of machinery - Functional safety of E/E/PE control systems)
ISO-26262
(automotive safety)
ISO-15889
(Functional safety for earth-moving machines)
ISO-25119
(Tractors and machinery safety for agriculture and forestry)

FIGURE 1.2: ISO/IEC STANDARDS RELATED TO THE SAFETY OF MACHINES

1.4.1. Machine Directive 2006/42/EC

The 2006/42/CE, also called *Machine Directive* (MD), can be considered as the highest level standard concerning the safety of machinery and its statute is very general. The MD supersede the previous EN 954-1 [13], introducing a more detailed risks assessment which is now extended to the E/E/PE systems.

The main point of this standard is that manufacturers, are responsible for the safety of their products and they must reduce unnecessary risks even in case of foreseeable misuses. Nonetheless, the norm itself does not specify what can be considered a tolerable risk and the methodologies to perform a safety-aware product design.

The standard refers to several harmonized ISO/IEC/EN standards and define a regulations hierarchy, which aims to cover the whole aspects of machinery safety.

According to the MD, the derived standards are divided into:

- *A-type* standards, which cover the basic concepts, the terminology and the design principles applicable to machinery. These regulations do are not sufficient for granting the MD conformity presumption, although they provide the essential requirement that have to be fulfilled.

- *B-type* standards, they are divided into two sub-categories, *B1-type* and *B2-type*. The first define specific safety aspects of the machines while the latter cover the safety components or the protection devices. The following of *B-type* standards guarantee conformity presumption, according to MD, only if there are no *C-type* standards for the specific application field.
- *C-type* standards, these standards are specific for a category of machines and they either refer to *A-type* or *B-type* standards or define different requirements that prevail on what specified by *A-type* or *B-type* regulations. The application of *C-type* statements grant the conformity presumption and usually they are articulated in several parts, a first part with the general specifications applicable to a machine category followed other parts with the integration to the first part for the different kind of machines, which the category is composed by.

In the following paragraphs a brief overview of most important standards is presented, in order to prepare the research context.

1.4.2. ISO 12100

The ISO12100 – *Safety of machinery -- General principles for design -- Risk assessment and risk reduction* [3] is an *A-type* standard which specifies the fundamentals principles and methodologies for risk assessment and risk reduction.

In 2010 the standard has been merged with ISO14121 – *Risk assessment* [14], unifying the procedures for hazards identification, risks estimation and quantification discussed in previous paragraphs.

The ISO12100 presents a three step process to reduce the risk. The first step is the elimination of hazard through a safety-aware design. The second step is the implementation of complementary protective measures to achieve a risk reduction. The external protective devices have to be used only if hazards cannot be removed through safe design. As a last step, the residual risk has to be reduced providing accurate information about the hazards, i.e. warning signs, warning indicators or by training the user.

1.4.3. IEC 61508

The IEC61508 is an *A-type* standard and it is the root of every standard concerning the safety of E/E/PE systems. It is a very generic and sector independent standard, it introduces several important principles and definitions, which are recalled and specialized by the application specific norms.

Other requirements of the standard are not solely specific to E/E/PE system development, but they also encompass the management of design process, the operation and the system maintenance throughout its whole lifecycle from concept to decommissioning, as shown in figure 1.3. The essence is that all activities relating to functional safety are managed in a planned and methodical way, with each phase having defined inputs and outputs. This enables a process of verification whereby a check is made at the conclusion of each phase to confirm that the required outputs have in fact been produced as planned. The ability to check (or validate) that verification has been properly implemented throughout the safety lifecycle is one of the foundations of functional safety. The premise is that such a structured approach will minimize the number of systematic faults which are built-In to the safety-related system.

The standard is composed by 7 parts:

- Part 1: general system safety requirements, documentation and safety assessment;
- Part 2: specific requirements for E/E/PE safety-related systems, system design requirements;

- Part 3: additional requirements for E/E/PE safety-related systems: software requirements;
- Part 4: definitions and abbreviations;
- Part 5: guidelines and examples for determining safety integrity levels;
- Part 6: guidelines on the application of parts 2 and 3, calculations, modeling and analysis;
- Part 7: techniques and measures to be used to control and avoid faults

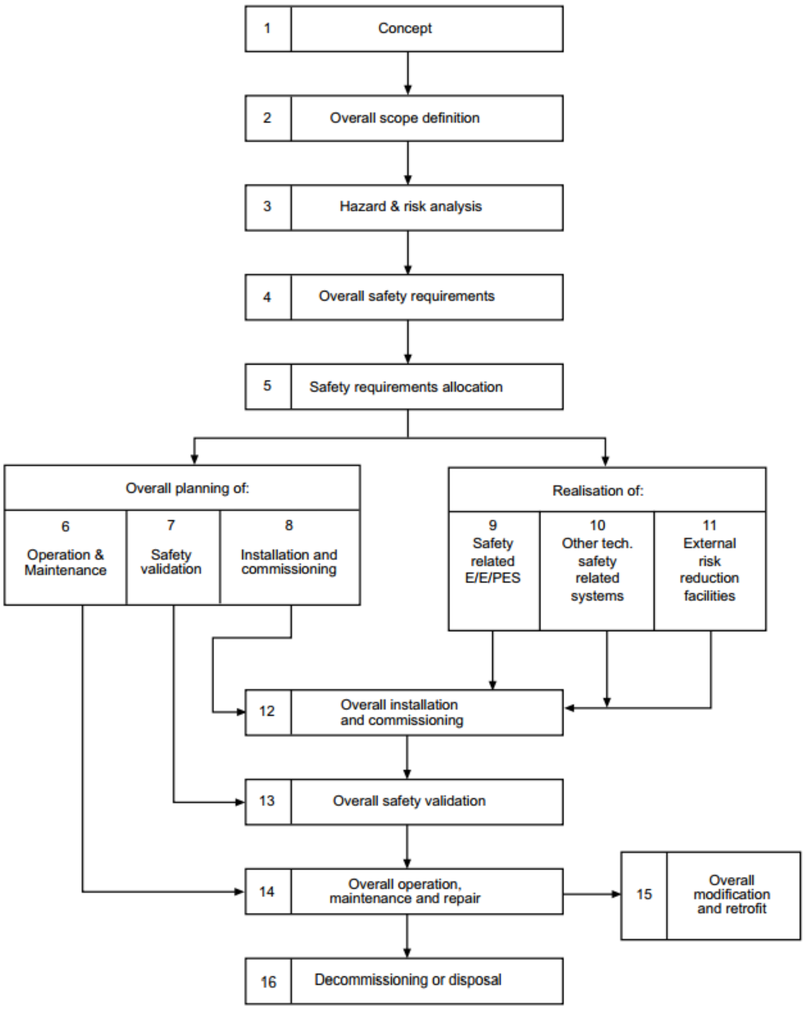

1 Concept
2 Overall scope definition
3 Hazard & risk analysis
4 Overall safety requirements
5 Safety requirements allocation
Overall planning of:
6 Operation & Maintenance
7 Safety validation
8 Installation and commissioning
Realisation of:
9 Safety related E/E/PES
10 Other tech. safety related systems
11 External risk reduction facilities
12 Overall installation and commissioning
13 Overall safety validation
14 Overall operation, maintenance and repair
15 Overall modification and retrofit
16 Decommissioning or disposal

FIGURE 1.3: IEC61508 SAFETY LIFECYCLE

IEC 61508 specifies 4 levels of safety performance for a safety function, defined as SIL. SIL1 is the lowest level of safety integrity and SIL4 is the highest level.

The standard details the requirements necessary to achieve each SIL. These requirements are more rigorous at higher levels of safety integrity in order to achieve the required lower likelihood of dangerous failure. An E/E/PE safety-related system will usually implement more than one safety function. If the safety integrity requirements for these safety functions differ, unless there is sufficient independence of implementation between them, the requirements applicable to the highest relevant SIL shall apply to the entire E/E/PE safety-related system. If a single E/E/PE system is capable of providing all the required safety functions, and the required safety integrity is less than that specified for SIL1, then IEC 61508 does not apply ([5]).

1.4.4. IEC 62061

The IEC 62061 [15] is a harmonized implementation standard for IEC61508, specifically for industrial machinery. The standard is primarily aimed at developers and manufacturers of complex plant and machinery, in particular to machinery which make use of programmable controllers and fieldbus networks for safety functions

1.4.5. ISO 13849

The ISO13849 ([16] [17]) is a *B-type* standard and gives guidance on the design of machinery control systems in order to comply with the safety requirements of the MD. It is applicable on control systems based on electrical, hydraulic, pneumatic and mechanical technologies. It presents strategies and methods that are proven to design systems that avoid, detect and/or tolerate failures in order to reduce hazardous and dangerous situations. The ISO13849 is more focused on electrical systems rather than complex electronics systems. Therefore it does not contain specific software requirements, but it recalls the generic prescription contained in the high level standard ISO62061.

1.4.6. ISO 26262

The ISO26262 [18] is the *C-type* standard related to automotive vehicles for series production with a maximum gross mass up to 3500Kg. The standard defines a set of top-level safety requirements, or safety-goals, that have to be implemented for risk reduction. The safety-goals, both hardware and software, depend on the *Automotive-SIL* (A-SIL) demanded the system, which definition differs from SIL of [5].

1.4.7. ISO 15998

The ISO15998 ([19] [20]) is the C-type norm specific for earth-moving machinery and it embraces the *electronic machine control systems* (MCS) as well as the mechanical, hydraulic systems involved in safety functions.

The standard gives a guidance for risk assessment and for the identification of required SIL as demanded by [5]. The norm defines a series of parameters that has to be considered for the functional safety analysis:

- Climatic conditions (i.e. temperature, humidity)
- Mechanical condition (i.e. vibration, shock)
- Corrosion conditions (i.e. salt spray, gas pollution)
- Electromagnetic compatibility
- Power source voltage fluctuation.

The ISO15998 also gives some examples for the hazards analysis of some safety functions such as steering, braking, propel and operating.

For MCS with SIL ≥ 1, the manufacturer must document system fault detection and tolerance mechanisms. A safe-state be achieved in the case of a malfunction or failure of a safety MCS, providing reduced system performance or a substitute function. The ISO15998 also considers the communication buses involved in a safety-related function, defining a model for the transmission of safety related message according to the ISO/OSI model.

1.4.8. ISO 25119

The ISO25119 is the C-type standard for agricultural and forestry machinery. The standard is composed by four parts ([21] [22] [22] [23]) and it defines the safety requirements for the safety-related parts of a control system. It inherits many safety principles from the ISO26262, particularly by placing a strong focus on the identification of the safety requirements both for hardware and software.

The standard enforce the adoption of a V-model for the overall safety lifecycle. This model defines a sequential path of execution of processes, each phase must be completed before the next phase begins. Each level of the development lifecycle has a corresponding test plan, as each phase is being worked on, a test plan is developed to prepare for the testing of the products of that phase. (depicted in figure 1.4)

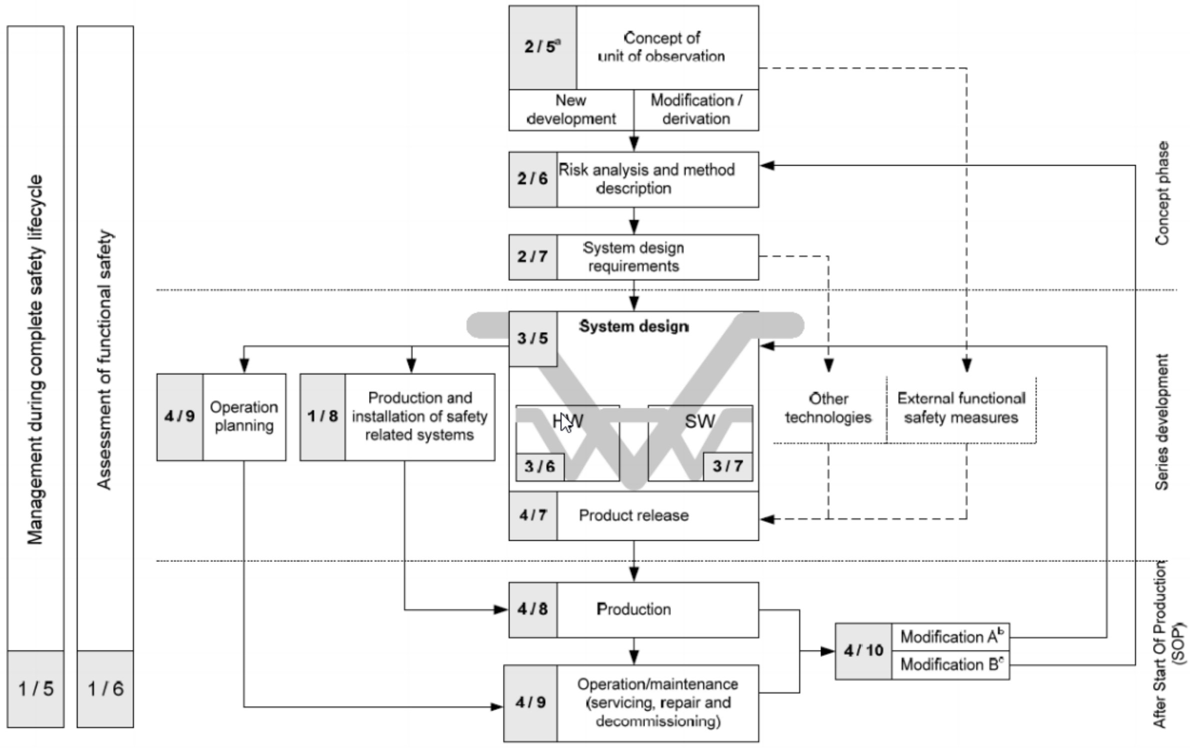

Management during complete safety lifecycle
1 / 5
Assessment of functional safety
1 / 6
2 / 5a
Concept of unit of observation
New development
Modification / derivation
2 / 6
Risk analysis and method description
2 / 7
System design requirements
3 / 5
System design
HW
SW
3 / 6
3 / 7
4 / 7
Product release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

FIGURE 1.4: ISO25119 SAFETY LIFECYCLE (V-MODEL)

The ISO25119 recalls the SIL level of [5] defining the *Agricultural Performance Level* (AgPL) concept. The achievement of a specific AgPL is made on the basis of several factors such as, hardware category, *the mean time to failure* (MTTF) of the components, *diagnostic coverage* (DC), *common cause failure* (CCF) and *software requirement level* (SRL).

1.5. Safety Principles Introduced by the Standards

All the standards exposed in the previous paragraphs deal with the functional safety of E/E/PE systems, but with a slightly different approaches borrowed from the IEC61508. These differences are at odds with the design of reusable methods and architecture for machinery development.

Nonetheless, it is possible to outline some common aspects that have to be considered for the determination of the functional safety requirements:

- The component reliability (MTTF);
- The channel diagnosis capabilities (DC);
- The hardware architecture of safety-related E/E/PE systems;
- The software components.

The analysis of these concepts will be exploited for the research of a reference architecture presented in next chapter.

1.5.1. Mean Time to Dangerous Failure

This represents the average mean time in years before the occurrence of a failure that could lead to the failure of the safety function. The MTTF can be considered as a measure for the quality of the component, its value is usually provided by the manufacturer or it can be obtained from statistical tables as [24]. In absence of data it can be considered equals to ten years.

For the functional safety analysis the MTTF has to be calculated for all the components of that compose the channel. The ISO13849 in [16] defines the formulas to determine the overall MTTF for single or dual channel system.

For a single a single channel is defined the formula 1, Where MTTF$_i$ is the MTTF value of the single component of the channel. For a dual channel systems there are two scenarios. The lowest MTTF of the two channel can be chosen for the system, according to the worst case scenario, otherwise the formula 2 can be used for the MTTF calculation. In the formula 2 MTTF$_{c1}$ and MTTF$_{c2}$ are respectively the MTTF of the first and second channel.

$$MTTF = \frac{1}{\sum_{i=1}^{N} \frac{1}{MTTF_i}} \qquad (1)$$

$$MTTF = \frac{2}{3}\left[MTTF_{c1} + MTTF_{c2} - \frac{1}{\frac{1}{MTTF_{c1}} + \frac{1}{MTTF_{c2}}}\right] \qquad (2)$$

For mechanical or mechatronics components it may be difficult to calculate the MTTF, which is given in years and which is required by this part. Most of the time, the manufacturers of these kinds of components only give the mean number of cycles until 10 % of the components fail dangerously (B$_{10d}$). The formula 3 gives a method for calculating a MTTF for components by using B$_{10d}$ given by the manufacturer and n$_{op}$ which is the number of cycle in a year. The parameter n$_{op}$ is calculated with formula 4, where d$_{op}$ is the number of working days in a year, h$_{op}$ is the number of working hours in a day and t$_{cycle}$ is the interval between the cycles.

$$MTTF = \frac{B_{10\mathrm{d}}}{0.1 * n_{op}} \qquad (3)$$

$$n_{op} = \frac{d_{\mathrm{op}} * h_{\mathrm{op}} * 3600\ \mathrm{s/h}}{0.1 * t_{cycle}} \qquad (4)$$

1.5.2. Diagnostic Coverage

The diagnostic coverage is the ratio of the probability of detected dangerous failures to the probability all the dangerous failures. The diagnostic coverage is defined by the formula 3, where λ_{dd} is the detectable failure rate and λ_{du} is the total dangerous failures rate.

$$DC = \frac{\lambda_{dd}}{\lambda_{dd} + \lambda_{du}} \qquad (3)$$

1.5.3. Common Cause Failure

The common cause failures (CCF) occur when two or more component fail at the same time or within a specified time due shared causes. The CCF can be caused from random failures or systematic failures made in the lifecycle of the system and replicated for several components.

Especially in redundant systems, they have to be carefully evaluated. Redundancy alone does not guarantee fault-tolerance, it is of paramount importance how redundancy is managed.

A successful risk analysis should identify the root-cause that may lead to failure and the potential susceptibility to a failure mode of a group of components. Moreover the diversity and independence between channels should be maximized.

The ISO13489 and ISO25199 gives a method to analyze the CCF, defining a checklist of countermeasure. The implementation of each countermeasure gives a certain score, the points are summed up to a total score, which define the addressing of the potential CCF as a percentage. The score table covers the following areas:

- Separation/Segregation of signal path or cables. The intention is to avoid interferences between redundant channels.
- Diversity in technologies, design or physical principles. The intention is to reduce the probability of a fault affecting both channels. An example is different sensitivity to electromagnetic interference in different

components or the application of diversity in software to reduce the risk of a programming mistakes affecting both channels.

- Design and application experience. This area considers if there is an external factor that could affects both channels and if the components have been successfully used in the same environmental conditions.
- Failure mode and effect analysis covering CCF failures. The intention is to identify critical components of the design and reduce the probability of a fault appearing in both channels.
- Suitable design with respect to environmental impact. Environmental aspects may affect both channels at the same time. An example is that EMC performance of the design has been tested and approved. This will reduce the probability of a disturbance affecting both channels.

1.5.4. Hardware Categories

The hardware categories describe the architectural design requirement for a safety channel. The categories differ from monitoring and redundancy point of view. The ISO25199 and ISO13489 define five types of hardware categories with almost identical requirements.

The simplest categories, such as the category B and category 1, are composed by a single logical blocks that acquire inputs and controls outputs.

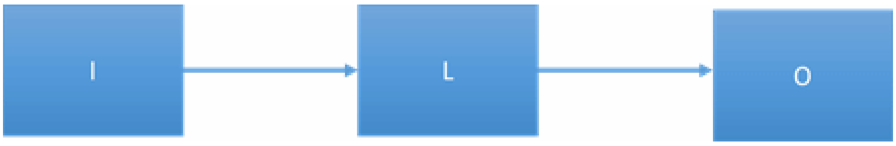


FIGURE 1.5: HARDWARE CATEGORY B OR 1

The category 1 differs from B for the adoption of *well-tried* components, which are been used with successful results. Furthermore it provides a high DC that contribute to lower the fault occurrences in respects of the category B. These categories do not provide any kind of fault tolerance and therefore they are not suitable for safety related functions.

The hardware category 2, as showed in figure.1.6, is composed by an electronic programmable block *L* that operates on the signals from the input block *I*, in order to drive the output state of the block *O*. In category 2 implementation safety function might be lost due to single fail, but a safe state is achieved.

The architecture requires a supervisor block, the *Test Equipment* (TE) which periodically checks the input, the logical block and the output. The TE can drive the system into the safe-state through the *Output Test Equipment* (OTE).

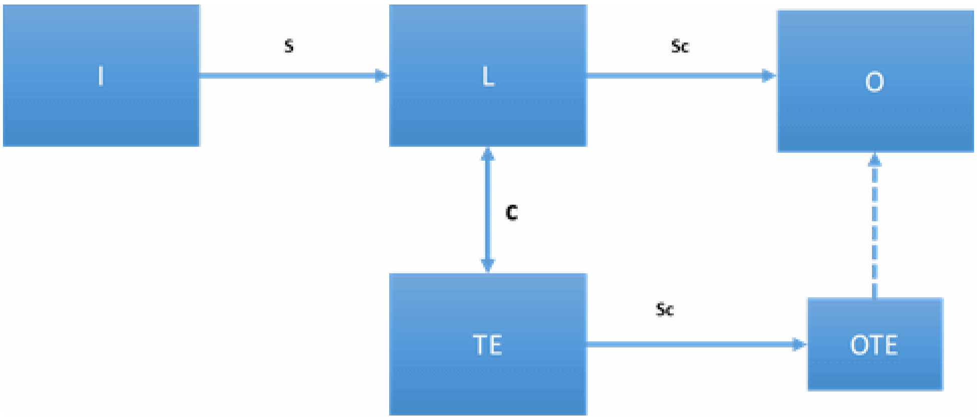


FIGURE 1.6: HARDWARE CATEGORY 2

The category 3, depicted in figure 1.7, provides a fail-operational channel, which can perform the safety function even in during a single fault. This can be achieved implementing a multi-channel system, where two channel performs the safety function. In addition to this, the outputs are monitored by feedback signals to detect unexpected behaviors and to extend the diagnostic coverage.

The category 4 is similar to category 3, but the required MTTF of the channels and the diagnostic coverage are improved to achieve the maximum degree of dependability.

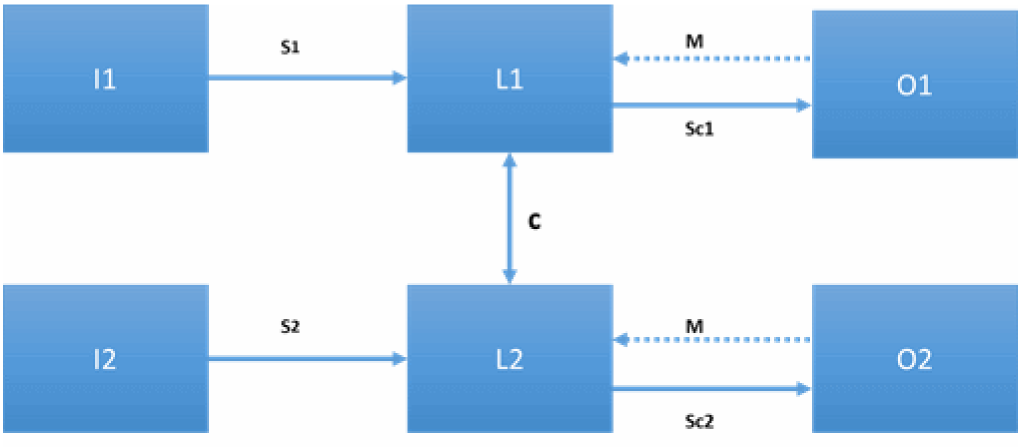


FIGURE 1.7: HARDWARE CATEGORY 3 OR 4

1.6. Determination of Safety Integrity Requirements

The safety integrity requirements are indicated with different names, such as SIL, PL or AgPL in according with the considered standard. They are qualitative estimated by a tabular risk graph depending on the results of risk assessment.

1.6.1. ISO13849 Performance Level

The ISO13849 estimate the PL_r according to three parameters:

- **Severity of injury**: *S1* for reversible injuries and *S2* irreversible injuries.
- **Frequency of occurrence**: It should be evaluated on the basis of an average value which can be seen in relation to the total period of time over which the machine is used. *F1* is demanded for low exposure while *F2* is demanded for the cases where there is a frequent or continuous exposure.
- **Possibility of avoiding the hazard:** this parameter identify the possibility of hazard recognition and avoidance before an incident. *P1* should only be selected if there is a realistic chance of avoiding an accident or of significantly reducing its effect; *P2* should be selected if there is almost no chance of avoiding the hazard.

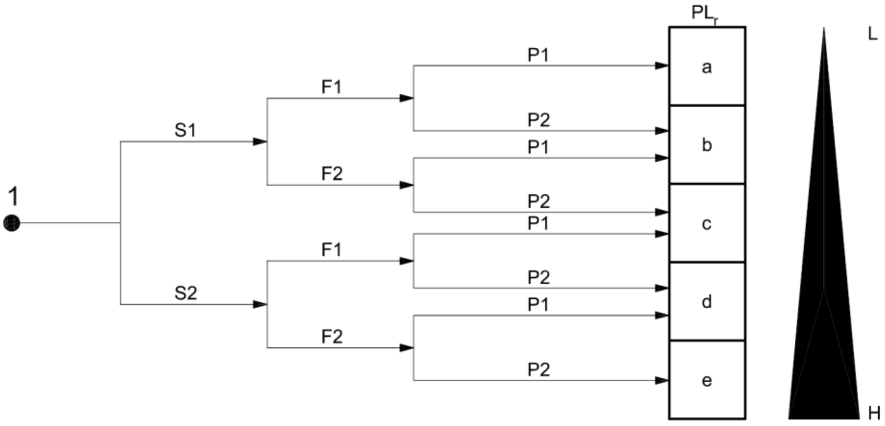


FIGURE 1.8: ISO13849 RISK GRAPH

From the estimation of these parameters, the PL required for the specific safety function can be identified using the risk graph of figure 1.8. The requested PL can be achieved with different combinations of hardware category, MTTF, and DC as shown in table 1.1. It is important to remark that the standard covers E/E/PE, mechanical and hydraulic systems, however it explicitly makes reference to other higher standards, as IEC61508 and ISO62061, for the software safety requirements.

TABLE 1.1: DETERMINATION OF PL ACCORDING TO ISO13849

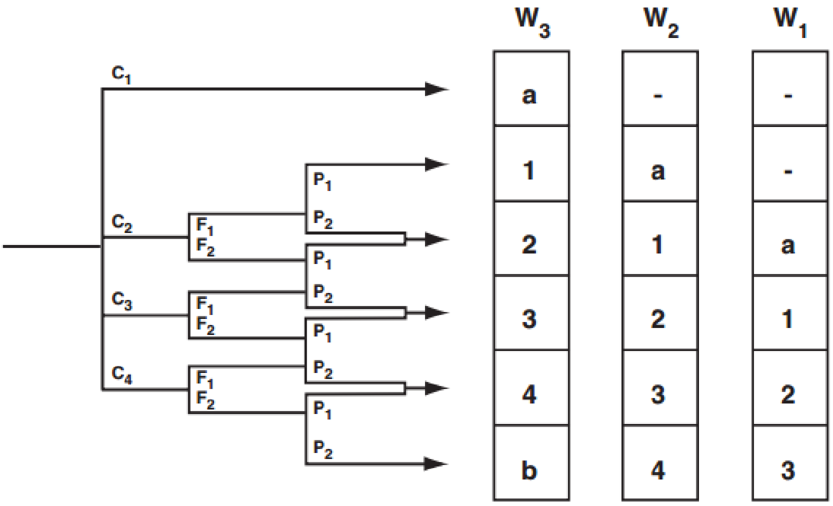
Category	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC$_{avg}$	**None**	**None**	**Low**	**Medium**	**Low**	**Medium**	**High**
MTTF							
Low	A	-	A	B	B	C	-
Medium	B	-	B	B	C	C	-
High	-	C	C	D	D	D	E

1.6.1. ISO15998 Performance Level

The definition of PL is slightly different for the ISO15998, the *severity* parameter of ISO 13849 has been replaced by the *consequence* (C) parameter which is composed by four levels:

- *C1*: minor injury;
- *C2*: Serious permanent injury to one or more persons or death to one person;
- *C3*: Death to several people;
- *C4*: many people killed.

For the estimation of the PL, the standard also considers the reductions achieved by other measures (for example by other technology SRS and external risk reduction facilities), introducing a scale factor *W*. The risk graph for the determination of the PL is reported in figure 1.9.



W_3	W_2	W_1
a	-	-
1	a	-
2	1	a
3	2	1
4	3	2
b	4	3

FIGURE 1.9: ISO15998 RISK GRAPH

The ISO15998 is substantially similar to ISO13849 for the components modelling and for the determination of architectural parameters, such as MTTF, DC and hardware category required for a specific PL. Since the similarity between the two standards, in this thesis will make reference to ISO 13849 for the heavy-duty vehicles.

1.6.2. ISO25119 Agricultural Performance Level

The AgPL is determined according to three parameters: severity, exposure and controllability.

The standard presents a different classification of the severity:

- *S0*: no significant injuries;
- *S1*: light and moderate injuries that require medical attention;
- *S2*: severe and invalidating injuries;
- *S3*: fatal injuries.

The *exposure* (E) parameters is an estimation of how often and how long an operator or bystander is exposed to a hazard where a failure could result in an injury. It is calculated as:

$$E = \frac{t_{exp}}{t_{avop}}$$

Where:

- t_{exp} is the exposure time by operator or bystander;
- t_{avop} is the average operating time for function in question.

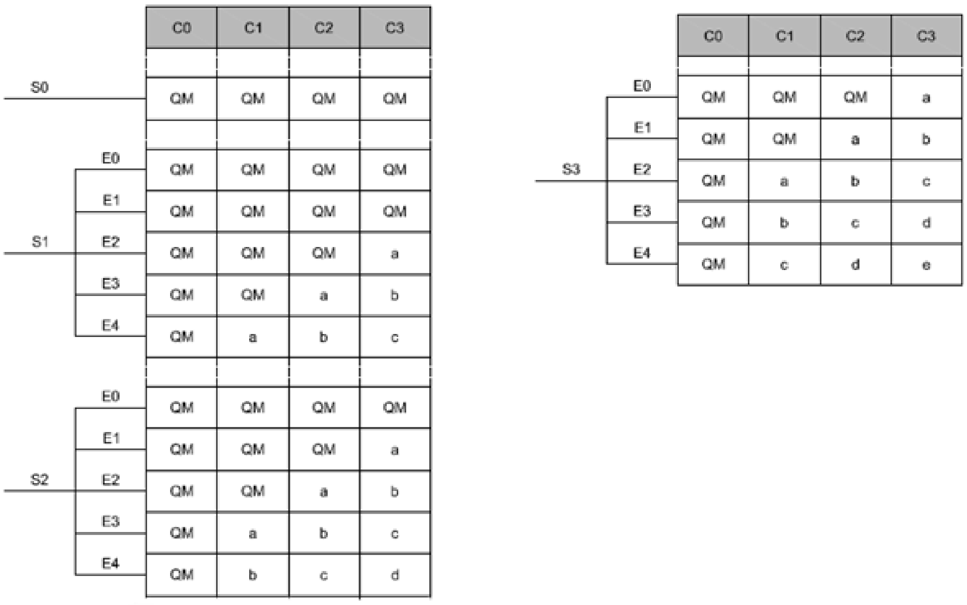
Five exposure categories quantify the probability:

- *E0*: improbable events, E < 0.01%;
- *E1*: rare events, 0.01% < E < 0,1%;
- *E2*: occasional events, 0.1% < E < 1%;
- *E3*: common events, 1% < E < 10%;
- *E4*: frequent events, E > 10%.

The *controllability* (C) is the assessment of possible avoidance of harm and it is classified in:

- *C0*: easily controllable, the harm can be avoided even by un-trained operator or bystander;
- *C1*: controllable, in more than 99% of occurrences the harm can be avoided;
- *C2*: mostly controllable in more than 90% of occurrences the harm can be avoided;
- *C3*: not controllable, the average trained operator or the bystander cannot generally avoid the harm.

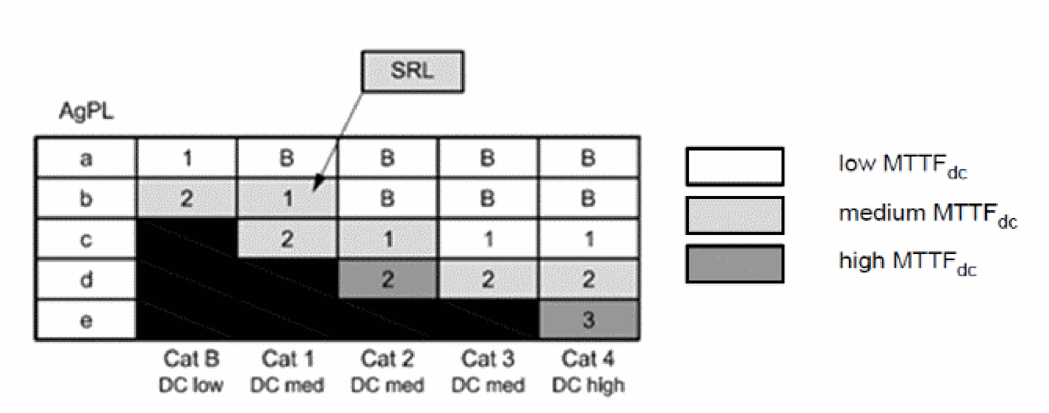
The risk graph of the ISO25119 is reported in figure 1.10. The standard classifies five different AgPL, from A to E plus a the general *Quality measures* (QM) level for the not relevant safety function.



		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

FIGURE 1.10: ISO25119 RISK GRAPH

In respect to the two previous standards, the ISO25119 is only appliable to E/E/PE system of safety channel and it do not cover the mechanical or hydraulic parts of the machine. Moreover it defines a specific set of software requirements which concur to the determination of the AgPL. The entire part 4 of the standard ([25]) is dedicated to the definition of the safety requirements for the software. These requirements will be explained in the next chapter. In figure 1.11 is reported the combinations of parameters to obtain the required AgPL.



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

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

FIGURE 1.11: DETERMINATION AGPL ACCORDING TO ISO25119

1.7. Aim of This Thesis

The analysis of the standards highlights that a functional safety evaluation of a system can be carried out with different approaches. Considering the growing importance of E/E/PE systems in agricultural machines and heavy-duty vehicles, the fulfilment of these standards has heavy implications of the machine design.
In this thesis the attention has been focused on the recognition of a common ground between different standards, especially the ISO13849 and ISO25119 that can be used for the safety-aware design of scalable system architectures and mechatronic components.
The main result of the thesis is the identification of an architectural archetype that provides an elevate performance level through robust hardware solutions in order to reduce the software safety requirements. This simplify the customization for different applications, minimizing the efforts required for the functional safety analysis. The prosed architecture has been used to implement a universal machine controller for agricultural machines that integrate several safety-

relevant functionalities and it has also been adopted by FEDERUNACOMA, as a reference design for the development of safety critical systems.

For a comprehensive evaluation of the functional safety, the focus cannot only be centered on the electronic systems but it must comprise all the systems involved in a safety function. This idea has been exploited during a technology transfer activity to reduce the performance level required by a steer-by-wire system for a 6 wheeled agricultural self-propelled machine. The design of the steering system has been completely revisited in order be compatible with the market reference price requested by the company.

In the last part of the thesis it will be presented a new mechatronic component, that is an enhancement of the displacement control system [26] presented by the MAHA research center of the Purdue University. This component has been designed in conjunction with other IMAMOTER researchers to allow the design of highly integrated and safety-oriented hydraulic-circuit architectures. The key idea is to design a component intrinsically safe, using double redundancy actuator that provides a fail-safe approach. Furthermore, the component can be stacked to realize a physical matrix where multiple pumps can be connected at the same time to a single actuator.

2. Scalable Safety-oriented Architecture for Agricultural Machines

The complexity increase of electronics control system in this agricultural and heavy-duty vehicles demands the development of new architectures which must deal with functional safety requirements defined in ISO25119, ISO13849 and ISO15998. The compliance with these standards makes difficult to develop reusable architectures and leads to a tremendous increase of the design costs, since the great diversification of agricultural machines and their relative small market.

In this chapter will be analyzed the safety requirements demanded by those standards, in order to identify common architectural solutions. In particular it will be presented a scalable architecture designed for safety-related function on agricultural machines, which can be also extended to heavy-duty vehicles due to its generality. From the analysis of the functional safety functionalities, it has been selected the optimal trade-off between the software and hardware requirements. The proposed architecture has been also implemented in a real application, for the development of an advanced machine controller. in compliance with ISO25119.

2.1. Identification of the Safety Requirements

The standards are quite generic about the solutions that have to be developed to achieve a specific PL/AgPL. Nonetheless, some principles can be recognized by the review of the standards. For each safety function must be defined a *safe-state* where the system is driven in case of failure, in order to minimize the risks and to avoid further hazards.

The system architecture also depends on the fault-tolerance demanded by the safety function. In the simplest case it can be deactivate in case of failure, implementing fail-silent approach, whereas for the most critical functionalities, it has to be implemented a fail-operational channel or even a fail-tolerant safety channel. This aspect comprises several architectural factors, such as the MTTF of the components, the DC of the channels, the CCF and the hardware category. Depending on the considered standard, these parameters contribute in different ways to the achievement of the required PL/AgPL, as presented in table 1.1 and figure 1.10.

The main difference between the two standards lies in the safety requirements demanded to the software. ISO13489 defines a set of general safety requirements, it states that *"software can be considered as "black box" or "gray box" and validated by the black-box tests or grey-box tests respectively."* ([16]). On the contrary, ISO25119 introduces the concepts of SRL, that recalls the automotive software requirements defined by [18]. The entire part 3 of the standard is devoted the description of the methodologies and requirements that must be used for the software development according to the required AgPL.

Whereas the hardware architectural requirements refer to common functional safety principles for the different standards, the approach of ISO25119 to the software safety is completely different than other standards. The development of safety-related software, according to ISO25119, is a challenging task, complex tools and methodologies are required both for the design and certification phase. This is especially true for the small and medium sized companies that usually do not have the budget or knowledge to deal with the development of safety-critical software. The key idea of the proposed architecture is to lower the demanded SRL, hardening the hardware aspects. By doing this, the achievement of a specific PL/AgPL is independent from the software implementation and therefore it that can be customized on the basis of application. In the next paragraph will be exposed the SRL defined in ISO25119.

2.2. Software Safety Requirements

The part 3 of ISO25119 deals with the definition of the software requirements. It defines a V model even for the software development phase, as shown in figure 2.1.

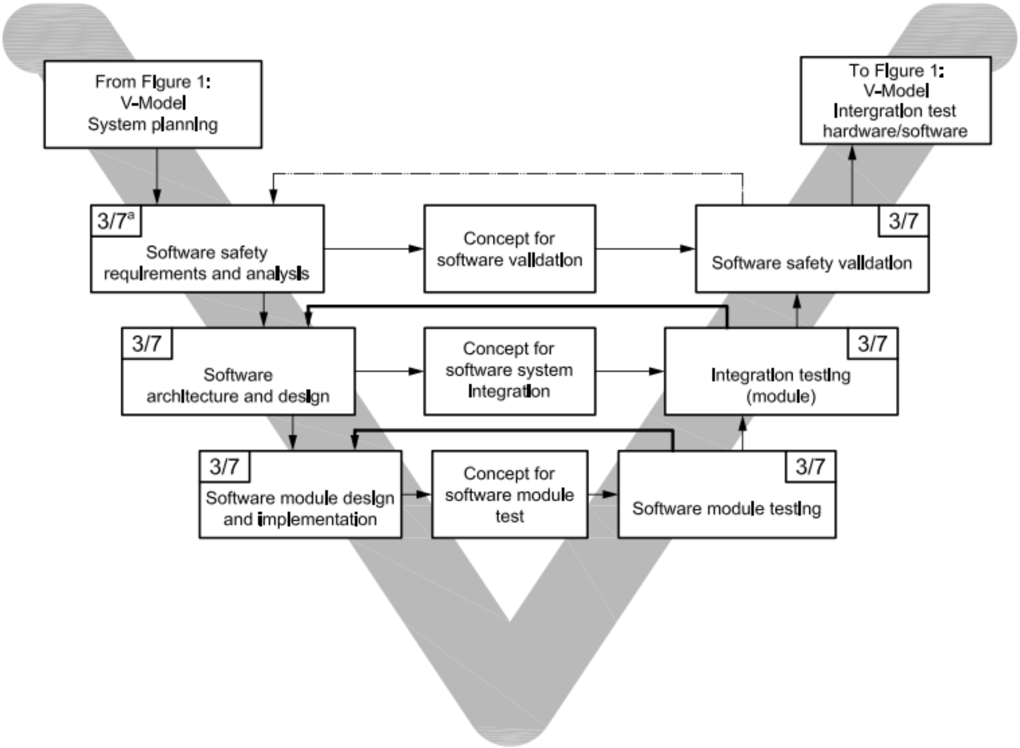


FIGURE 2.1:ISO25119 SOFTWARE DEVELOPMENT CYCLE

Depending from the SRL, the software specifications have to be implemented in natural language, with semi-formal methods or informal methods. Since many logical errors are due to poor specification, the objective of semi-formal/formal methods is to avoid the semantical or syntactical ambiguities of natural language. With semi-informal methods the software requirements are expressed with state-transition flowcharts, UML diagrams and finite-state machines whereas, with formal methods, they are expressed in mathematical language.

To improve the overall safety of the software life-cycle, the standard also encourage the adoption of software management and versioning tools, to record the software changes. For the highest SRL is mandatory the utilization of project management tools, i.e. [27], [28], that keep track of the requirements, to perform automatic inspections in order to assess their consistency and completeness.

For SRL ≥ 1 is required a strongly typed programming language as ADA, JAVA. Since the very limited diffusion of such languages on embedded platforms, especially for the ag-mobile and heavy duty compartments, some languages subsets are considered as an alternative, i.e. [29], [30].

For SRL ≥ 2 is recommended the usage of well-tried tools and libraries for software implementation, in order to simplify the code verification, validation and maintenance. Even the use of defensive programming techniques is recommended to decrease the likelihood of erroneous data processing and to control the software execution flow. Some defensive programming techniques include: range and plausibility check of variables, separation between read-only and write-only memory areas, dynamic control of underflow/overflow events.

The standard also defines some general programming practices that have to be fulfilled even for low SRLs. The software should be organized in small modules which are practical to be analyzed without the code execution. The use of interrupts should be limited as well as the recursive functions in order to control the function execution time. Complex branching and the use of non-structured constructs, i.e. *goto* statement, has to be avoided. The use of dynamic memory allocation is restricted for the highest SRL.

One of the most demanding part of the software development process consists in the software validation, which is composed by three steps: module tests, integration tests and safety validation. For the module test is prescribed an individual test for each software requirement. Depending on the SRL, module test may require the usage of static and dynamic analysis [31], [32]. The integration test aims to verify the co-existence of software module on the same platform, analyzing the performance, the function portioning and the workload of the system. Afterwards, the software safety requirements are tested. For the SRL < 1 this involves the test of ECU in a network with other ECU. For SRL ≥ 2 is demanded a hardware-in-the-loop testing which requires expensive tools such as [33], [34]. For the highest SRL the software must be tested in a real environment and for every possible configuration.

In the table 2.1 is shown a comparison between the most important requirements demanded by the various SRL. The "+" symbols stands for demanded whereas "-"stands for not requested for the specific SRL.

TABLE 2.1: SOFTWARE REQUIREMENTS FOR A SPECIFIC SRL

Requirements	**SRL=B**	**SRL=1**	**SRL=2**	**SRL= 3**
Informal design methods	+	+	+	+
Semi-formal / formal design methods	-	-	+	+
Computer-aided specification tools	-	-	+	+
Strongly typed language or subset	-	+	+	+
Use of trusted or verified software	-	-	+	+
No dynamic variables or objects	-	-	-	+
Static code analysis	-	+	+	+
Dynamic module test	-	-	+	+
Resource budget testing	-	+	-	-
Performance requirements testing	-	-	+	+
Hardware-in-the- loop tests	-	-	+	+

To summarize, with the ISO25199 gives to the software development process a key importance. The design of software compliant with the standard may represent a big part of the overall design process, especially for SRL ≥ 2. The required usage of formal and semi-formal methods demands a level of computer science knowledge not common in the industry. Moreover at increasing of the SRL, also increase the number of tests required for the software validation. In particular, test case execution from boundary value analysis may is extremely demanding. A complete coverage of all the possible inputs values can be achieved with the usage of complex and expensive tools, such as [35] and [36], which are typically used for avionics or automotive compartments.

2.3. Analysis of Safety-related Functionalities of Agricultural Machines

As discussed in 1.6.3 the AgPL depends on the requirements of the safety functions and from the result of risk analysis performed with the method FMEA methods.

Performing a comprehensive list of safety-related functions for ag-mobile is not a trivial task due to the range of different machines. For this research it has been evaluated a set of most important functionalities, such as:

- Automatic gear splitter;
- Engine;
- Auxiliary electro-valves;
- 3-point hitch;
- PTO;
- 4 Wheel Drive;
- Cruise control;
- Differential lock.

In the next paragraphs will be presented the results of the FMEA and the recognized safe-state.

2.3.1. Automatic Gear Splitter

For the automatic gear splitter it has been considered several failure modes, as reported in table 2.2. The most critical failures are the missed gear engagement and the unwanted gear engagement because they can lead to severe injuries to the bystanders and have an exposure equal to E3. The required AgPL for these functionalities is C and the related safe-state is the gear splitter disengagement.

For what concerns the transmission lock and the missed engagement of neutral gear have the same severity level of the previous failure modes but they are less frequent. The required AgPL for these functionalities is B, the de-energization of transmission actuators or the forced engagement of neutral gear can be considered as a safe-state.

A missed up or down shift by the automatic splitter only require a warning to the operator due to the severity equal to S0.

TABLE 2.2: GEAR SPLITTER HAZARD ANALYSIS

Hazard description	Severity level	Exposure level	Controllability	Required AgPL	Safe state
Missed gear engagement	S2	E3	C3	C	Gear splitter disenagement
Unwanted gear engagement	S2	E2	C3	C	Gear splitter disenagement
Undesired transmission lock	S2	E2	C3	B	Forced shifting to neutral / De-activation of actuators
Missed shift to neutral gear	S2	E3	C2	B	Forced shifting to neutral / De-activation of actuators
Automatic gear up/down shift	S0	E2	C1	QM	Warning to operator

2.3.2. Auxiliary Valves

TABLE 2.3:AUX VALVES HAZARD ANALYSIS

Hazard description	Severity level	Exposure level	Controllability level	Required AgPL	safe state
Undesired function activation	S3	E3	C1	B	De-energization of hydraulic system
Undesired function deactivation	S0	E3	C2	QM	Warning to operator
Oil flow lowering	S3	E3	C2	B	System restart
Oil flow increasing	S3	E3	C2	B	De-activation of hydraulic system
Undesired valve stops	S3	E3	C2	B	De-activation of hydraulic system

The consequence of a failure on an auxiliary valve may lead to sudden activation of the implement connected to it, hence, to a potential risk for operators or bystanders located nearby. The auxiliary valves failure modes have an AgPL requested equal to B in most of the cases and the identified safe-state is the de-energization of hydraulics. The undesired deactivation of a valve is coincident with the safe-state, so it does not has to be considered.

2.3.3. Hitch Controller

TABLE 2.4: HITCH HAZARD ANALYSIS

Hazard description	**Severity level**	**Exposure level**	**Controllability level**	**Required AgPL**	**Safe state**
Undesired fast rising function activation	S3	E3	C1	B	System stop
Undesired fast lowering function activation	S3	E3	C2	C	System stop
Unable to maintain requested position	S2	E3	C2	B	System stop

The hitch controller has several implication on functional safety. It is used to lift weights or implements such as plows or tiller and it can be manually activated by commands located outside of the cabin. Hence, an unwanted activation of the hitch, especially a fast lowering activation, may lead to severe harm for both operator and bystanders.

2.3.4. Engine Controller

TABLE 2.5: ENGINE HAZARD ANALYSIS

Hazard description	Severity level	Exposure level	Controllability level	Required AgPL	Safe state
Undesired vehicle acceleration	S2	E4	C1	B	RPM limitation
Undesired vehicle deceleration	S2	E4	C1	B	RPM limitation
Undesired PTO acceleration	S2	E4	C1	B	RPM limitation
Undesired PTO deceleration	S0	E4	C0	QM	No action

A failure of the engine channel may lead to unwanted accelerations/decelerations, with risks for the operator and for the bystanders. The analysis must considers even the effect of engine control system failure of the PTO, since the torque applied to the PTO is related to the engine speed.

2.3.5. 4 Wheel Drive

TABLE 2.6: 4-WHEELS DRIVE HAZARD ANALYSIS

Hazard description	Severity level	Exposure level	Controllability level	Required AgPL	safe state
Undesired activation	S0	E4	C3	QM	Warning to operator
Undesired deactivation	S1	E4	C1	A	Warning to operator

The risks related to an unwanted activation/deactivation of the 4 wheel drive are negligible. The operator can control the failure in most of the cases. Since the deactivation may lead to a loss of stability in some conditions the required AgPL is A.

2.3.6. Differential Lock

An undesired activation of the differential lock forces the wheels on the axle to rotate at the same speed, leading to understeering problems. This hazardous situation has severe implications on operator or bystander safety and therefore the requested AgPL is C. When this condition is detected, the vehicle speed must be limited to prevent hazardous situations.

TABLE 2.7: HDL HAZARD ANALYSIS

Hazard description	**Severity level**	**Exposure level**	**Controllability level**	**Required AgPL**	**Safe state**
Undesired activation	S3	E3	C2	C	Speed limitation
Undesired deactivation	S0	E2	C3	QM	Warning to operator

2.3.7. Power Take-off

The PTO is used to transmit power from the engine to connected implements. In direct drive mode the PTO speed is directly proportional to engine RPM, while in ground drive its speed is proportional to wheel speed. The PTO is one of the common cause of injuries on agricultural machines, as for the hitch, the PTO may be engaged from outside of the cabin and the operator is exposed to hazards during the attachment/detachment of an implement.

TABLE 2.8: PTO HAZARD ANALYSIS

Hazard description	Severity level	Exposure level	Controllability level	Required AgPL	safe state
Undesired direct mode activation	S3	E3	C2	C	PTO deactivation
Undesired direct mode deactivation	S0	E4	C2	Qm	PTO deactivation
Rotational speed higher than requested	S2	E3	C1	A	PTO speed limitation
Undesired ground drive activation	S2	E3	C2	B	PTO deactivation
Undesired ground drive deactivation	S1	E3	C3	A	PTO deactivation
Simultaneous activation of direct and ground drive	S3	E3	C2	C	PTO deactivation

2.3.8. Cruise Control

The *cruise control* (CC) system has to retain the speed set-point settled by operator. It does not directly driving the engine RPM and it is automatically disengaged by the press of clutch or brake pedal. The unwanted activation, the missed set-point reset or a failure on speed decrease command require an AgPL equal to A.

TABLE 2.9: CRUISE CONTROL HAZARD ANALYSIS

Hazard description	Severity level	Exposure level	Controllability level	Required AgPL	Safe state
Undesired activation	S2	E3	C1	A	CC deactivation
Wrong speed increase	S1	E3	C1	Qm	CC deactivation
Missed set-point erasing	S2	E3	C1	A	CC deactivation
No deactivation after request	S1	E3	C1	Qm	CC deactivation
Bad level activation (high instead of low)	S1	E3	C1	Qm	CC deactivation
Bad level activation (low instead of high)	S2	E3	C2	A	CC deactivation

2.4. Architecture Design

The results of risk analysis highlight that for some systems, such as transmission, hitch, engine control, HDL and PTO the requested AgPL is equal to C. The safety critical functions have been divided into:

- *Fail-operational functionalities:* the engine control must ensure an operational state even in case of fault. The speed demand to the engine must be less or equal to the speed set point requested by the operator as well as for the torque that depends on the load connected to the PTO.
- *Fail-silent functionalities:* The analysis that have been carried out highlights that, when de-energized, the electro-mechanical and hydraulics systems configure the system in a safe-state thus, the PTO, the Hitch Control and the Cruise Control were designed to be fail-silent. In case of fault these systems are de-activated until the proper recovery procedure removes the fault conditions.

Considering the figure 1.10, an AgPL = C can be reached with different combinations of architectural requirements. For the first:

- HW category 1;
- MTTF medium;
- DC medium;
- SRL 2.

The second alternative comprises:

- HW category 2;
- MTTF medium;
- DC medium;
- SRL 1.

While the last:

- HW category 3;
- MTTF low;
- DC medium;
- SRL 1.

As discussed in paragraph 2.2, the implementation of safety requirements demanded by an SRL=2 have a tremendous impact on the software development and validation. Moreover, all the software implemented on the systems must be developed at the SRL of the most critical function if it is not possible to ensure the complete partitioning of the software.

Therefore, the proposed architecture implements robust hardware solutions to lower the software requirements. By doing this, it can be achieved the optimal trade-off between architecture scalability and development/validation efforts.

In literature there are different approaches concerning the functional safety most of them related to automotive systems. In [37] a comprehensive analysis of fault-tolerant system is reported, with a strong focus on the X-by-wire system for automotive systems. In [38] is proposed a novel architecture based on a hardware/software co-design, where the adoption of software layers and hardware redundancy provides a fail-operational architecture. The [39] and [40] contain a review on fault-tolerant architectures for automotive system. In those paper the authors highlights that, although the dual-core architectures seem to be a good solutions for safety-critical systems, some limitations have to be taken into account: first, the peripherals are not redundant but shared between the cores, thus it is not possible to replicate completely the channel path. Secondly, the cores are integrated on the same silicon and built by the same manufacturer, this is not optimal to prevent the CCF. Considering the principles discussed in chapter 1, such as diversity and redundancy, multi-core systems might not be sufficient to achieve and adequate PL/AgPL for the most demanding safety-functions.

The next paragraphs will explain the different solutions that have been implemented, focusing on how they can cope with the specific safety requirements or arranged to provide the required scalability.

2.4.1. Dual Microcontroller

The architecture is based on a heterogeneous dual microcontroller design from, connected through a SPI interface. The two microcontrollers are defined as:

- Main microcontroller (MMC): it implements all the logics related to safe channels and to the standard channels.
- Safety microcontroller (SMC): it is used as supervisor and for redundancy. It is in charge to monitor the status of the main microcontroller and of the channels diagnosis. Depending on the AgPL required, it can act as an intelligent watchdog which monitors the execution status of the main system, or as a redundant safety channel.

Some points have to be considered while defining the architecture implementation since there is always a possibility that two identical microcontroller will both suffer the same common defect or that both present a systematic error in the software. Therefore, it is important for reduce the CCF incidence to ensure the diversity principles for these key aspects:

- uC manufacturers;
- hardware family;
- Compilers and toolchains;
- Embedded software implementations, i.e. real-time operating systems or bare-metal programming.

The SMC is the master of the communication through the SPI channel, even that it is used as TE or as secondary logical path a. In either cases, the SMC performs some check on the operational status of MMC, triggering the inputs acquisition and monitoring the outputs status. Since the compelling requirements on reaction time in case of fault, the SPI has been chosen to provide high throughput and synchronicity.

2.4.2. Inputs

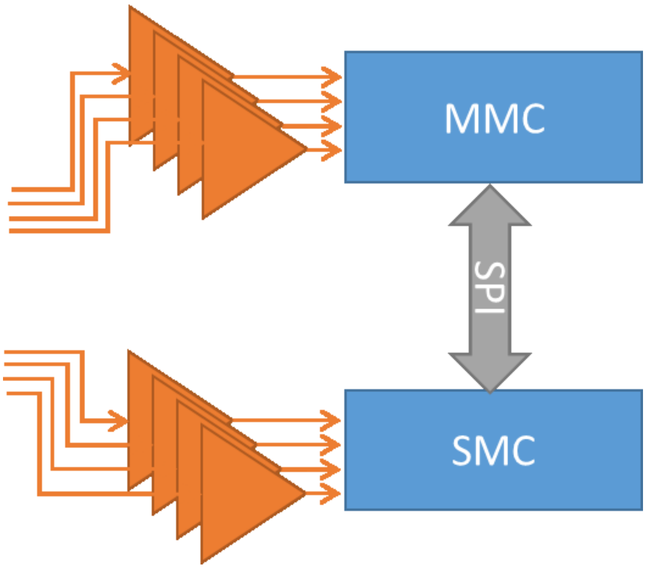


FIGURE 2.2: REDOUNDED INPUTS

The channel inputs are redounded as in the HW cat. 4 (figure 2.2), therefore they are acquired independently by MMC and SMC. In this way, the acquisition of the inputs can be synchronized, the SMC can trigger the inputs acquisition on the MMC, thus performing a simultaneous sampling on both microcontroller. Moreover it is possible to cross-check of the values acquired by inputs.

2.4.3. Outputs

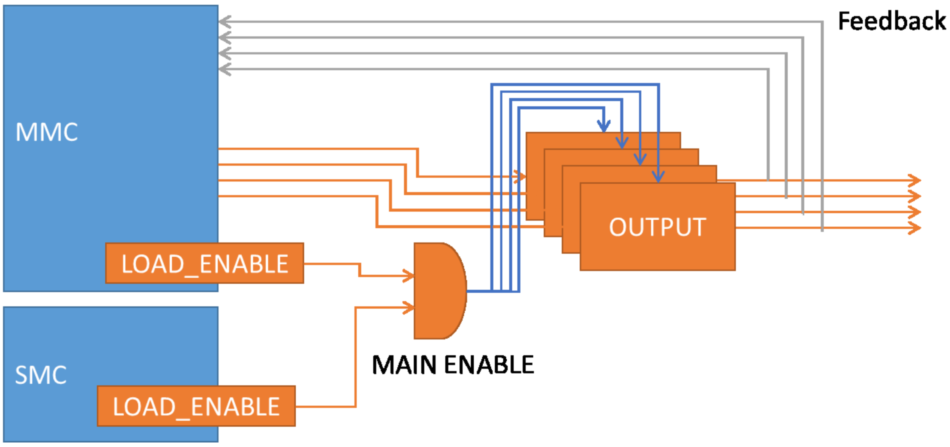


FIGURE 2.3: OUTPUT STAGE

The outputs of safety-related channel are provided with a feedback signal to ensure the correct command execution, as shown in figure 2.3. Thus the diagnostic is improved, as required for HW cat. 4, the faults on output lines can be detected and deactivated to drive the system in a safe state.

The proposed architecture also provides a countermeasure in case that one of the microcontroller is in a fault condition or that it is not able to detect the fault within the required time deadline. The safety related outputs are enabled by double confirmation system, that implement a logical AND between the MMC and SMC. As further improvement, the load-enable signal from microcontrollers is provided as a PWM signal. This signal drives a charge-pump, in case of time drifting or stuck-at line, the charge-pump de-asserts its output, disabling the related actuators. (figure 2.4)

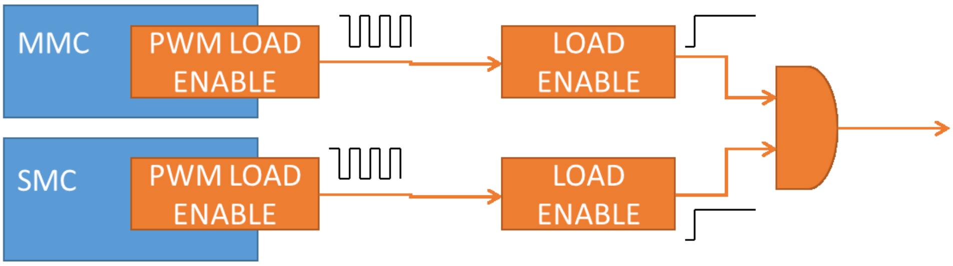


FIGURE 2.4: OUTPUT DOUBLE CONFIRMATION

2.4.4. Reset Management

Another important point to be addressed is the reset hierarchy of the system, the SMC can reset the MMC in case of malfunctioning, but the SMC itself is not a safe system and it can be affected by faults. The proposed architecture present a dual reset mechanism, in order to prevent unwanted reset due to the malfunctioning of the SMC. To avoid potential deadlock between the microcontrollers, the SMC can directly reset the MMC while the MMC can only perform a reset request to the SMC. The SMC is performed by an external watchdog on power supply.

2.4.5. Communication Protocol Between SMC and MMC

The communication protocol between SMC and MMC is a prominent feature of the proposed architecture. The hardware itself cannot provide the required AgPL without a supervision system that increase the channel controllability and the diagnostic coverage. Moreover, the implementation of a cross-checking protocols leads to a reduction of the safety level requirement of software.

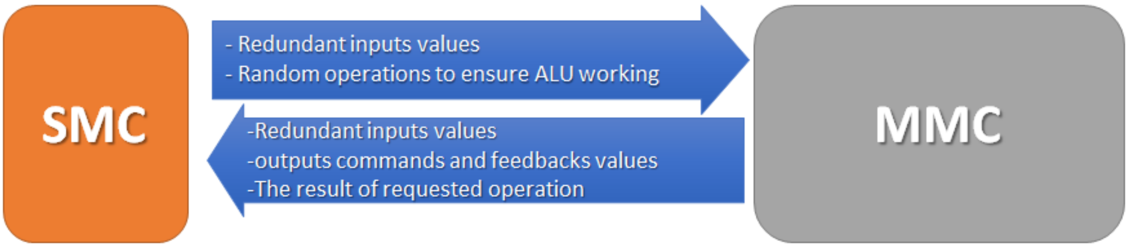

SMC
- Redundant inputs values
- Random operations to ensure ALU working
-Redundant inputs values
-outputs commands and feedbacks values
-The result of requested operation
MMC

FIGURE 2.5: PROTOCOL BETWEEN SMC AND MMC

The implemented protocol is based on the EGAS system introduced by BOSCH [41] for its engine control units and from the Infineon CIC61508 [42] safety watchdog, either widely used in automotive systems. The main features are:

- Execution timing control of MMC;
- ALU and peripherals checking;
- Inputs controls;
- Output feedback control;
- Test vector generation and comparison.

The monitor of MMC execution status is performed through a series of periodic questions generated by the SMC. The questions trigger a set of tests on the MMC and there are defined in a manner so that a comprehensive fault detection of MMC ALU, RAM/ROM and task execution time is possible. The received answers are verified against a static stable stored in SMC, it is also expected that MMC reply within a specified deadline.

The SMC also control the status of the safety-relevant input which are acquired by both microcontrollers. For the configurations which require a higher level of safety, the redounded inputs have to be selected in order to minimize the CCF, i.e. selecting sensors with different output characteristic or logic. In the same way, the feedback signals from the safety-related outputs are monitored by SMC to prevent unwanted activation.

2.4.6. Fault Management

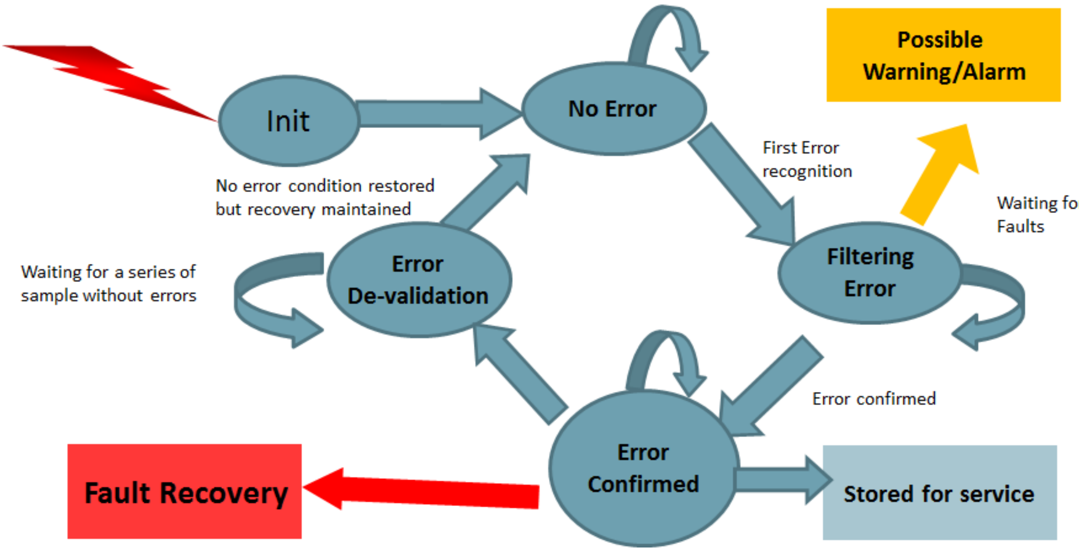


FIGURE 2.6: FAULT DIAGNOSIS FSM

The SMC must deals with sporadic malfunctioning as well as severe faults, so it is important to evaluate with each error condition in order to avoid an unwanted and sudden system block. Therefore on the SMC it has been implemented a diagnosis and recovery finite state machine (FSM) as in figure 2.6. Each error detected by the SMC and consequently by the FSM should be evaluated separately, for instance a redounded inputs may have several fault typologies:

- Sensor underflow, the output signal is under the minimum threshold;
- Sensor overflow, the output signal is above the maximum threshold;
- Incoherent read, the outputs from a redounded sensor are different.

The FSM provides three different diagnosis lines, each one handled differently and that lead to the safe-state in a different manner. The FSM implemented was designed to be highly configurable, as general as possible and it was divided into five states:

- *Init,* in this case the FSM reset all the internal structures, it performs some check on the inputs and outputs, the calibration of new sensors if needed and synchronization with the MMC.
- *Steady-State,* if no errors are detected the FSM continues to perform the standard diagnostic cycle of the inputs, outputs and MMC status.
- *Fault Recognition,* if at least an error is detected.
- *Fault Confirmed,* the FSM enter in this state upon an error confirmation and, depending on the configuration, the system could be driven to the safe-state or incremented the error counter.
- *Fault De-Confirmation,* the error was de-asserted and the error counter are decremented before returning to the steady-state.

The fault recognition is carried out through a statistical function which value is incremented by each confirmed fault and decremented by the opposite. The statistical limit is based on the minimum fault reaction time as well as the limit for fault confirmation and de-confirmation which counter are usually incremented or decremented with different speeds. All fault recovery procedures are maintained even if the fault disappear and stored in the internal memory for statistical purposes, they are only removed by the de-confirmation of the fault conditions and after a system power-cycle.

2.5. Architecture Implementation

A machine controller for agricultural machines has been developed using the aforementioned architectural principles. It manages several safety critical functionalities such as engine and transmission control, the differential lock and 4-wheel motion, in addition to the management of the PTO and auxiliary valves. The machine architecture is depicted in figure 2.7.

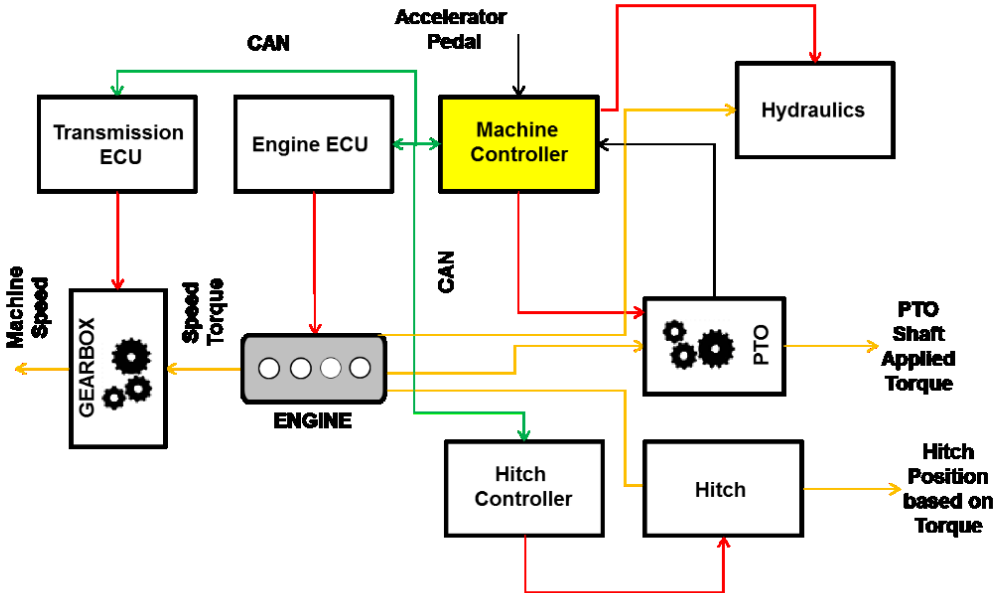


FIGURE 2.7: SYSTEM VIEW

For the MMC it has been used an ARM Cortex M3 and a Microchip dsPIC for the SMC. The two microcontrollers follow the principle of diversity, they are from different manufacturers, the MMC is 32-bit architecture while the SMC is 16-bit, and thus the firmware was generated from different compilers. The SMC detects the accelerator pedal and the hand accelerator, with direct sensors acquisition in parallel with the MMC and it performs an active check of the MMC. Also the CAN interface is redounded, the CAN SAE J1939 bus is monitored by the SMC to detect anomalous response to commands or to substitute the MMC for critical functionalities, such as accelerator set-point.

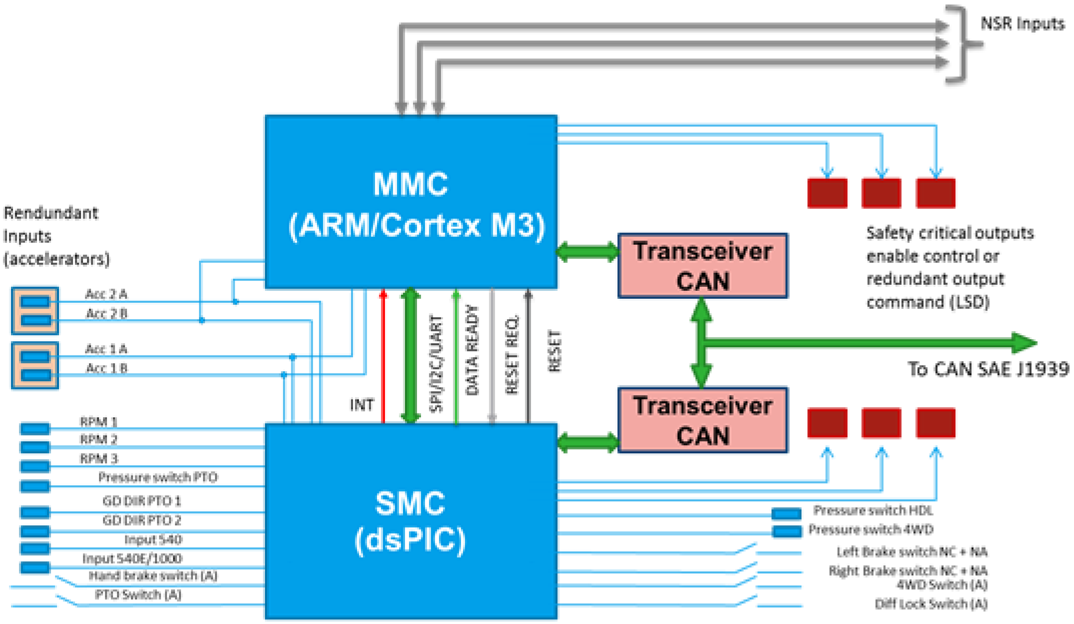


FIGURE 2.8: MACHINE CONTROLLER

For what concerns inputs from sensors or commands, they were chosen in order to be easily diagnosable. For each diagnosable input scheme has been used as shown in figure. 2.8, where the output signal was converted into an analog signal. The available range for signals is smaller than the electrical range read by the microcontrollers, it depends on the selected polarization resistors, and thus short/open-circuits are detected because the readings are outside the valid threshold.

In addition to this, the accelerator pedal is acquired by two sensors, with different output characteristics. The pedal position is obtained crossing the outputs of both sensors and this ensure a protection against the degradation of the ground of the vehicle chassis. The effects of a series resistance are immediately recognized because the two values acquired from the sensors recall to different position for the acceleration pedal thus highlighting the fault, as explained in figure 2.9. Moreover, mechanical limits were defined, as shown in figure. 2.10. The accelerator position obtained from sensors is compared with the mechanical limits defined during the end-of-line calibrations, thus idle and maximum position outside of the defined range are mechanically diagnosable even if they are inside of the electric available range for the sensors.

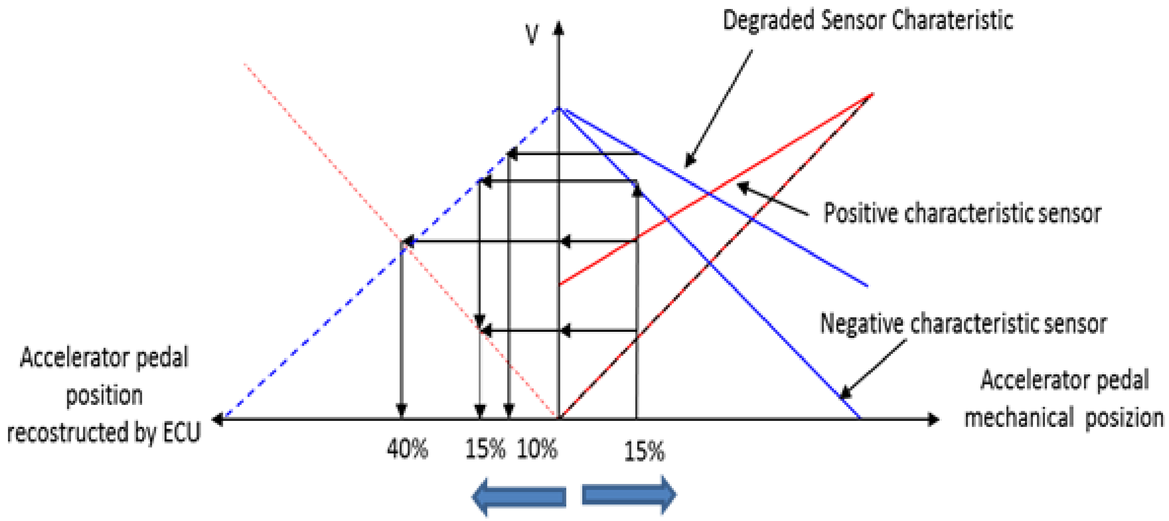

V
Degraded Sensor Charateristic
Positive characteristic sensor
Negative characteristic sensor
Accelerator pedal position recostructed by ECU
Accelerator pedal mechanical posizion
40%
15%
10%
15%

FIGURE 2.9:REDUNDANT SENSORS FOR ACCELERATOR PEDAL

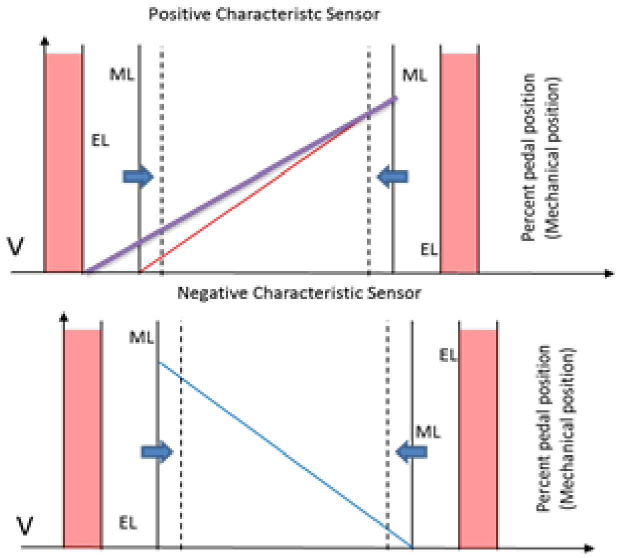

Positive Characteristc Sensor
ML
EL
ML
EL
V
Percent pedal position (Mechanical position)
Negative Characteristic Sensor
ML
EL
EL
ML
V
Percent pedal position (Mechanical position)

FIGURE 2.10: ACCELERATOR SENSORS MECHANICAL AND ELECTRICAL THRESHOLDS

Another important point regards the safety-related outputs that are provided with a feedback mechanism to monitor the command response from hydraulic parts. The outputs are enabled by a logic combinations of two commands, one from the MMC and one from the SMC, as explained in paragraph 2.4.3. To improve the DC and the overall MTTF of the output channels, it has been used "well-tried" components, available from different manufacturers, i.e. [43]. Those devices provide several diagnostic and fault protection capabilities, such as short-circuit protection, over-temperature protection, output state detection and current control, thus they can discover a fault that is incoherent with the command received.

2.6. Conclusion:

The architecture presented in this chapter has been specifically designed to cope with the problematics of functional safety design for agricultural machines. The concepts of Hardware category, DC and MTTF have been pursued so that the AgPL requested can be achieved with a lower SRL, implying lesser costs for the manufacturer and a faster development time. The architecture has implemented in a test application, realizing an advanced machine controller. This design has been recognized by FEDERUNACOMA and proposed to its associate as a reference design for development of safety-relevant electronic controller.

It also deal with the issue of designing a reusable architecture that can be adapted to many different applications. In fact, the recognized solution is not only compliant with the ISO25119 but also for the heavy-duty specific regulations, such as ISO13849 and ISO15998, which approaches to the functional safety is very similar.

Depending on the application, the SMC be used as a simple watchdog or as a fully redundant microcontroller. On the basis of the AgPL required by the safety channels, it can be up or down-scaled to meet the specific system safety requirements. For this reason it represent a practical and convenient approach for small and medium production series, where the implementation costs of functional safety requirements are be divided by a low number of pieces.

3. Rear Wheels Electro-Hydraulic Steering Control System with Reduced Performance Level Required

The new X-by-Wire systems under study for commercial and heavy-duty vehicles, as well as for agricultural machines, are increasingly real autonomous systems, capable to autonomously control vehicle functionalities, actuating the operator's commands. For instance, in the field of precision agriculture, the human intervention has been almost totally overtaken by machine automation ([44], [45], [46], [47]), in order to improve the efficiency.

Many mechanical systems have been replaced by electronic systems or X-by-wire systems, with important implications from the functional safety point of view. As electronic systems are less reliable than mechanical components, fault-tolerant electronic system are required

Fault-tolerant electronic systems are required to meet the high safety requirements, since of the lower reliability and different fault behavior of electronic and electrical components compared to mechanical components. This is especially true for some systems, such as steer-by-wire or brake-by-wire systems, that must provide a fail operational condition even in faulty circumstances.

In this chapter will be presented the technology transfer activities held at IMAMOTER institute for the "Maschio-Gaspardo" company. The activity involved the functional safety analysis of the steer-by-wire systems and the realization of new design in compliance with the ISO25119. The methodology applied for the safety analysis of a drive by wire steering system will be explained.

In addition to this will be described the realized solution that allows reduction of the AgPL required through the modification of the electro-hydraulic machine architecture.

3.1. Machine Description

The "Unigreen-Talpa" machine, shown in figure 3.1, is an innovative self-propelled digestate injector, provided with a complete drive-by-wire system.

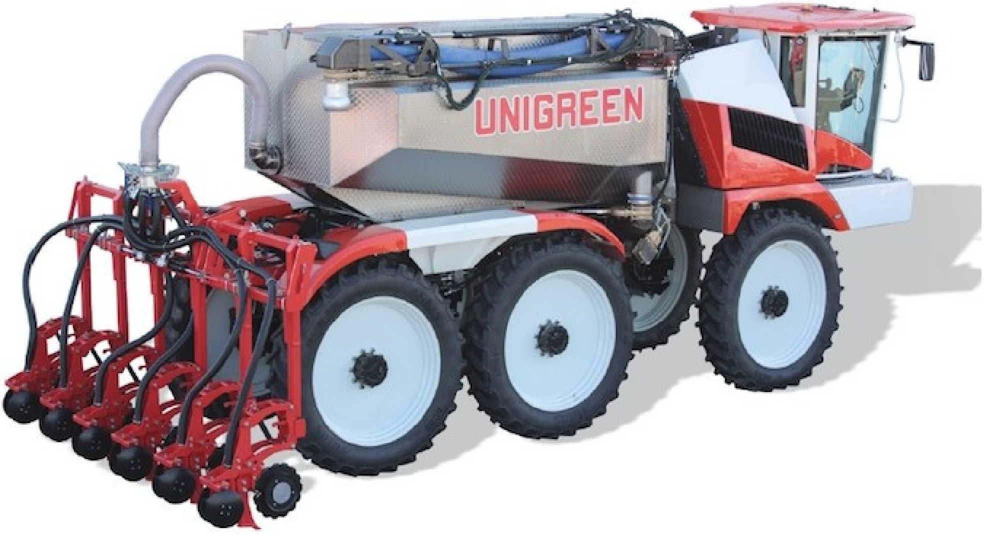


FIGURE 3.1: THE TALPA MACHINE

In order to improve the steering dynamics, the machine is provided with three couples of wheels: one frontal couple and two rear couples. The 6 wheels are all independent and controlled by a steer-by-wire system.

The accelerator pedal and machine speed management, as well as cruise control and machine layout (wheel base and machine height) are managed by the electronic machine controller. The machine can be configured in different modalities, which modify the maximum speed, limited by road regulation at 40 km/h, and the powertrain management.

The available modalities are:

- travel mode, for road travel with maximum speed 40 km/h;
- full power, working modality with engine rpm 1700 – 2200, maximum speed 22 km/h;
- eco mode, working modality with engine rpm 1450 – 1800, maximum speed 22 km/h;
- parking mode, for charge and discharge operations.

In addition to this, the electronic machine control can also dynamically modify the number of tracking wheels and the steering angle on the basis of the selected modality.

3.2. Functional Safety Analysis

From the functional safety point of view, in important to evaluate the risk and the failure modes of the system in relation to the working scenario.

The machine mission is to distribute in the field at high pressure the material resulting from the “digestion” of the biogas plants. These plants generate energy from the bio-transformation of gases of materials and sewage coming from fields and livestock. The typically machine usage is in the field or in the yards, for loading and unloading operations. Part of the life of the machine is also spent travelling on public roads to move from a field to another, typically in the same region. The average load factor of the machine is 1400 hours/year and the typical task breakdown is shown in table 3.1.

TABLE 3.1: MACHINE MISSION IN HOUR/YEAR

Operation	Hour/year	% of total time
Work in field	800	57,2
Charging in the yard	150	9,3
Discharging in the yard	50	3,6
Travel in public roads	300	21,4
Operations in the farm	100	7,1

The analysis of the mission profile highlight a high percentage of machine usage on public road. This leads to some issues concerning the functional safety of the system. The higher speed in road-travel modality and the potential presence of other road users have a tremendous impact on the risk of injuries for the operator and for the other people. Consequently, the design of some systems have to be performed with higher safety requirements than a machine which typical usage is on the field.

As previously discussed, the machine key functionality relies in the highly dynamic steering system that allows small steering radius even at slow speed.

3.3. Steering System Analysis

From the functional safety point of view, the steer-by-wire system implemented in the machine is the most safety critical functionality. Due to the machine length of 11.1 meter, to provide an adequate turning radius and improve the drivability in public roads, the front axle and the rear wheels were designed as shown in figure 3.2. The steering angles of the rear wheels are kept independent from each other and are changed, as a function of machine articulated front angle, with respect to the desired trajectory. The minimum steering radius of the machine is 4.5 m.

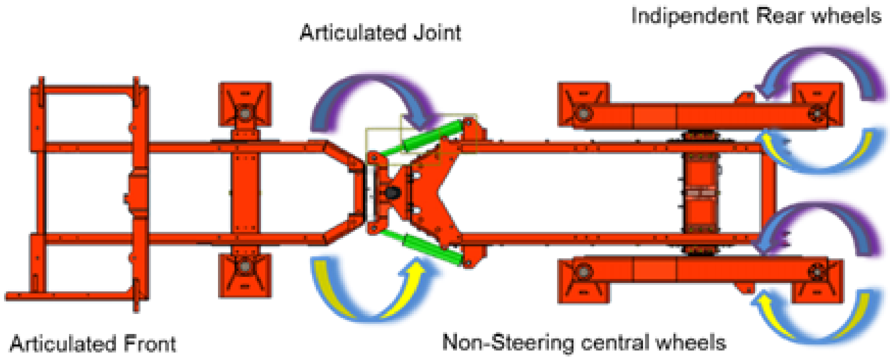


FIGURE 3.2: MACHINE CHASSIS AND STEERING MECHANICAL STRUCTURE

In the original design proposed by the Company, shown in figure 3.3, a proportional directional valve is fully responsible for steering in function of the front axle steering angle, as a follower of the front steer. A central valve in series configuration enables the steering of rear wheels. The steering angle of the front wheels as well as the articulated joint angle are acquired by the three sensors.

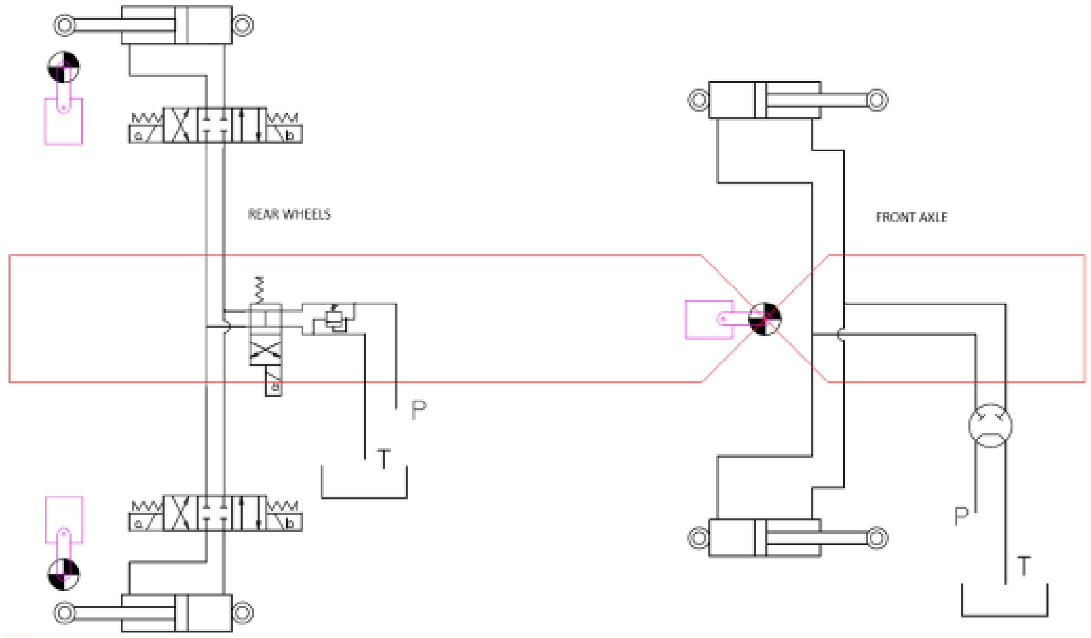


FIGURE 3.3: FIRST IMPLEMENTATION OF STEERING SYSTEM

This kind of actuation system is very simple and effective in control especially in big and relatively slow machines, where the maximum speed allowed is 40 km/h. In the architecture of figure 3.3, the power steering system is directly connected to the steering cylinders of the front axle. This solution implements a fault-tolerant channel, in case of failure of the steer-by-wire system, the steering functionalities is completely performed by the hydraulic system.

On the contrary, the rear axle steering system does not have this capability. The rear steering angle has to be a percent of the front steering angle and it changes as a function of the machine driving mode. To achieve the performance demanded by the manufacturer, the machine must implement an electronic control of rear wheels that provides a dynamic steering control. With a full hydraulic solution, even a small leakage in the circuit can lead to a difference in wheel direction, both with respect to front axle and to each rear wheel and therefore a performance degradation.

The initial idea was to implement a fully hydraulic solution for the rear steering, in order to follow the prescriptions of ISO13849, and avoid the more demanding compliance of ISO25119. However, for the reasons above, a fully hydraulic solution was not applicable.

TABLE 3.2: HAZARD ANALYSIS

Hazard Description	Condition	Severity	Exposure	Controllability	AgPL
Uncontrolled/ undesired steer	Road user injury	S3	E3	C3	D
Uncontrolled/ undesired steer	Confined Area bystander Injury	S3	E3	C2	C
Uncontrolled/ undesired steer	Field driver injury	S3	E4	C2	D

In table 3.2 are shown the classification of the steering system failure for each usage scenario. The AgPL requested for this solution depends on the *Severity*. Its value is high, because losing the machine control in public road may potentially cause severe injuries or fatalities. The *Exposure* shall be evaluated as "high" because the steering function is always active except in a small fraction of time when the machine is performing the load and unload operations. Finally the *Controllability* is very low, because the proportional three way valve is the only actuator for the rear wheels steering and its malfunction cannot be corrected. The global evaluation for the AgPL according to this analysis is equal to D.

Therefore, to implement the solution proposed by the Company, the control system has to be design as a redundant hardware category 3 with an SRL = 2. As discussed in chapter 2, the design of complex system with high SRL is not affordable for many heavy duty and agricultural machines manufacturers.

On the basis of these results, it has been chosen to redesign the steering system, modifying its dynamics, in order to lower the safety requirements without reducing the machine performance.

Consequently, it has been analyzed the parameters that contribute to determination of the AgPL. The *Severity* cannot be changed, because it is related to the nature of the hazard in respect to machine function. On the contrary, both *Exposure* and *Controllability* can be modified by design. The *Exposure* is a sensitive parameter, because it depends on the electro-hydraulic system structure and it has large variability that affects the AgPL calculation. In the same way, the easiness of controlling a hazard, can be very different in function of the channel DC and thus to the observability of the system. The *Controllability* is also related to the authority and to the dynamic of the actuator, both in terms of amplitude and of actuation power. If, at the fault occurrence, the electronic control systems would be able to recognize the fault, even if they could not isolate it, they will be able to modify the whole machine mode in order to reduce the hazard effect. This would help the operator in controlling a faulty machine. On the other hand, if the dynamics of the fault consequences on the machine steering are slow, the operator would have enough time to lead the machine in a safe condition.

These considerations have been exploited for the development of a new steering architecture.

3.4. The Electro-Hydraulic Steering System

As briefly described in the previous paragraph, the initial solution may lead to an incorrect steering angle. Analyzing in detail the system proposed in Figure 3.3, once the rear wheels steering is enabled, all the steering operations are managed through a single valve electronically controlled for each wheel, and a single fault of one of these two valves may lead to a wrong steering angle and then to a critical hazard. Therefore a single fault causes the loss of a safety function and nothing can be done to change the steering angle of the faulty wheel. The two sensors on wheels are functional to the main steering functionality, because they will observe the actual steering angle to be related to the steer angle of the articulated front of the machine. For the entire period of time when the rear steering is enabled, the operator, bystanders, or other road users, are exposed to a possible hazard, because the function can result in a fault.

Therefore the system should be designed in order to avoid this occurrence. Concerning the DC, the usage of two sensors, if properly chosen, can improve the diagnostic information and can be connected to strategies related to the machine mode and speed, in order to reduce machine velocity in case of fault.

3.4.1. First Implementation

The key idea of the proposed solution is to change the steering architecture in order to implement a “rear electro-hydraulic steering correction system”, with a very limited dynamic and authority. By doing this, the required AgPL is significantly reduced, since the limited working hours of the system, considering the machine task and mission.

The proposed architecture, shown in figure 3.4, implements a copy and a slave cylinders for rear wheels steering. In the hydraulic circuit, two pulled cylinders are added in parallel with the front axle steering actuation system; these two cylinders directly control the oil in the actuation cylinders of the rear wheels. This architecture can be affected by wheel misalignments, so a couple of load dump valves are added (one for each wheel), in order to correct a wrong wheel angle only dropping a small oil flow, and only if an electro-hydraulic on/off enable valve is powered.

In the proposed solution, the control valve is activated only when the hydraulic system controlling the rear wheel steering is affected by a steering angle error, in respect to the front axle of one or both rear wheels and only in the direction of increasing the steering angle. If no errors are detected by the angle sensors the drop valve and the enable valve are not activated.

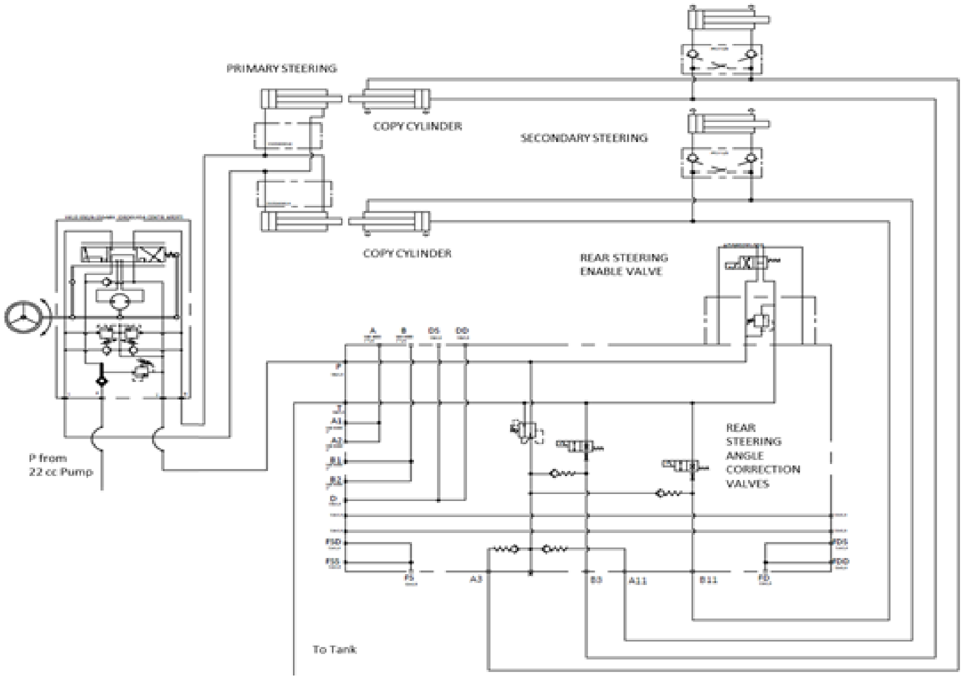


FIGURE 3.4: CONCEPT OF THE ELECTRO-HYDRAULIC SOLUTION

The functional safety of the electro-hydraulic component shall be performed considering a reduced exposure, because most of the steering actions will be performed by the hydraulic components without any electronically controlled steering correction. This can be stated only if an uncontrolled activation of the function is ensured by a very robust control system.

The controllability is much higher with respect to the fully electronic solution, because of the reduced oil flow of the dropping on/off valve that only serves steering angle correction and not steering angle actuation. Moreover a fault in a single valve does not affect the steering angle, if the enable valve is de-energized. It can be said that the design is safe state oriented. Moreover the system is much easier to design because it is possible to define a safe state: the function of “steer angle correction” can be stopped if faulty, because the steering function is actuated by the hydraulic system. Finally, the DC of this solution is at least equivalent with the previous one.

In order to avoid cavitation and to maintain the control pressure in all the cylinder sides, a feeding valve is added, to avoid that the oil flow dropped from the control valves lead to low oil pressure conditions.

3.4.2. Second Implementation

The correction capability asymmetry of the proposed solution was determined to be insufficient, because the correction of the steering angle could be required in both directions. Therefore it has been designed a new architecture, symmetric in angle correction capability, with independent control for both sides of the actuation cylinder, and maintains the two valves in series topology, for a safer enable of the angle error correction control (shown in figure 3.5).

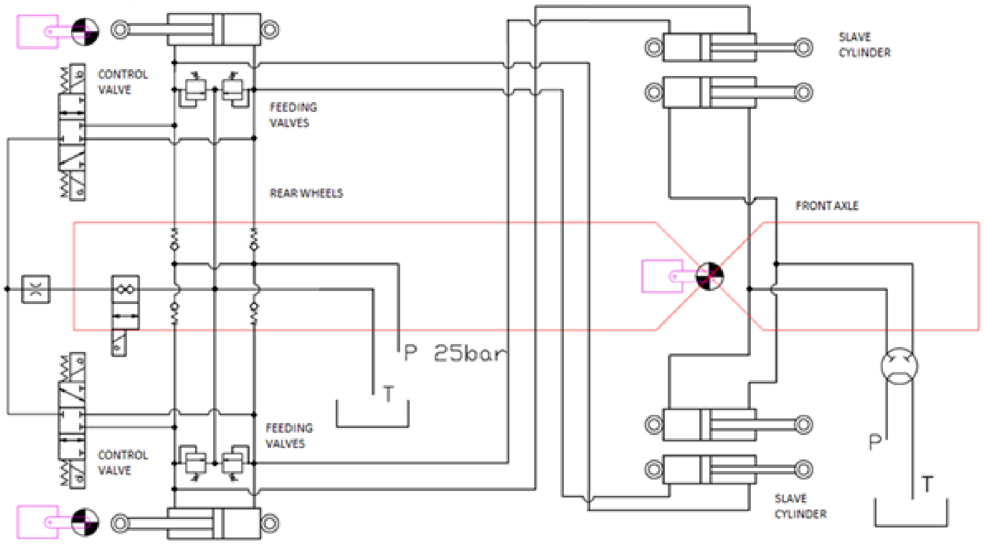


FIGURE 3.5: FINAL IMPLEMENTATION

Concerning the slave cylinders structure, the oil drop actuation system has been totally changed, using a three way valve for each wheel, in order to discharge the oil flow to reservoir every time a correction in the steering angle of a rear wheel is needed. The enable valve is in series to the drop valve, so a fault with an unintended activation of one of the control valves results in a no-hazard condition because of the enable valve presence, under the hypothesis of a single fault.

Exactly as in the previous system, the steering actuation is performed by the hydraulic system and, in absence of errors, the electronic system is idle. The electronic correction system is activated only if the rear wheels steering angles are affected by an error. This modifies the safety function requirements, since the functional safety analysis is performed not on a rear steering function but on a rear steering error correction function.

This function will be active in the life of the machine considerably shorter with respect to the rear steering, that is fully hydraulic. From the functional safety point of view, the resulting exposure is dramatically reduced and the AgPL is consequently lower.

The AgPL can be reduced also because of the slow correction action performed by the electronic control system controlling the drop valve. The small flow resulting in a wrong actuation due to a fault, can be easily corrected by the operator controlling the steering wheel and reducing the machine speed, and the operator can also be alerted by signaling devices like buzzers, lights and a message on the machine display, once the fault is recognized by electronic systems.

Considering the exposure to be less than 1% of the total machine time per year and the controllability as "easy controllable", the resulting AgPL = C, reachable with a lower hardware category and a lower SRL as the machine controller presented in chapter 2.

3.5. The Machine Electronic Control System

The rear steering system is not the only machine function that has to be considered for the functional safety. The machine is a fully electronically controlled, the cruise control, the speed control with joystick and different machine modes, that modify many machine functions, and enable the work of the machine in the field, demand a complex machine electronic control.

The machine control is managed by a distributed control system, performed using seven ECU connected through two CAN networks. The main machine control ECU acquires all the main signals by sensors or through the CAN network and sets the machine mode, enabling the machine functions. The CAN networks are the main communication channel and are considered critical for safety and for machine function, as already stated in [47]. For all these reasons, the CAN network is redounded, in order to be able to safely move the machine in case of network fault. The machine is therefore equipped with a powertrain SAEJ1939 network, where transmission control and engine control exchange the main signals, and with a machine control network, where the inputs from operators and commands to steering, machine setup and rear implement functions are exchanged.

The MMCU is a Category 2, depicted in figure 3.6, ECU capable to reach the AgPL=C, that is required by other machine functions, while the SRL required level is 1, easy to be reached under a proper development lifecycle control. The unit was designed in accordance with basic safety principles already published in chapter 2.

The networked control is ensured, in the most important and safety related units, by a redundant CAN network. The Main Control Unit and its peripherals are designed to comply at least Diagnostic Coverage Level = Medium.

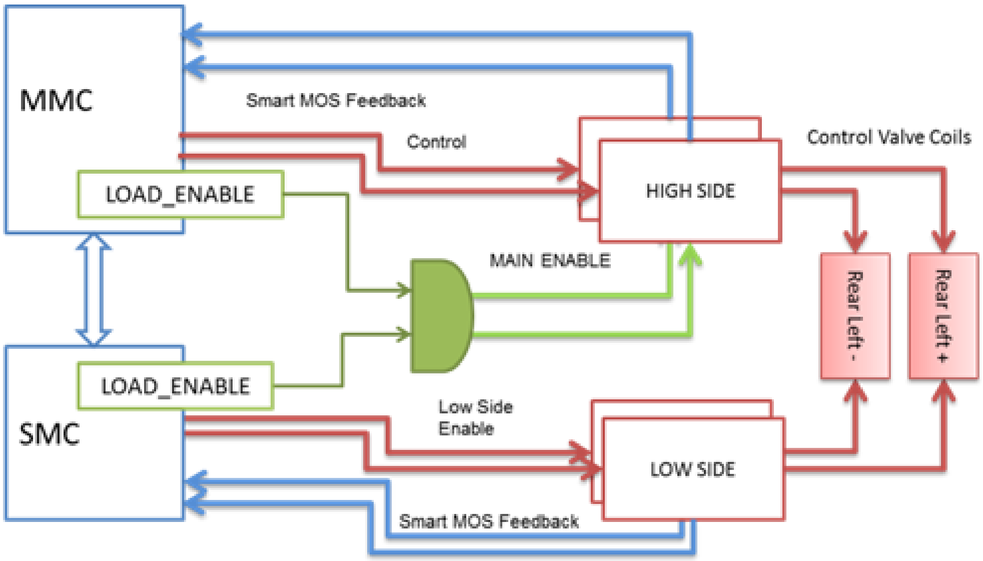


FIGURE 3.6: VALVE CONTROL ARCHITECTURE

In order to accurately acquire the steering angle, in front axle and rear wheels as well, three redundant double angle sensors are installed respectively in the articulated joint, in the machine front, and in each rear wheel. By doing this, the position of each part responsible for steering is acquired and diagnosed using redundant angle sensors.

From the actuation point of view, the steering correction of the rear wheels is enabled by a load dump central valve and by the single wheels oil dump control valves in series configuration (AND configuration). Only when both valves are enabled the steering correction can be performed. A single fault on a valve cannot affect the steering function.

All valves, even are if only ON/FF valves, are controlled through a double electronic power stage, composed by an high-side driver and a low-side driver in asymmetrical half bridge configuration, as shown in figure 3.6. Therefore a single short fault on electronic actuation stage, cannot unintentionally activate the valves, and the consistency of command action is ensured by the main enable command, that is activated by both microcontrollers in AND configuration.

The high-side is used for the valve control, while the low side driver is kept active and is de-energized only in case of fault. Both drivers provide a feedback to the microcontroller, in order to recognize the faults and activate fault recovery strategies. This architecture is replicated for each rear steering correction valves. From the work session and machine usage point of view, the electronic system acts on rear wheels not for steering, but only to correct angle errors in the rear wheels. In case of angle error the operator is warned by an audible alarm and a visual message on the machine display, but also he is requested to acknowledge the correction angle if the error is recognized in travel mode. In fact when the machine is travelling in public roads a special attention is paid to the steering angle. The operator must change the machine mode from travel to work. Subsequently, with a limited maximum speed, the electronic control system can start the steering angle correction. The operator is responsible to verify that the road conditions are suitable to activate steering correction. In order to regulate the amplitude of the angle correction, an intervention threshold in angle degree can be set.

3.6. Conclusions

The functional safety analysis of electro-hydraulic systems under the new regulations for agricultural machines ([21]) often results challenging because of the PL required compliance. The Severity of hazards related to heavy-duty machines lead to high levels of PL required, that need for complex electronics and an SRL very difficult to be reached by the most part of SME companies.

For a proper analysis of the system, the consciousness that hydraulic components can be classified as “well tried” and then reliable from the safety point of view can help the designers to find a compromise between function required and functional safety performance. In this chapter is presented a methodology to obtain an acceptable AgPL maintaining the full function required by the machine specifications. In this case a solution was found by modifying the machine function; from a fully electronically controlled steering system, to a hydraulic steering system with electronic correction; in order to reduce the impact of the fault from the functional safety point of view.

4. Electro-hydraulics Architecture Design for Safety-related Systems

The adoption of mechatronic systems, together with the new functional safety regulations in mobile machinery, are raising the need for new machine architectures and components oriented to safety and efficiency. New design ideas are especially needed where application requirements demand fail operational systems and a minimum functionality shall be ensured even in case of faulty system. One of the most promising ideas is to implement multiple hydraulic power sources that can be dynamically reconfigured to serve each actuators. The main drawback of this solution is the high number of switching valves required to implement the hydraulic circuit.

In this chapter will be presented a safety-oriented mechatronic component developed at IMAMOTER for the realization of new electro-hydraulic architectures for mobile machinery. The input for this research came from the displacement control systems developed at the MAHA research center of Purdue University [48] [26]. The contribution of this thesis relies in the design of an intrinsically safe mechatronic valve that realizes the pump switch management, creating a matrix framework of the hydraulic flow connections.

4.1. Background

In the field of mobile machines two architectures are the most commonly used: the open-center hydraulic system and the *load sensing* (LS) system [49]. From the efficiency point of view the open-center architecture is penalized due to its own working principle: the flow rate directed to actuators is obtained by subtracting the excess flow directly discharged to tank from the total flow generated by the pump.

LS systems [50] offer some energy and control advantages: the flow rate is adjusted to the actual request of consumers through proportional valves, so utilizing a variable displacement pump [26], only the requested flow rate is delivered. In this kind of circuits the delivery pressure is determined by the highest load while lower loads are controlled by throttling in local compensators, moreover all overrunning loads are controlled by meter out edges, not allowing the recovery of gravitational energy.

A proposal to work out these drawbacks using a single supply can be found in [51] and in [52]. The former basically proposes a compensated LS system with the addition of a supplementary line with the aim of regenerating energy in case of high load difference and overrunning loads, the latter basically optimizes the throttling control and allows additional features such as regeneration.

Realizing that the weak point of the LS system is to have a unique supply which has necessarily to be adapted to the highest load, various alternatives have come up taking advantage of splitting the hydraulic power source: Digital Pump [53] and Valve Systems [54], Two Level Constant Pressure System (“STEAM”) [55].

The idea to create the new component was inspired by [56] which has stimulated a large current of research. This architecture in the most basic version has a variable displacement pumping unit for each actuator. A major drawback of the original concept is the very high costs of plant in reason of the requirement of a high performance variable displacement pump for each actuator.

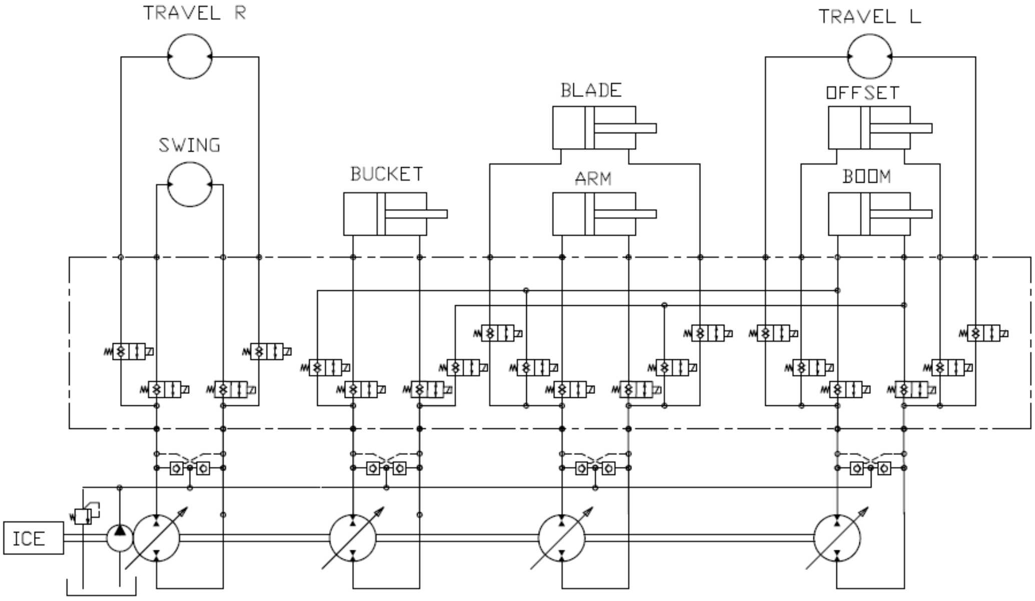


FIGURE 4.1: DISPLACEMENT CONTROL SYSTEM

In recent years a more advanced architecture [26] (depicted in figure 4.1) including a distributing manifold was presented, giving the opportunity to utilize a smaller set of pumps that can be switched between actuators and eventually summed.

The resulting manifold is a quite complex distributor system composed by 20 ON-OFF Valves. In this system the association between each pump and actuator is determined and unmovable: the layout is defined and dimensioned aiming at performing the digging operation. Since excavator is a multifunctional machine, an optimal layout for a particular work cycle isn’t necessarily the best for all conditions, for example with the proposed layout it is impossible to swing while the excavator is in travel mode.

A more flexible distribution could possibly open up to even more efficient operation and a further downsizing of pump units, anyhow the distributor complexity has to be justified by the sensible benefits.

The limit of this solution is that a new interconnection design should be made for each machine type and probably for different machine missions, especially in complex machines.

4.2. The Oil Flow Control Matrix working principle

The above mentioned limits drove the idea of a novel matrix architecture component that can overcome the constraint of having a specialized manifold for each machine type.

The new component design takes advantage of the roto-translating valve working principle [57], developed at IMAMOTER institute, where a proportionally actuated sleeve and a proportionally actuated spool generate a variable flow area in a safe proportional valve. The same concept has been exploited to design the component, changing the function of both actuators: the sleeve is now used as a selector, while the spool is used as an enabler for oil flow. The matrix architecture can be represented by a functional schematic where the component is represented using the conventional components (basically a network of 2/2 ON-OFF valves, just as for the displacement control of figure 4.1), in order to evaluate the number of valves required to implement the equivalent matrix. The rows are connected to the pump, and represent the power source, while the columns are connected to the actuators, and represent the loads. In figure 4.2 a single *pump switch matrix* (PSM) component is presented.

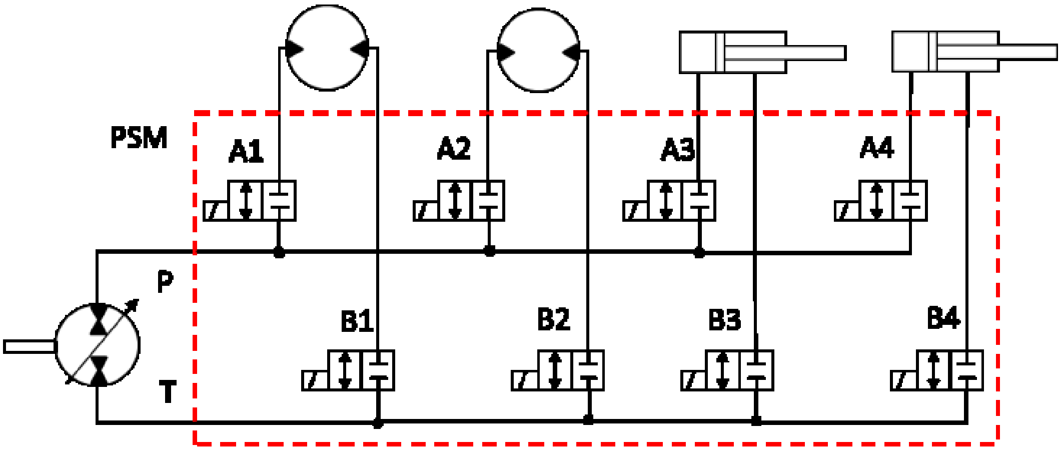


FIGURE 4.2: THE NEW PUMP SWITCH MATRIX (PSM) COMPONENT WORKING PRINCIPLE SCHEMATIC

The component is able to connect a single pump to four actuators. The MA and MB lines are connected to the actuators through the 2/2 ON/OFF valves denominated Ai and Bi, where *"i"* is the index of actuator. An important constraint of the system is that only a couple of valves (Ai, Bi) can be activated at a time. In conclusion a total of 8 valves are necessary to connect a pump to four actuators.

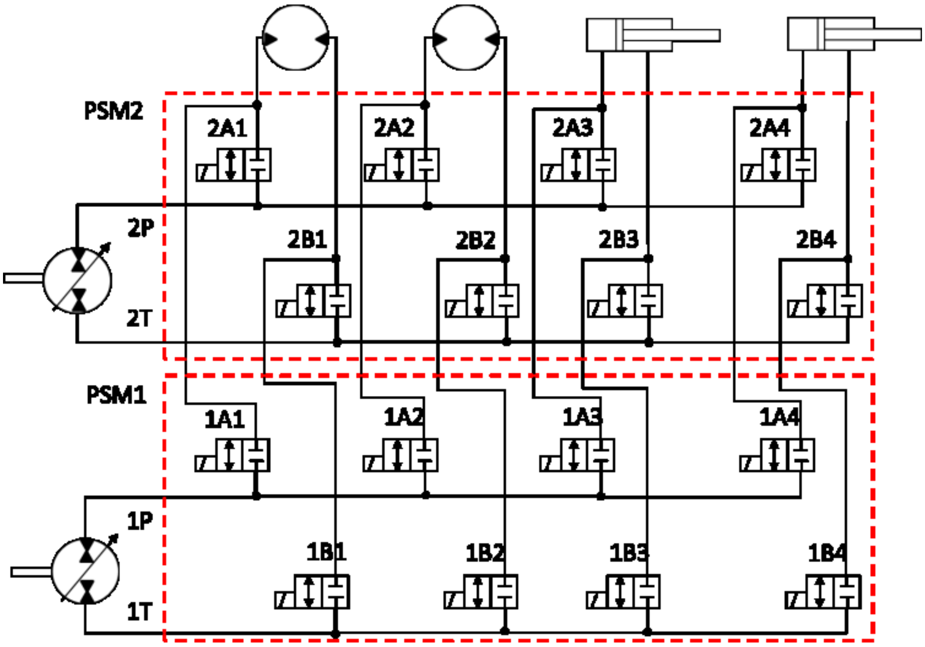


FIGURE 4.3: A 2 PUMPS AND FOUR ACTUATOR MATRIX REALIZED WITH THE DISPLACEMENT CONTROL WORKING PRINCIPLE

The solution presented in figure 4.3 helps to understand how to calculate the number of valve needed by a physical matrix, if this topology is expanded to a larger number of pumps.

With simple algebraic passages, a number of valve equal to the double of the number of pumps multiplied for the number of actuators is necessary to create a full matrix achieving the same range of possible connections. Referring the solution presented in figure 4.1, where four pumps and eight actuators are installed, coherently to the matrix principle, a manifold with 64 valves should be designed. The circuit schematic in figure 4.3 represents all possible connections between actuators and supplies.

Going more into detail to the matrix architecture presented, obviously not all connections can be achieved at the same time: in particular some basic principles have to be stated:

1. each source port can be connected to only one actuator at a time;

2. when a particular supply is connected to a specific actuator port, the corresponding return port will be connected to the opposite actuator port;
3. it is possible to achieve confluence with more sources connected to a single actuator
4. despite the conventional hydraulic proportional distributor systems, each hydraulic source port is not meant to feed multiple actuators at the same time.
5. the configurations are discrete, the matrix valve is of the directional type and it is not meant to be proportional neither to have metering functions

These rules have the effect of decreasing the number of allowable combinations. Since the presented architecture provides a large number of possible connections it is advantageous to adopt matrix representation and alphanumeric codes to represent the system topology. It is possible to represent the connection scheme with a connection matrix where the rows correspond to ports and the columns to actuators. Each entry of the digital matrix can have two value 1 or 0 according to ON/OFF state of associated connection. In reason of the architecture a single 1 value is possible in each row, on the contrary multiple 1 values on a single column indicates a flow summation in a single actuator.

TABLE 4.1: TABLE REPRESENTATION OF THE CONNECTION MATRIX

		Actuator1	Actuator2	Actuator3	Actuator4
Pump1	1MA	1A1	1A2	1A3	1A4
	1MB	1B1	1B2	1B3	1B4
Pump2	2MA	2A1	2A2	2A3	2A4
	2MB	2B1	2B2	2B3	2B4

Looking at connection matrix it is possible to build the equivalent ON-OFF valve scheme that in practice can be very complex and difficult to implement with a network of ON-OFF valves. Therefore the new component is proposed to overcome the drawbacks of cost, size, and complexity of a high number of ON-OFF valve manifold.

As a basic example, it is possible to connect the pump matrix valve with pumps in a closed circuit system obtaining a displacement controlled system (figure 5), without the constraint of having one pump per actuator, taking advantage of confluence to downsize the pumps and to avoid the manifold design for any application.

4.3. The Pump Switch Matrix Component

In the following section the construction of the valve will be detailed, starting from the description of the PSM architecture. In figure 4.4 a 3D sectional view of the valve is illustrated.

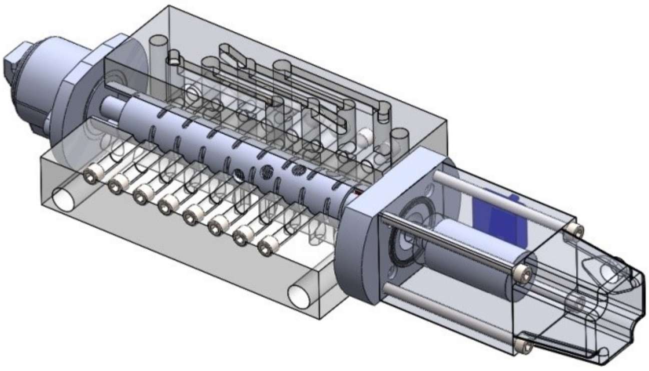


FIGURE 4.4: 3D MODEL OF PUMP SWITCH MATRIX VALVE

The valve is made up of six main elements, as shown in figure 4.5: the Rotation Spool (6), actuated by a Stepper Motor (1), the Translation Spool (5) placed inside the hollow rotation spool, moved by the Solenoid (10) and kept in neutral position by the Spring (9), the Housing (7) taking on the role of interface with the other elements of the circuit.

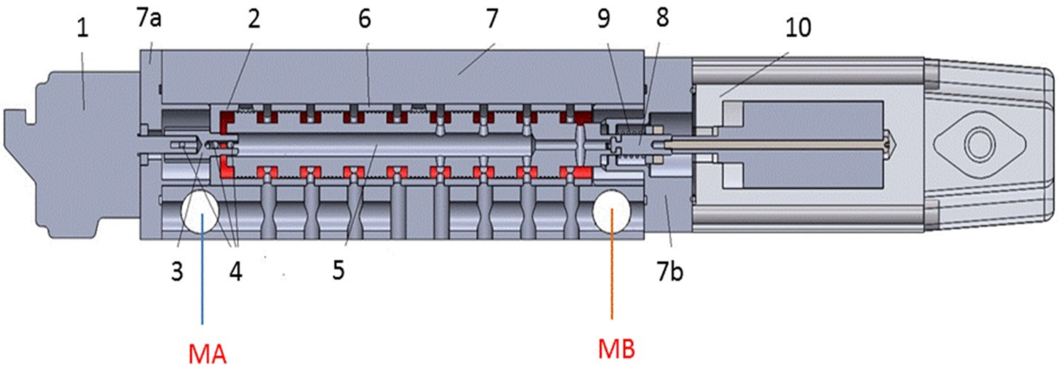


FIGURE 4.5: SECTIONAL VIEW OF PSM VALVE

In the rotation spool, a longitudinal bore containing the translation spool is provided, multiple supply and return slots are radially fitted to provide connection with MA and MB ports, the sequence of the actuator bores are radially drilled, spaced by a suitable phase lag so that they can align sequentially with each given actuator channel at a certain rotation angle.

The translation spool, shown in figure 4.6, has multiple control edges designed in order to alternately open or close the passage between supply slots and actuator bore (return slot and the opposite actuator port bore respectively). The internal axial bore has the function of depressurizing the dead volumes at the end of both spools connecting them to return to avoid static pressure unbalance.

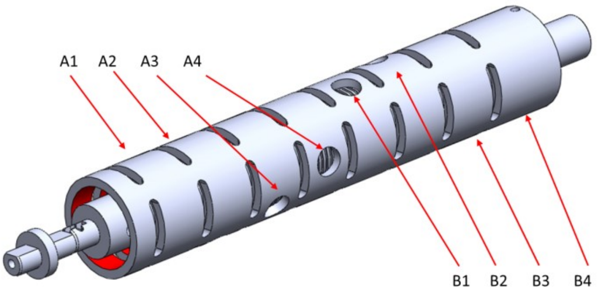


FIGURE 4.6: PSM ROTATION SPOOL DESIGN WITH CONNECTION TOPOLOGY

The translation spool is moved by means of the solenoid forced against a spring. To minimize rotary movement friction the rotation and translation spool rotate rigidly (through joint 3, figure 4.5), with the effect to be subjected only to the housing-rotary spool friction and not to the two spools mutual friction.

The primary function of the translation spool is to keep all connections closed during the switching between different actuators, preventing unwanted movements in the transitions between the operating positions. The secondary function is those of safety, offering the possibility of blocking the flow at any time.

The dynamic performance of the valve is an important issue that can be reasonably developed only after the prototype construction, since the dynamic behavior largely depends on factors related manufacturing process such as geometrical and dimensional tolerances, surface finish. Furthermore the translating spool opening/closing timing with respect to those of rotation spool have to be carefully considered in the elaboration of control strategy since it can have a sensible effect on the control of transients encountered during the switching operations.

In the architecture of the system presented the solenoid is an on/off type, but depending on the architecture, the supply type and control requirements, it could be also considered to use a high performance or even a proportional type solenoid.

The housing has the function to connect with outer components, this is attained through upper face ports, lower face ports and lateral face ports via actuator channels and via supply and tank channels. The supply and return ports are placed on lateral faces and are independent for each valve module. On the contrary the upper and lower faces had been designed to interface corresponding actuator port of various sections with each other when multiple valves are stacked together to form a control block.

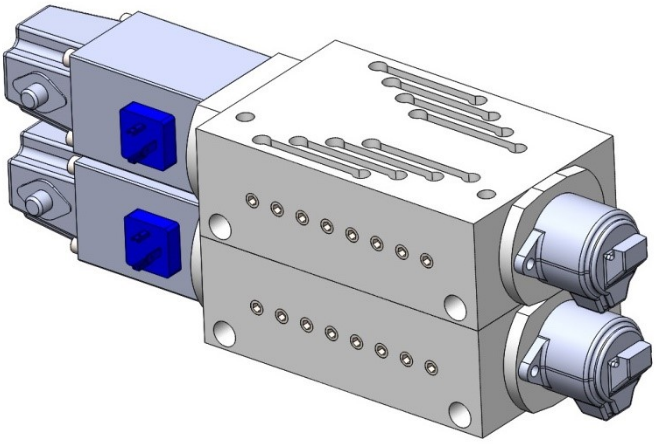


FIGURE 4.7: ASSEMBLY VIEW OF TWO PSM VALVES STACK

A connection plate is mounted on the last block of the stack to provide the appropriate connection to the actuators, while the pumps connection ports are obtained on lateral faces of each section.

4.4. PSM Stackability

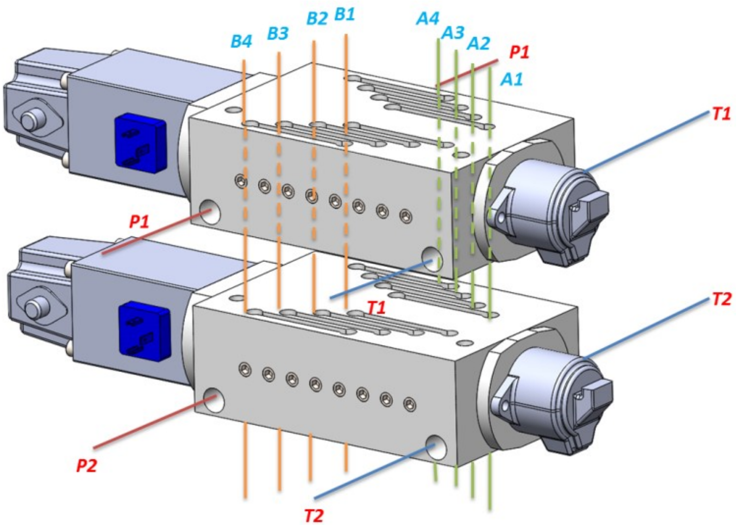


FIGURE 4.8: DISASSEMBLED STACK VIEW OF TWO PSM VALVES STACK

The PSM valve has been designed to be stackable, thus the upper face of each valve housing is conceived to interface with the lower face of following stack element so that the corresponding actuator ports of the two layers are linked together.

To sum up, supply and return ports of each valve are kept independent and can be connected to different hydraulic sources while all corresponding actuator channels are joined together, allowing optimal matching between supply and actuators; this topology provides the possibility of the confluence of Pumps with the maximum grade of flexibility.

Figure 4.7 presents a view of two PSM valves assembled in a stack that enables the matrix connection of two pumps with four actuators, the compactness of the solution is the most evident characteristic, while the topic of flexibility will be addressed later on.

The figure 4.8 evidences the internal connection of the two PSM valves, the internal parallel actuators channels cross all stacked sections, thus allowing the oil flow summation.

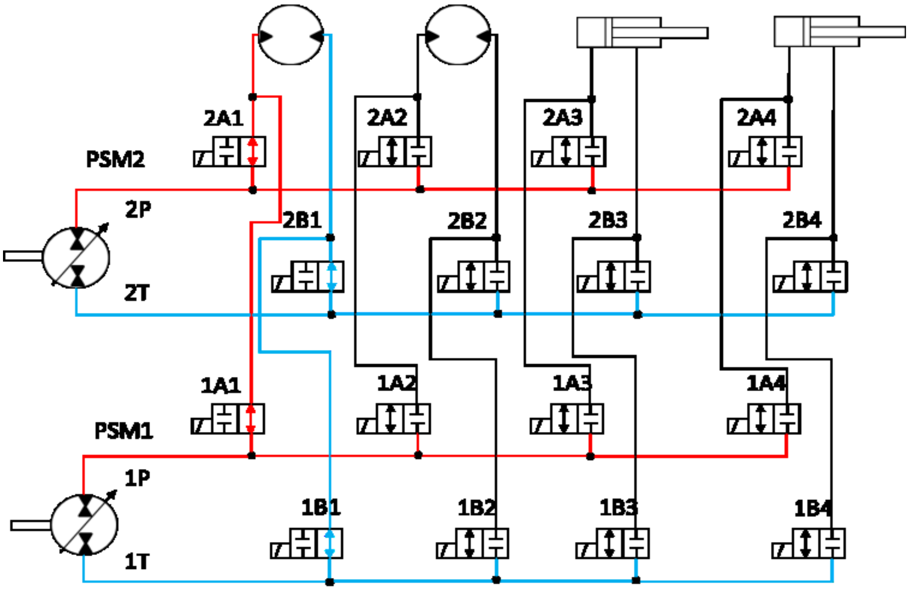


FIGURE 4.9: EXAMPLE OF OIL FLOW SUMMATION OF TWO PUMPS TO ONE ACTUATOR IN THE PSM STACK

The matrix carries out the independent connection of a pump to any actuator connected to the PSM element, allowing thus flow summation. The matrix flexibility can be as well appreciated looking at the resulting circuit topology shown in figure 12.

As a result the stackability of the component offers a wide range of possibilities bringing a high grade of flexibility; potentially it could be profitable in different types of multifunctional machines.

For a better comprehension of the architectural concept, a working principle schematic is reported in figure 4.9. The picture displays a 2 pumps and 4 actuators system, where both pumps are serving the same actuator 1, while all other actuators are disconnected and then blocked. Any other combination can be attained with the only constraint of not feeding more than an actuator with a single pump.

In figure 4.10 a more complex system is presented, in order to show a possible solution to allow pumps controlling more actuators. With a parallel of MA (1MA and 2MA, 3MA and 4MA) and MB (1MB and 2MB, 3MB and 4MB), one pump can be connected to more PSM elements (pump 1 to PSM1 and PSM2, pump 2 to PSM3 and PSM4), in order to be connected to a larger number of actuators. This topology get over the number of actuators connected to each PSM element limit. The solution can be easily expanded to four pumps, simply doubling the number of PSM and then crating a parallel of two stack, each one composed by four PSM connected in parallel and connected to four pumps; the solution will be equivalent of the one presented in figure 1, using 8 PSM components instead of 64 on off valves.

With 8 sections basically all possible combination of pump-actuator for excavator is possible, in a rational architecture where all hydrostatic units are connected one of the lateral faces and all actuators to upper connection plate. A manifold with comparable characteristics would provide 64 slots for the cartridge ON-OFF valves, however the last word on comparison of size and manufacturing cost would be said only after the prototyping of the PSM system.

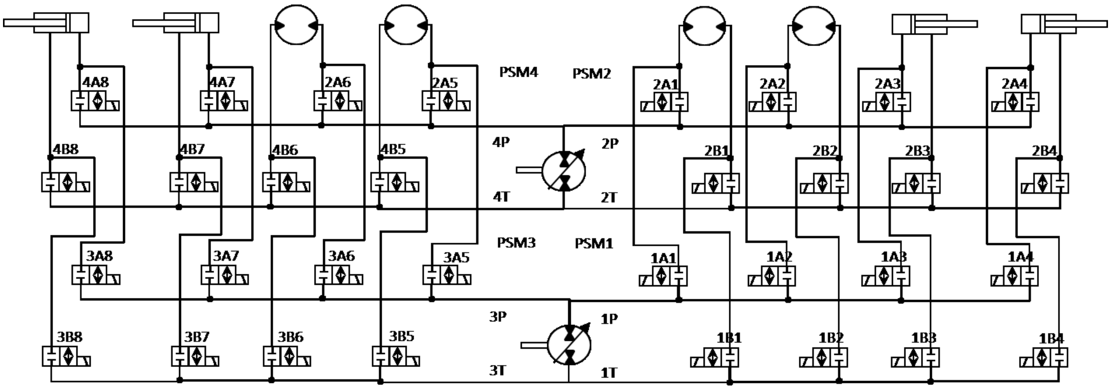


FIGURE 4.10: EXAMPLE OF A 2 PSM STACK EACH ONE WITH 2 PUMPS SERVING 4 ACTUATORS, THE COMPLETE SYSTEM HAS 2 PUMPS SERVING 8 ACTUATORS.

4.5. Mechanical Safety Oriented Design

Spool valves, for instance, and in general all single actuator components, are Category B or 1 classified, in fact they are single actuator systems, then described by a single input to output chain.

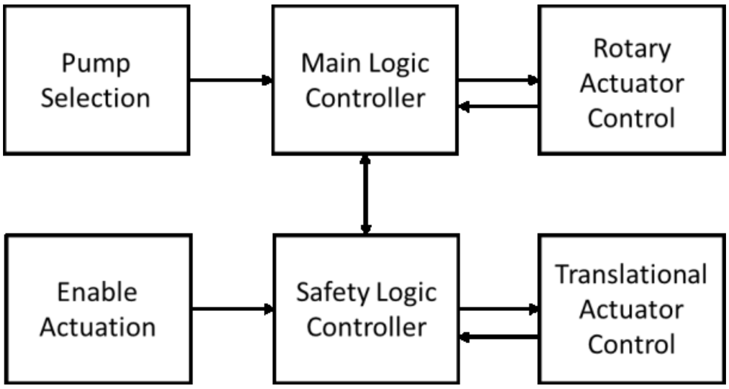


FIGURE 4.11: CATEGORY 4 PSM ELECTRONIC CONTROL SYSTEM ARCHITECTURE

On the contrary, the new component is compliant to category 2 or category 3 or 4 (figure 4.11) hardware, depending on the electronic controller configuration adopted. In fact, the rotation actuator controlling the actuation of the distribution matrix is separated and independent from the translation actuator enabling the pump-actuators connection.

In fact, if the first function of the translation actuator is to enable the oil flow only when the rotation actuator is faced with the desired actuator A and B connections, the secondary function is safety: the actuator movement can be stopped at any time just by switching off the translation spool. Moreover in case of power failure all the movements are blocked.

Another feature, is the possibility to perform an emergency opening in case of fault of one of the two actuators. In fact, in electro-mechanical and electro-hydraulic systems, such as proportional valves and motors, a current control is ever possible, allowing the total electrical faults control over the actuator, and a position sensor is most of times included in safety critical applications, in order to totally control the actuator status in respect to both type of faults (mechanical and electrical). By the system point of view many different fault coverage can be applied through pressure switch or pressure sensors, depending on the safety integrity level of the application. All these acquisitions can contribute to evaluate the valve status.

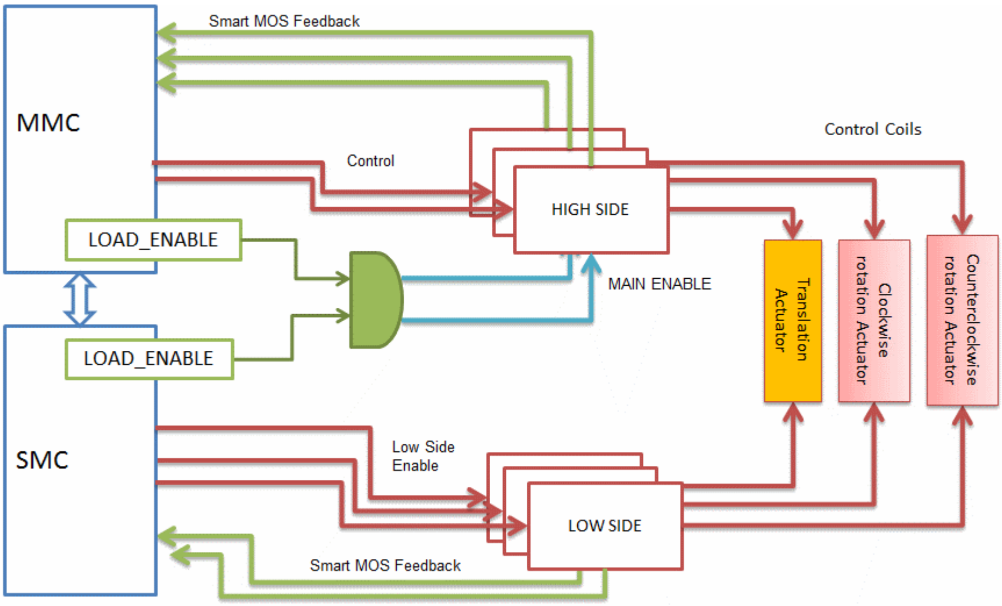


FIGURE 4.122: ELECTRONIC CONTROL SYSTEM ARCHITECTURE

A possible solution can be implemented reusing the general architecture described in chapter 2. The electronic solution using a Category 3 is shown in figure 4.12, where a complete redundant electronic control structure is presented. In the figure a couple of microcontrollers are connected with rotation actuator and translation actuator respectively. Then from the safe state point of view, the two actuators are connected to different logic controllers, offering a fully redundant control of the safe state condition, represented by null oil flow from the pump to the actuators.

The single PSM component can be defined as a fully redundant fail safe component. But the use of more PSM enable also more safe and performant systems.

The new matrix pump switching component, used singularly, is a robust fail silent component; it goes beyond category 1, and it offers the possibility to block oil flow to hydraulic actuators for each fault occurring to one of the two electro-hydraulic actuators (translation and rotation actuators).

When stacked in multiple actuators and multiple pumps configuration, the matrix component stack offers a failure operational features, both in open and in closed circuit configuration, due to the possibility of serving each actuator using any of the pumps. If one of the matrix system sections is faulty, then it will be commanded in the safe state, in which the valve is closed, while the other sections will be able to move any of the actuators. In short every actuator can be operational in case of single fault.

From the system point of view, if any of the pumps is faulty, none of the functionalities will be lost (ensuring safety) meanwhile the performance will be downgraded and the degree of freedom of the system will be reduced. Conversely, from the "single actuation" point of view, the system can be classified Fault Tolerant, due to the possibility of delivering flow from any pump to every single actuator.

On the contrary traditional architectures, based on state of art distribution systems, are generally classifiable as single fault critical, in the sense that "a single fault can cause loss of safety function".

For instance, considering the system described in figure 4.1, when feeding the bucket with the pump 2 and the boom with the pump 4, if one of the valves connecting the pump2 with the boom is faulty open, it can result in an uncontrolled movement of one of the actuators, in consequence of the different load pressures in bucket and boom. In any case this type of faults result, in the best case, in a safe state, where both bucket and boom can no longer be moved. In the worst case instead, the fault leads to an uncontrolled movement of one of the actuators.

Moreover, implementing new connections into scheme of figure 4.1 with traditional 2 way valves in order to increase flexibility worsen the safety because the statement “a single fault can lead to the loss of safety function” is generally true and relevant for each additional valve that can be implemented.

4.6. Conclusions

The matrix pump switching component here presented is a new solution to enhance the flexibility and safety and can be applied to the new efficient architectures for actuation control, like displacement control systems. The compact stacked solution presented implement a physical matrix that, combined with proper pump control, could be employed in a wide range of applications.

The proposed solution applied to multiple pump systems can increase the degrees of freedom in actuators control, enabling effective solutions with a lower number of pumps, corresponding to the number of maximum simultaneous movements expected for the mission profile of each machine type.

The PSM valve, having a double redundancy actuator, is a fail-safe and stackable component that offers a flexible solution without the limits of the existing solutions.

The PSM valve concept includes all possible connections between one pump and all the actuators, moreover the stack of these components build a physical matrix where, in the proposed implementation, more pumps can be connected at the same time to a single actuator.

This solution offers fault recovery capabilities allowing the actuator control even in case of a single matrix component failure. In fact, the faulty component can be driven in its safe state, corresponding to absence of oil flow from the pump to the actuators which can be controlled by another PSM.

To support the PSM system development many challenging activities and research studies have to be planned in the future. First of all further research studies will be addressed to the component design both from functional and manufacturing point of view to correctly evaluate performances, cost and size. Second, the architectural and machine implementation issues have to be approached to estimate the benefits of the new system. Finally after the prototype construction accurate and extensive testing is necessary to assess the performance of component and system.

5. Bibliography

[1] International Electrotechnical Commission, *Functional safety of eletrical/electronic/programmable elctronic safety-related systems,* IEC, 2010.

[2] J. D. Smith and G. L. Kenneth, Functional Safety: A Straightforward Guide to Applying IEC 61508 and Related Standards, Elsevier Butterworth-Heinemann, 2004.

[3] International Organization for Standardization, *ISO 12100 - Safety of machinery - General principles for design - Risk assessment and risk reduction,* ISO, 2010.

[4] A. Avizienis, "Toward systematic design of fault-tolerant systems," *Computer,* vol. 30, no. 4, pp. 51-58, April 1997.

[5] International Electrotechnical Commission, *IEC 61508 - Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 5,* IEC, 2010.

[6] International Electrotechnical Commission, *IEC 61508 - Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems - Part 1,* IEC, 2010.

[7] A. E. Clifton, Hazard Analysis Techniques for System Safety, Wiley, 2005.

[8] International Organization for Standardization, *ISO 60182 - Analysis techniques for system reliability - Procedure for failure mode and effects analysis,* ISO, 2006.

[9] SAE, *SAEJ1739 - Potential Failure Mode and Effects Analysis in Design, Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes.*

[10] N. M. Fenton N., Risk Assessment and Decision Analysis with Bayesian Networks, CRC Press, 2012.

[11] M. Stamatelatos and W. Vesely, Fault tree handbook with aerospace applications, NASA, 2002.

[12] European Parliament, Council of European Union, *Approval and market surveillance of agricultural and forestry vehicles,* Bruxelles, 2013.

[13] European Parliament, European Council, *Directive 2006/42/CE on machinery,* 2006.

[14] International Organization for Standardization, *ISO 14121 - Risk assessment,* ISO, 2010.

[15] International Organization for Standardization, *ISO 62061 - Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems,* ISO, 2012.

[16] International Organization for Standardization, *ISO 13849 - Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design,* ISO, 2010.

[17] International Organization for Standardization, *ISO 13849 - Safety of machinery - Safety-related parts of control systems - Part 2: Validation,* ISO, 2010.

[18] International Organization for Standardization, *ISO 26262 - Road vehicles - Functional safety,* ISO, 2011.

[19] International Organization for Standardization, *ISO 15998 - Earth-moving machinery - Machine control systems using electronic components - Part 2: Use and application of ISO 15998,* ISO, 2012.

[20] International Organization for Standardization, *ISO 15998 - Earth-moving machinery - Machine-control systems (MCS) using electronic components,* ISO, 2008.

[21] International Organization for Standardization, *ISO 25119 - Tractors and machinery for agriculture - Safety-related parts of control systems. Part 1: General principles for design and development,* ISO, 2010.

[22] International Organization for Standardization, *ISO 25119 - Tractors and machinery for agriculture - Safety-related parts of control systems. Part 2: Concept phase,* ISO, 2010.

[23] International Organization for Standardization, *ISO 25119 - Tractors and machinery for agriculture - Safety-related parts of control systems. Part 4: Production, operation, modification and supporting processes,* ISO, 2010.

[24] US Department of Defense, "MIL-HDBK-217F - Military Handbook: Reliability Predicition of Electronic Equipment," 1995.

[25] International Organization for Standardization, *ISO 25119 - Tractors and machinery for agriculture - Safety-related parts of control systems. Part 3: Series development, hardware and software,* ISO, 2010.

[26] E. Busquets and M. Ivantysynova, "The world first displacement-controlled excavator prototype with pump switching - A study of the architecture and control," in *Proceedings of the 9th JFPS International Symposium on Fluid Power,* Matsue, Japan, 2014.

[27] Polarion, *https://www.polarion.com/.*

[28] IBM RATIONAL DOORS, *http://www-03.ibm.com/software/products/en/ratidoor.*

[29] MISRA, *Guidelines for the Use of the C Language in Critical Systems,* MIRA, 2014.

[30] Jet Propulsion Laboratory, *JPL Institutional Coding Standard for the C Programming Language,* JPL.

[31] Gimpel PC-Lint, *http://www.gimpel.com/.*

[32] VECTORCAST, *https://www.vectorcast.com/.*

[33] DSPACE, *http://www.dspace.com/.*

[34] National Instruments HIL, *http://www.ni.com/hil/.*

[35] Astreé, *http://www.astree.ens.fr/.*

[36] POLYSPACE, *http://it.mathworks.com/products/polyspace/.*

[37] R. Isermann, R. Schwarz and S. Stolzl, "Fault Tolerant X-by-Wire System," *IEEE Control Systems, vol. 22, no. 5,* pp. 64-81, 2002.

[38] S. Bak, D. K. Chivukula, O. Adekunle, M. Sun and M. C. L. Sha, "The System-Level Simplex Architecturefor Improved Real-Time Embedded System Safety," in *The 15th Real-Time and Embedded Technology and Applications Symposium*, San Francisco, CA, 2009.

[39] E. Beckschulze, F. Salewski and S. Kowalewski, "A Comparison of Dual-Core Approaches for Safety-Critical Automotive Applications," *SAE International Journal of Passenger Cars - Electronic and Electrical Systems,* vol. 2, no. 2, pp. 301-308, 2009.

[40] A. Kohn, M. Kabmeyer, R. Schneider, A. Roger, C. Stellwag and A. Herkersdorf, "Fail-operational in safety-related automotive multi-core systems," in *10th IEEE International Symposium on Industrial Embedded Systems*, 2015.

[41] VDA, *Standardized E-Gas Monitoring Concept for Gasoline and Diesel Engine Control Units,* 2008.

[42] Infineon, "CIC61508 User Manual," 2012. [Online]. Available: http://www.infineon.com/dgdl/CIC61508-User-Manual-v2.2.pdf. [Accessed 15 02 2016].

[43] Infineon, "HITFet Application Note," [Online]. Available: http://www.infineon.com/dgdl/ApplicationNote_v12.pdf.

[44] R. Eaton, J. Katupitiya, K. W. Siew and K. S. Dang, "Precision Guidance of Agricultural Tractors for Autonomous Farming," in *2nd Annual IEEE Systems Conference*, Montreal, Canada, 2008.

[45] T. K. Hamrita, J. S. Durrence and G. Vellidis, "Precision farming practices," *IEEE Industry Applications Magazine,* vol. 15, no. 2, pp. 32-42, 2009.

[46] International Organization for Standardization, *ISO 11783 -Tractors and machinery for agriculture and forestry - Serial control and communications data network,* ISO, 2010.

[47] C. Fantuzzi, S. Marzani, C. Secchi and M. Ruggeri, "A distributed embedded control system for agricultural machines," in *IEEE International Conference on Industrial Informatics*, 2006.

[48] J. Zimmerman and M. Ivantysynova, "Hybrid Displacement Controlled Multi-Actuator Hydraulic Systems," in *Proceedings of the 12th Scandinavian International Conference on Fluid Power*, Tampere, Finland, 2011.

[49] G. L. Zarotti, "Circuiti oleodinamici - nozioni e lineamenti introduttivi," Quaderni tematici - IMAMOTER, 2006.

[50] P. Marani, G. Ansaloni, R. Paoluzzi and A. Fornaciari, "Test methods for flow sharing directional valves," in *Power transmission and motion control*, Bath, 2006.

[51] P. Marani, G. Ansaloni and R. Paoluzzi, "Load sensing with active regeneration system," in *Proceedings of the 7th JFPS International Symposium on Fluid Power*, Toyama, 2008.

[52] C. Meyer, O. Cochoy and H. Murrenhoff, "Simulation of a multivariable control system for an independent metering valve configuration," in *Proceedings of the the 12th Scandinavian International Conference on Fluid Power*, Tampere, Finland, 2011.

[53] A. Dell'Amico, M. Carlsson, E. Norlin and M. Sethson, "Investigation of a Digital Hydraulic Actuation System on an Excavator Arm," in *The 13th Scandinavian International Conference on Fluid Power*, Linkoping, Sweden, 2013.

[54] M. Heikilla, M. Linjama and K. Huhtala, "Digital Hydraulic Power Management System with Five Independent Outlets –Simulation Study of Displacement Controlled Excavator Crane," in *The 9th International Fluid Power Conference*, Aachen, Germany, 2014.

[55] M. Vukovic, S. Sgro and H. Murrenhoff, "STEAM - A holistic approach to designing excavator systems," in *9th International Fluid Power Conference*, Aachen, Germany, 2014.

[56] C. Williamson, J. Zimmerman and M. Ivantysynova, "Efficiency study of an excavator hydraulic system based on displacement controlled actuators," in *ASME Symposium on Fluid Power and Motion Control*, Bath, UK, 2008.

[57] M. Ruggeri and P. Marani, "A new high performance roto-translating valve for fault tolerant applications," in *SAE 2014 Commercial Vehicle Engineering Congress*, Rosemont, Illinois, 2014.

6. Author's publication list

Conference papers

[1] M. Ruggeri, G. Malaguti, M. Dian, C. Ferraresi "Quasi Isochronous Wireless Communication Protocol For Co-Operative Vehicle Clusters", ISTVS 2012

[2] C. Ferraresi, M. Dian, G. Malaguti, M. Ruggeri "Isobus Over Ethernet: A First Implementation", 7th FPNI 2012

[3] G. Malaguti, M. Dian, C. Ferraresi, M. Ruggeri "Comparison On Technological Opportunities For In-Vehicle Ethernet Networks", IEEE INDIN 2013

[4] G. Malaguti, C. Ferraresi, L. Dariz, M. Ruggeri "Augmented Reality Vehicle-Connected Apps for Diagnosis, Fault Recovery and Vehicle Maintenance ", SAE COMVEC 2014

[5] L. Dariz, M. Ruggeri, C. Ferraresi, "A Comparison Between Configuration Strategies for IEEE 802.15.4 Low-Latency Networks", IEEE ICIT 2015

[6] M. Ruggeri, P. Marani, G. Massarotti, C. Ferraresi "New Matrix Pump Switching Valve", SAE COMVEC 2015

[7] M. Ruggeri, A. Ceversato, C. Ferraresi, "Rear Wheels Electro-Hydraulic Steering Control System with Reduced Performance Level Required", SAE COMVEC 2015

Journal Papers

[J1] M. Ruggeri, C. Ferraresi, L. Dariz, G. Malaguti "A High Functional Safety Performance Level Machine Controller for a Medium Size Agricultural Tractor", SAE International Journal of Commercial Vehicle 2014