Tampere University

Vili Eloranta (TAU)

SAFETY OF ZONAL HYDRAULICS IN NON-ROAD MOBILE MACHINERY

Master of Science Thesis
Faculty of Information Technology and Communication Sciences
Asst. Prof. Tatiana Minav
Assoc. Prof. Paavo Rasilo
June 2020

ABSTRACT

Vili Eloranta: Safety of Zonal Hydraulics in non-road mobile machinery
Master of Science Thesis
Tampere University
Master's Degree Programme in Electrical Engineering
June 2020

As governments from multiple nations encourage novel and inherently emission free power trains to be commissioned, multiple machinery manufacturers are developing their own solutions in response. This thesis focuses on one of the solutions, a Zonal Hydraulics concept that is a combination of electrohydrostatic actuators implemented in non-road mobile machines.

When the new novel systems are introduced to market the safety must be ensured. Currently standards mainly cover the conventional mobile machines with 12 – 24 VDC systems, and therefore they are not up to date for the ZH designed for higher voltages.

The system design for NRMM, which has replaced the conventional hydraulics with Zonal Hydraulics concept, includes direct electric motor control that has expected voltage levels of 700 – 800 VDC and hydraulic actuators. Currently this type of complete system is not covered in a single standard and requires designers to investigate from multiple sources. In this thesis, a review of the current safety standards from multiple fields was realized to gain knowledge on possible future requirements.

This thesis includes a hazard analysis for an electrified micro-excavator case that has Zonal Hydraulics system implemented to replace the conventional hydraulic ones. The hazard analysis was performed by using the Japanese digging cycle (JCMA07) in a tight operational environment to increase possible hazards when using the novel hydraulic system. The hazard analysis was done based on ISO 19014, and the gained performance level requirements were later used in the safety system design.

The safety system design was proposed following the requirements found in standards and based on the performance level attained from the hazard analysis. The safety system was designed to be redundant for high reliability. The system was composed from two control units that each had their corresponding electric and hydraulic safety actuators.

Keywords: EHA, electrification, functional safety, hazard analysis, NRMM, Zonal Hydraulics

TIIVISTELMÄ

Vili Eloranta: Zonal hydrauliikan turvallinen implementointi muuhun kuin tieliikennekäyttöön suunnatuille työkoneille
Diplomityö
Tampereen yliopisto
Sähkötekniikan diplomi-insinööri tutkinto-ohjelma
June 2020

Koska useat valtiot pyrkivät säännöksillä ohjaamaan laitesuunnittelijoita luomaan uusia luonnostaan päästöttömiä voimansiirtoratkaisuja, myös monet laitevalmistajat ovat alkaneet kehittää omia ratkaisujaan. Työssä keskitytään yhteen mahdolliseen ratkaisuun, Zonal-hydrauliikkakonseptiin, joka on muuhun kuin tieliikennekäyttöön suunnatun työkoneen hydrauliikkajärjestelmä ja koostuu useasta erillisestä sähköhydraulisesta toimilaitteesta.

Kun uusia ratkaisuja tuodaan julki, on niiden turvallisuus taattava. Nykyiset standardit käsittelevät käytännössä vain 12 – 24 VDC tason työkoneita, eivätkä siksi ole ajan tasalla toimilaitteille, jotka on toteutettu korkeammalla jännitetasolla.

Käsitellyissä sähköistetyissä työkoneissa on korvattu perinteinen hydrauliikkajärjestelmä Zonal-hydrauliikkakonseptilla, joka sisältää suoran moottoriohjauksen, 700 – 800 VDC odotetun jänniteluokan ja hydraulisen toimilaitteen. Vastaavaa järjestelmää ei ole käsitelty yksittäisessä standardissa, mikä vaatii suunnittelijoita tutustumaan useaan aihetta sivuavaan dokumenttiin. Työssä toteutettiin katsaus nykyisiin standardeihin tarkoituksena kerätä tietoa vaatimuksista sekä mahdollisista tulevista säännöksistä.

Työ sisältää riski- ja vaara-arvioinnin sähköistetylle mikrokaivinkoneelle, jossa perinteinen hydrauliikkajärjestelmä on korvattu Zonal-hydrauliikkakonseptilla. Arviointi toteutettiin ahtaassa työtilassa ajetulle japanilaiselle kaivuusyklille (JCMA07), jotta tarpeeksi korkeat turvavaatimustasot saavutettiin. Arvioinnissa käytettiin ISO 19014 standardia ja saatuja turvallisuusvaatimustasoja hyödynnettiin turvajärjestelmäsuunnitelman luomisessa.

Turvajärjestelmäsuunnitelma toteutettiin käyttämällä standardeista löydettyjä vaatimuksia sekä aikaisemmin saatuja vaatimustasoja. Jotta korkea toimintavarmuus saavutetaan, on ehdotettu turvallisuusjärjestelmä toteutettu redundantilla mallilla. Turvallisuus toteutettiin kahdella ohjauspiirillä, jotka molemmat ohjaavat omia sähkö- ja hydrauliikkatoimilaitteita.

Avainsanat: EHA, ei-tieliikenne työkoneet, riski ja vaara arviointi, sähköistäminen, toiminnallinen turvallisuus, Zonal hydrauliikka

PREFACE

I want to thank both teams in Aalto and Tampere university that provided me support and help during my master's thesis. I wrote this thesis under surprising circumstances, and the flexibility of the groups really made it all possible.

I would like to thank my supervisor Asst. Prof. Tatiana Minav for providing me this opportunity and Assoc. Professor Paavo Rasilo for providing me important feedback.

For my friends and family, I want to express my deepest gratitude for trusting in me and helping me in more ways than one during my studies. Know that I will be there for you whenever you need me.

For my lovely fiancée I just want to say,

I can't wait to start my life together with you.

Tampere, 24 June 2019

Vili Eloranta

CONTENTS

LIST OF ABBREVIATIONS AND SYMBOLS

AC	Alternative Control
AR	Ability to React
AW	Awareness of Hazard
BMS	Battery Management System
DC	Diagnostic Coverage
E	Exposure
EHA	Electrohydrostatic Actuator
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
HIPOT	High Potential Test
ICE	Internal Combustion Engine
PELV	Protective Earth Low Voltage
PL	Performance Level
QM	Quality Measure
RESS	Rechargeable Energy Storage System
S	Severity
SCS	Safety Control System
SIL	Safety Integrity Level
SRP/CS	Safety Related Part of the Control System
MCSSA	Machine Control System Safety Analysis
MPLr	Machine Performance Level required
MTTFd	Mean Time to Dangerous Failure
PFHd	Average Probability of Dangerous Failure per Hour
PLC	Programmable Logic Controller
PMSM	Permanent Magnet Synchronous Machine
VAC	Voltage, Alternative Current
VDC	Voltage, Direct Current
ZH	Zonal Hydraulics

A	*application use case*
a	*acceleration*
F	*force*
H	*hazard time*
P	*person group exposure*
S	*severity*

1. INTRODUCTION

As emission regulations become tighter and governments are planning to ban internal combustion engines (ICEs) [1], various sectors must respond to the challenge with alternatives. The automotive industry is already adapting and provides more eco-friendly solutions to private customers, such as hybrids or fully electric vehicles. The same type of movement can now be recognized with non-road mobile machinery (NRMM), but in smaller scale. In the private market sector, customers are willing to pay for ecological and green products [2] but companies and industries still value low investment costs more than efficiency and fear long payback times. Therefore, it is of utmost importance for the new emerging green solutions to be also cost effective in order to get a foot hold in the market.

Many machine manufacturers are currently working on the electrification of NRMM for emerging market sectors but have yet to gain breakthroughs with their products. Current solutions mainly consists of existing machine designs with slight changes, for example an excavator swing drive switched from conventional hydraulics to electrically driven [3–5]. When utilizing the electrically driven methods for control the excess kinetic or potential energy recovery is made possible.

Easy Zonal hydraulics (EZE) project funded by Business Finland has focused on more efficient and controllable hydraulic system by replacing the conventional centralized valve system. The new concept, called Zonal Hydraulics (ZH), improves the energy efficiency while keeping the benefits of fluid power technology and increasing the controllability by opening a path for full automation.

As the most applications that utilize ZH includes multiple actuators that are all inducing electric currents to chassis, through switching inverters or electromagnetic properties of electric motors, the protection and limitation of these phenomena must be well thought. Currently there does not exist a standard that would cover all the topics related to ZH or even proposed solution. This increases the difficulty to design safety systems and the sheer number of standards can overwhelm the researchers.

The main goal for this thesis was to gather informative package of the most relevant and current standards for implementation of ZH. The standards mostly focused in this thesis are from earth-moving machinery (EMM) as the later performed hazard analysis and system design will focus on a micro-excavator. But if the requirements are not governed

in that sub-category, they are picked from other related fields, such as agricultural machines or electrically propelled machines. The requirements are mainly gathered around safety functions that can be implemented by machine manufacturers. This thesis does not cover tests that are used by standardization organizations to ensure the requirements are followed.

Together with the safety requirements and functional safety standards the hazard analysis was performed for micro-excavator with a purpose of achieving the functional safety level requirement for individual actuator in ZH system. The hazard analysis was done with the methods found in ISO 19014.

After achieving requirements from the standards and the required safety level from hazard analysis, conceptual safety system design was proposed. The design was based on methods found in ISO 13849 but complete estimation of achieved safety levels would require actual building of prototype, and thus was not provided.

This thesis will first gather necessary background explanations and introduce the reader to NRMM and to ZH in chapter 2. In Chapter 3, there is summarized information related to regulations and recommendations found in standards. The information was picked from different standards in hopes of gaining safety information for: high-voltage, hydraulic systems, functional safety and other relevant information. Chapter 4 in the thesis, includes case study of hazard analysis for a micro excavator to define the necessary safety level for ZH. With the safety level requirement, a conceptual safety system design is proposed in chapter 5.

2. BACKGROUND ON THE ELECTRIFICATION OF NON-ROAD MOBILE MACHINERY

The term NRMM can be applied to describe a broad variety of machines, from compact to large, from work to consumer machines. Examples of NRMMs employed in work operations can be observed in Figure 1. Depending on the designated work, the operation time and energy demands vary significantly from a few hours of low power operation for gardening vehicles to around the clock operation of high-power underground machines. The variety of machines is as high as the number of different work tasks that demand to be fulfilled [2]. Traditionally, these machines are driven by ICEs to perform work tasks and hydraulic systems is connected to the same engine. Now as the fuel resources are finite and emission regulations are getting tighter, many machine manufacturers are investigating hybridization and electrification as an alternative solution. Both solutions inherently increase the energy efficiency as well as limit the local emissions created [6]. This by itself solves many challenges, for example one of the clearest fields to benefit, the mining industry, could gain large savings from reducing the amount of costs tied to ventilation of exhaust gasses out of tunnels in underground mining [2].

Figure 1. *Examples for NRMM: Volvo wheel loader (left), Komatsu micro-excavator (top right), Sandvik mining machine (bottom right) (from manufacturers' websites)*

One of the significant disadvantages of conventional ICE powered NRMM is the difference in average power required and peak power demand. With conventional NRMM the

engine is sized for the maximum loads that are in most cases present only a fraction of the work cycle, thus wasting power [2]. Also, while operational, the hydraulic pumps and motors are constantly rotating to be able to respond to the sudden power spikes. This means that the machine is wasting energy even when just idling [6].

The NRMM focused in this thesis is JCB 8008 cts 1-tonne micro excavator, which is modified to include the ZH and fully electric power train. The machine can be examined in Figure 2.

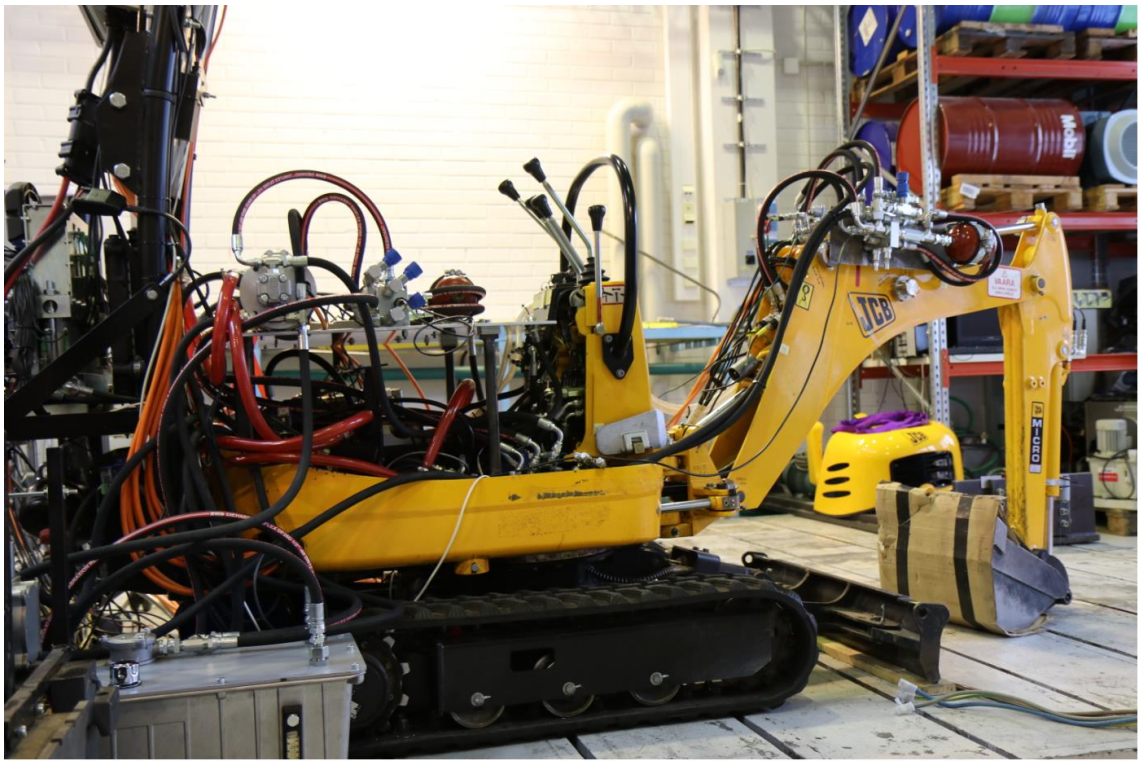


Figure 2. *Electrified JCB 8008 cts with earlier version of ZH*

This thesis focuses on the analysis of requirements for the safe operation of the machine in question. The challenges related to electrification of the machine are investigated and a conceptual actuator design is proposed based on the requirements found in the standards.

2.1 CHALLENGES FOR THE ELECTRIFICATION OF NON-ROAD MOBILE MACHINERY

Even though there are definite benefits to be gained with electrification, it took a long time until a more noticeable breakthrough in the market was achieved. There are many reasons which are slowing down the progression. There are for example, the technological challenges, lack of customer base for green solutions, high costs of power electronic

components as well as the policies from regulatory bodies to encourage more energy efficient solutions [7].

One other factor slowing down the process is the diversity of machine types and machine manufacturer'. There is no single power train model suitable for all machines. Usually these types of machines are designed for highly specified operations, overlooking factors such as consumption, efficiency, and emissions. Also, electric power trains cannot be easily implemented on all of the machines, for the strict specifications of work cycles, and power demands [6]. For this reason, this thesis is providing broader guidelines and limitations for safe implementation of the actuator.

The challenges that designers and manufacturer face with electrified NRMM include:

- High costs of power electronic components, (converters, power switches…)
- High energy and power demands
- Large loads-, and impact shocks for actuators
- Strict requirements for components durability and reliability
- Harsh environmental conditions
- Compliance with electrical safety standards

Only a short and realistic payback time can justify higher investments and make electrified NRMM compatible on the market. Even though the prices for individual components such as power electronics, motors, and batteries are constantly decreasing as the production amounts increase, one valid option is to do partial electrification through hybridization. With hybridization, various benefits of electric systems can be achieved, while retaining longer operation times and achieving higher efficiencies [8]. With hybrids, it is also possible to achieve a more redundant system as by having two separate power trains allows the utilization for two separate power sources. This would, if properly implemented, increase the reliability and safety of the machine. This thesis will focus on the requirements for the components to ensure the safety of the proposed system, thus easing the implementation of more electrified solutions. The proposed ZH system will be introduced in the next section.

2.2 ZONAL HYDRAULICS IN FULLY ELECTRIFIED NON-ROAD MOBILE MACHINERY

To answer the challenges related to electrification, researchers at Aalto and Tampere university, have proposed to utilize ZH with electro-hydraulic actuator (EHA) instead of conventional hydraulic systems. This way metering losses caused by valve control are eliminated while the benefits of the conventional hydraulic systems remain. The EHAs can be implemented in both fully and partially electrified machines. Both have the benefit of energy recuperation thus increasing the efficiency even further.

The ZH system refers to combination of EHAs implemented in singular machine. The ZH concept is aimed at have energy efficiencies close to the ones of mechanical and electrical power trains while having the robustness of conventional hydraulic systems. The system should also be as power-dense as conventional hydraulic systems. For conventional hydraulic actuators only the weight of the cylinder itself and its tubes is attached to the moving parts of NRMM but with ZH, the weight of all power electronics is added right next to the cylinder [6, 7]. Simplification of ZH system implemented in excavator is depicted in Figure 3.

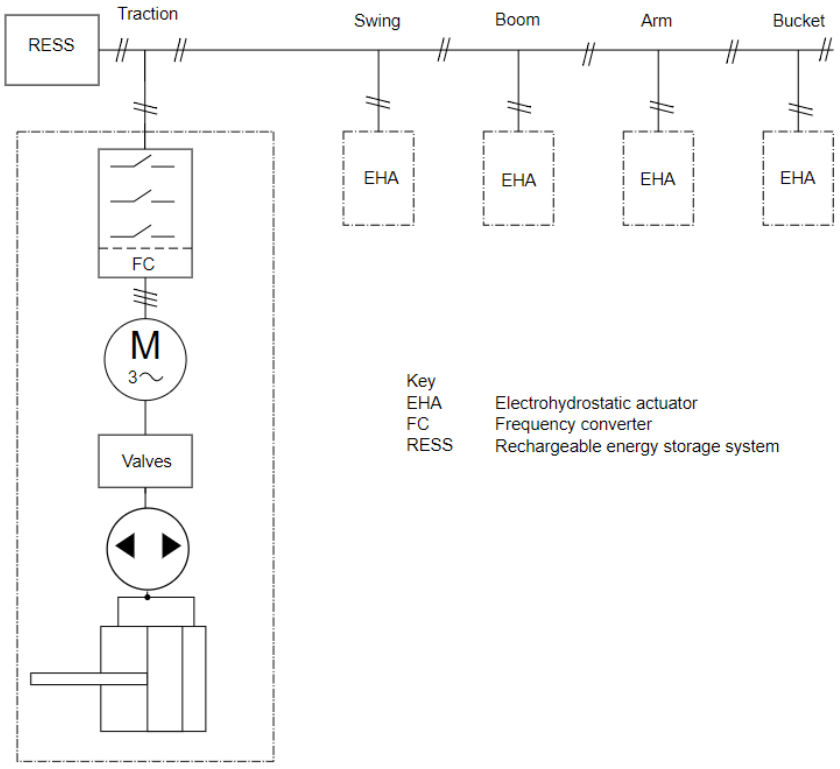
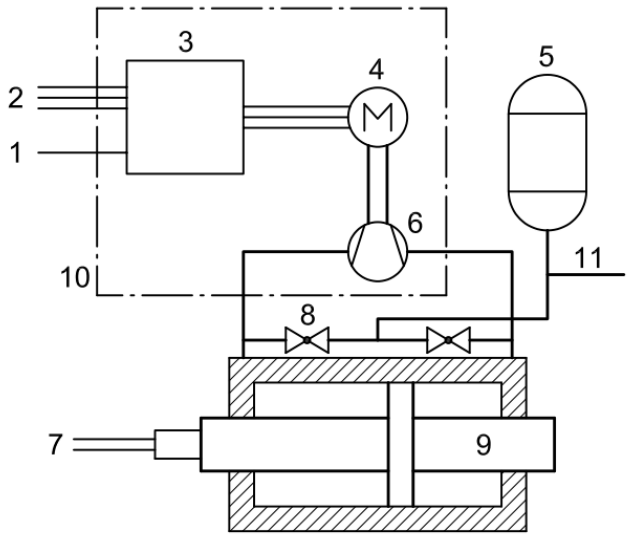


Figure 3. *Presentation of Zonal Hydraulics in excavator*

ZH concept consists of multiple individual EHAs that are connected to the same voltage bus where the power is delivered with RESS. The depicted Figure 3 demonstrates some of the benefits and disadvantages of the system. Now with more localized hydraulic systems the piping's are left short, but this means that the electric power cables are longer compared to the conventional system. Also, as the cylinders on NRMM might be located outside the frame, for example on the tip of an excavator arm, the electric cables require to be selected to withstand the imposed friction and environmental challenges.

For the first time, EHAs were introduced in aerospace industry. There regulations have quite heavily affected their safety design, which in turn has increased the costs of the said systems, making it difficult to adopt them in other industries. With NRMM the same limitations and requirements are not imposed, at least not at the same scale, making EHAs a viable option for replacing conventional hydraulics. The ISO 22072 [9] was created for aerospace as a tool to help defining and documenting individual proposed EHAs for aircrafts. Its basic system model is introduced in Figure 4.



Key

1	command signal	7	position transducer signal
2	power supply	8	anti-cavitation check valve (two places)
3	electronic module	9	piston
4	electric motor	10	**Electro hydrostatic module**
5	reservoir	11	filling port
6	pump		

Figure 4. *EHA defined by ISO 22072 [9]*

The EHA consists of power electronic components, such as power source, and inverter, which controls the electric motor, which then drives the pump that provides flow to hydraulic system. Usually the electric motor is selected to be a permanent magnet synchronous machine (PMSM). This allows improved control, high power densities, reduced parasitic losses, and lowered maintenance costs compared to other available motor designs

[10]. The PMSM is utilized to drive the pump, with a desired direction, which then results in flow for the hydraulic cylinder. A single NRMM can employ multiple of these individual EHAs on the complete machine. The operational voltages are usually high which require to be considered in the safety design [8].

The term high voltage can be somewhat misleading especially when comparing multiple separate standards and sources. In this thesis as well as for example ISO 16230 [11], high voltage is meant to represent voltage between 75 VDC to 1500 VDC. But for example in ISO 14990 [12], the high voltage safety is derived from electricity grids thus refers to voltages from 1kVDC up to 36 kV. The voltage level requires to be carefully designed to consider the current to wire-size ratio and voltage to arching ratio. The voltage level that is currently being standardized for NRMM in ISO 23316 would wind up to 700VDC/480VAC.

As the new proposed ZH differ heavily from conventional hydraulics, the safety requirements must be rethought as well. To start this process, safety designers must investigate hydraulics, high voltage, machinery, and functional safety standards in the design process. Specified standards also provide necessary limitations and operational ranges for the actuators. However, as with the highly specified work machines, designers should keep in mind that the actuator should be flexible in the design depending on the use case scenario.

3. REVIEW OF STANDARDS AND REGULATIONS

In this chapter the safety standards for NRMM, especially for ZH are reviewed. To ensure the safety of purchased machines, the standardization organizations were created. They propose standardized design process and limitations for machines which all the machine manufacturers should follow, thus leveling the competitive advantages. Standardization organizations exist in all levels of regulatory bodies, from international to national. Table 1 below lists these organizations.

Table 1. *Standardization organizations [13], [14]*

	International	European	National (Finnish)
General	ISO	CEN	SFS
Electrical	IEC	CENELEC	SESKO
IT/Tele	ITU	ETSI	Traficom

Mainly the new standards are firstly created by the international organizations together with experts and public hearings where all participants can comment on suggestions. Then it gets adopted by European and later national organizations. Therefore, for products that wish to gain international certificates and acceptance, they should start by creating their designs with the regulations according to the international standards.

Standards are divided to categories, such as basic, product, service, method, and control system. This thesis will focus on the product as well as the control system standards, to inform the reader on compatibility, reliability, structure, and safety regarding implementation of ZH. Standards are also created for multiple fields and from individual actuations to safety of movements. Even category for work machines is divided to multiple fields, which are for example agriculture or earth moving machinery (EMM). These categories can still hold the same requirements with only slight alterations.

The main subcategories include information related to individual mechanics, actuators, and components. ZH are no exception and can be said to be of the more complex end of systems as it involves parts from hydraulic, electrical, and control system points of view. All these parts require their own evaluation, as each one of them can create their own hazards in the system. But when complying with the standardization process machine manufacturers can achieve safety markings for their products.

3.1 ELECTRICAL SAFETY OF ZONAL HYDRAULICS

Even though the hybrid and electrified solutions have been researched and available in the markets for a long time, the fully electric excavator solutions have begun emerging only recently [15]. For the same reason the standardization organizations haven't been able to provide industries with specific information concerning safe implementation of high voltage solutions in a single package. The current standards for high voltage systems in EMM are mainly on a rather basic level derived from those applied in stationary machinery and electricity grids. They state the requirements for which individual actuations and systems need to be safe but does not include the methods nor information on how to achieve higher reliability. Most specific standards that currently exist are for electrical propulsion, especially for electrical road vehicles. One of these standards is ISO 6469 series that focuses on high voltage electrical vehicles. When designing the safety of electrified non-road machines, the relevant applied safety methods from this standard should also be taken into consideration even though the method of movement is different. The basic system design for electrified EMMs is introduced in ISO 14990-3 [16] and depicted in Figure 5.

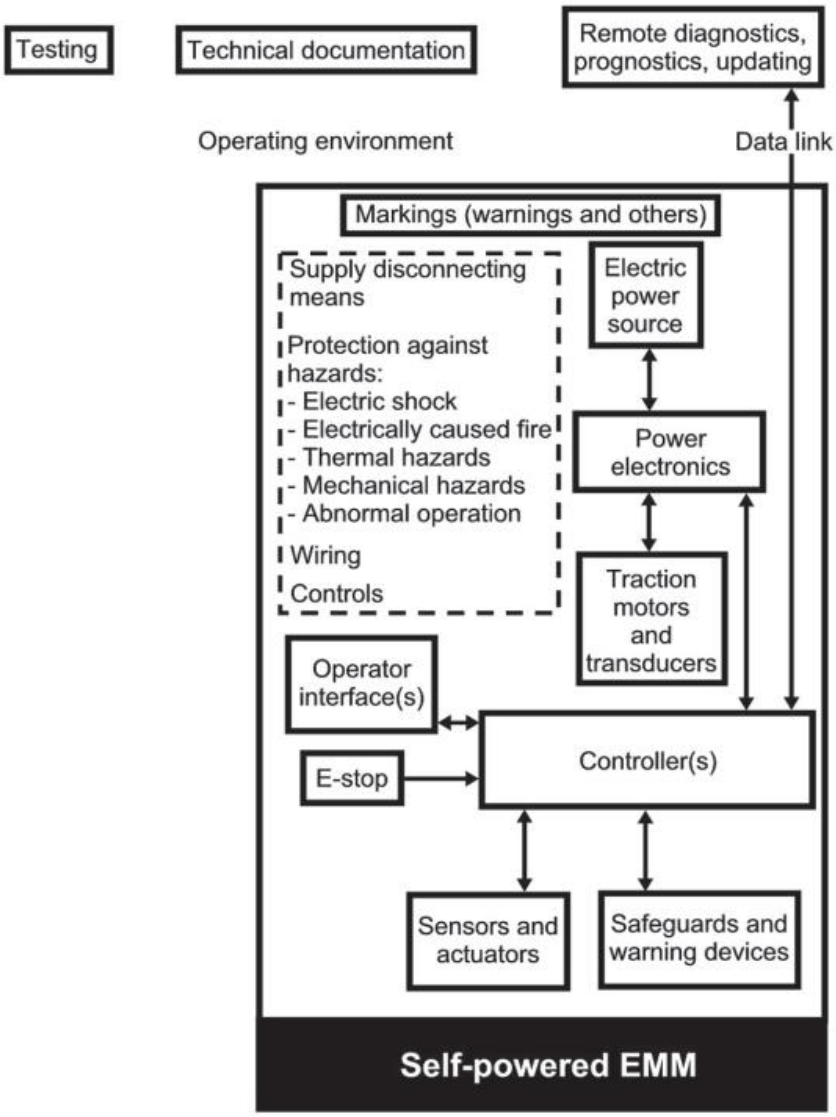


Figure 5. *Typical EMM according ISO 14990-3 [16]*

Figure 5 clarifies the basic design of self-powered EMMs. It depicts the most fundamental protection methods as well as hazards. Most of the individual parts, power electronics, power source, or e-stop has their own standards that must be taken into consideration. In the next sections specific areas of standards are explained and information gathered to help the design process of ZH.

3.1.1 VOLTAGE LEVELS

Traditionally, the NRMM included batteries with voltage ranges of 12 – 24 VDC, which places them in VC-A1 category, which can be examined in Table 2. This has been possible as the traditional NRMM utilizes ICE engines to provide energy for propulsion and the electrical energy is mostly employed for startup and lighting when the engine is not

operating. However, when designing a system that includes electrical propulsion, the higher voltage levels are usually utilized [17]. All related voltage classes are defined in Table 2 below.

Table 2. *Voltage level definitions from standards [11]*

Voltage class	**Maximum working voltage**	
	VDC	VAC
VC-A	$0 < U \leq 60$	$0 < U \leq 30$
VC-A1	$0 < U \leq 32$	$0 < U \leq 21$
VC-A2	$32 < U \leq 60$	$21 < U \leq 30$
VC-B	$60 < U \leq 1500$	$30 < U \leq 1000$
VC-B1	$60 < U \leq 75$	$30 < U \leq 50$
VC-B2	$75 < U \leq 1500$	$50 < U \leq 1000$
U = nominal voltage		

Almost all modern electrified vehicles (EVs) operate in VC-B and in particular at B2, both of which are depicted in Table 2. The increase in voltage provides improvements but also new requirements for the system [18]. The weight of the current carrying part of the voltage cables is decreased, but for example, insulation values must be increased as well as protection methods tightened. Higher voltages pose greater hazard for operator through touch currents, and therefore require strict rules to ensure the safety.

In most cases the resulting machine includes a high voltage bus for energy transfer but also a control voltage bus. Therefore, the safety limitations for combining the two voltage systems must be included in design.

3.1.2 HIGH VOLTAGE SAFETY

Looking into the high voltage safety without strict design limits can prove to be difficult. The requirements differ depending on the connections and if the system has VAC and VDC linked together. As high voltage systems are defined in multiple standards and have small differences between requirements, the ones found in ISO 14990 have the highest factor in this thesis. The standard is directly created for EMMs but is at times lacking as it was created based on stationary and electricity grid standards. Therefore, necessary additional guidelines are taken from standards aimed at electrically propelled vehicles or agricultural machines.

Main difference with low and high voltage machines is that the latter systems must be completely isolated from the chassis in case of the mobile applications. This in practice

means that from the high voltage rechargeable energy storage system (RESS) the cable travels from positive terminal all the way through the machine back to the negative terminal. In conventional machines the chassis is usually kept as the negative return path for circuitry.

The basic protection methods for ensuring insulation [12]:

- Enclosures
- Insulation
- Residual voltage protection
- Barriers
- Placing out of reach
- Class II design
- Automatic disconnection
- Protective Earth Low Voltage (PELV)

Enclosures are implemented to keep the operator from physically accessing the high voltages but also providing protection for circuitry and path for induced voltage to dissipate through the whole chassis. The most basic level of requirements for enclosures containing high voltages are listed in ISO 14990-1 [12] and are:

- IP2X or IPXXB, if enclosure is placed to have limited access, or
- IP4X or IPXXD, if placed so that it is accessible to all persons.

Enclosures also house the power electronics parts that possess their own electromagnetic compatibility (EMC) ratings and limits which are required to be checked when the placement of the said enclosures are decided. This in practice means that to ensure two separate enclosure boxes include a large enough air gap between not to interfere with each other.

All enclosures that contain high voltage open circuitry inside them must be protected with barriers that are meant to limit access, either with complete inaccessibility, accessing with tools, live parts are properly insulated or voltage drops to safe limits [5, 6, 16]. The barriers must also be equipped with the warning symbol W012 as identified in Figure 6.

Figure 6. *High voltage warning symbol W012 [20]*

Insulated wires ensure that without breaking the cable, the operator cannot access hazardous voltages. In stationary cases the insulation usually also works as the outmost layer. With NRMM many of the high voltage cables are connected to actuators that traditionally might have been located outside of the frame. The standards currently inform that cables located in moving parts that might flex during normal operation is required to be relieved from mechanical stress [11].

The standard includes a few recommendations for the protective measures of wear and tear. The first one of these was to encase the cable in protective layering that relieves the tension created from movement. Another was to include the cable in the frame so that they are protected from impacts. The extreme use cases that occur when the cables are located in moving parts and therefore, exposed to the environment, are required to be as high as stated in class 5, from IEC 60228. All factors reducing the operating life such as abrasion, high tensile stress, limited radius bending or high duty cycles, are required to be taken into account when selecting the applied cables [12].

The insulation for high voltage systems, VC-B2, should follow the guidelines from the standards [11, 12, 16, 20, 21]. The minimum insulation should be as follows according to ISO 6469-3:

- VDC circuit systems, $100\,\frac{\Omega}{\mathrm{V}}$
- VAC-circuit systems, that include additional protection in accordance to standards, $100\,\frac{\Omega}{\mathrm{V}}$
- VAC-circuit systems without additional protection, $500\,\frac{\Omega}{\mathrm{V}}$
- And system including both, VAC and VDC the separation insulation, $500\,\frac{\Omega}{\mathrm{V}}$

Or from ISO 14990-3, which states that for all voltages, up to 36 kVDC, the insulation value should be kept at $1\,\mathrm{M}\Omega$. Additional measures to ensure that insulation holds the complete designated life cycle, and keeps high voltage separated from electrical chassis of the machine are [20]:

- double insulation
- reinforced insulation
- protective barriers as well as the basic protection
- protective enclosures as well as the basic protection
- conductive protective barrier that is equipotentially bonded as well as the basic insulation
- sturdy protective barriers and enclosures that are designed to last the complete service life of the machine

With high voltage systems the preventive safety method for insulation failure, is to connect all conductive surfaces together. The equipotentiality is in most cases achieved with protective conductor. Protective conductor is connected to every conductive surface, including not only the chassis of the machine but also enclosures and actuators [16]. This limits the capacitive voltage and capacitive coupling that could gather between circuits and barriers, thus limiting possibility for electric shock to the recipient. The current between electric chassis and all live parts must be limited to touch currents, less than 10 mA [16]. The connection can be assembled with wire, cable, welding or by bolts. Example equipotential connection is demonstrated in Figure 7.

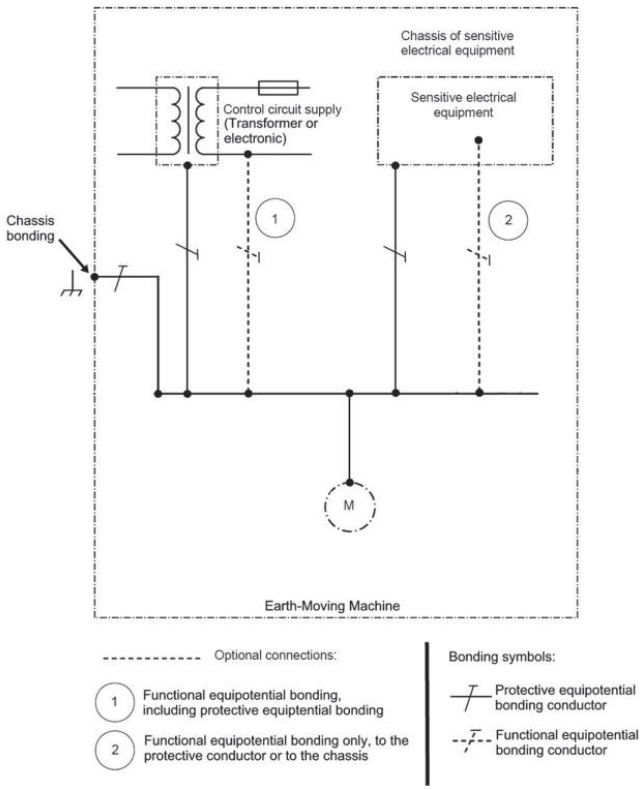


Figure 7. *Example equipotential bonding for EMM [16]*

The complete equipotential path that is formed by connections, chassis, and protective barriers must be rated to handle the maximum currents created in single fault situation [21]. This means in practice that all paths that can be touched simultaneously by one person must possess resistance values less than 0.1 Ω [11]. The equipotentiality cable that is connected to every conductive surface must be designed to handle the thermal and mechanical stress that the earth or chassis fault induces. Cables that carry voltages less than 1000 V shall have the cross-sectional area examined from standards IEC 60364-5-54 or IEC 61439 [21]. The continuation of the protective equipotential bonding must be ensured by placing the cables and conductive parts so that when an individual component is removed the continuation is still ensured [11]. Most of the adjustable speed electrical power drive systems, even when following IEC 61800, have a leakage current greater than 3,5mA VAC [20]. For more details about testing the leakage currents, IEC 61800-5-1 should be referred to[12].

As with most electric systems, it is especially crucial that the high voltage systems are equipped with overcurrent and overcharge protection [12]. As the machine has multiple actuators that all include inverter and an electric motor, the manufacturer should include safety design with high emphasis on the current paths and individual actuators. The safety design must investigate whether each actuator path requires these protection methods, or if ensuring that the whole machine is de-energized in fault condition proves to be enough. These designs are also limited by individual components and drive manufacturers requisitions in creating these complex systems.

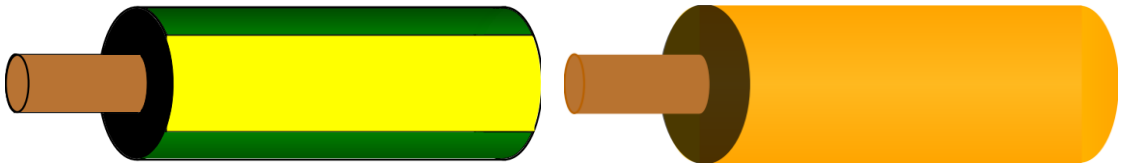
Location of the live parts also affect their safety ratings. If they are located in the operator's workplace they must be within enclosures and protected as IPXXB. Mated connections must be waterproofed, minimum of IPX7 class. Also, the design of the plug and socket is to be formed, so that the equipotential bonding is the first connection to be inserted and last to break. The interlocking device is attached as last part so that it will break first. This ensures that the power outlet either de-energizes within 1 s after disconnection or meets IPXXB and the de-energization value is specified by manufacturer [11].

When shutting off high voltage NRMM, it must be completely de-energized so that no voltage is present in any conductive parts [11]. When the machine is de-energized the voltage must drop below 60 VDC in under 10 s, the circuits possess stored energy less than 0,2 J and touch currents are 5mA for alternative current and 25mA for direct current [11, 12, 20].

One of the most important method for protection against electric shock is to include constant monitoring on insulation between electric chassis and high voltage circuits as well

as for the continuation of the protective conductor [21]. In fact depending on the protective conductor, if it is not able to handle the stress created by a single ground fault, it is vital that the monitoring is constant and able to trigger de-energization of the machine to ensure the safety of the operator [20]. In minimum, if the protective conductors continuation is cut-off, either auditory or visual warning must be issued for operator [12]. Depending on the application, it might be preferable to include insulation measurements to every actuator to ensure that, if necessary, only the faulty actuator can be disconnected, thus maintaining the operation of the rest machine.

When earth leakage currents can be greater than 10 mA, the protective conductor must be protected against mechanical damage or to have cross sectional area minimum of $10\ \mathrm{mm}^2$ for copper or $16\ \mathrm{mm}^2$ for aluminum [19]. The most important cables should be quickly identifiable through coloring. The colors for high voltage cable, orange, and protective conductor, yellow-green, are depicted in Figure 8 [11, 12, 20].



a) b)

Figure 8. *Examples of protective earth conductor (a) and high voltage cable (b)*

The coloring from Figure 8 must hold true also for the protective casing. Another important factor for connections is to ensure that when the operator connects additional implements to the possible power output, it should be galvanically isolated from high voltages for safety reasons. In practice, there should be an isolation transformer between the high voltages and the lower voltage implement. This way, if a single fault occurs, the high voltage cannot “pour down” to operators implement thus creating a hazard [22].

3.1.3 ELECTROMAGNETIC COMPATIBILITY

High voltages do not only create hazards if touched directly by user, or by single fault leading to short circuit, but also for their capacitive and inductive properties. In the previous chapter the equipotential path was introduced, which is used as the main protection against induced electric hazard [19].

The cabling routes must be carefully designed to lessen the mechanical stress but also to limit the electromagnetic interference (EMI). Therefore, it is highly recommended to

keep separate voltage level cables on their corresponding routes or ducts [12]. Alternative option would be to include high enough insulation to block the interference. In IEC 60664-1, there are clearance calculations, if only single duct is utilized. Alternative cabling management can be examined in Figure 9.

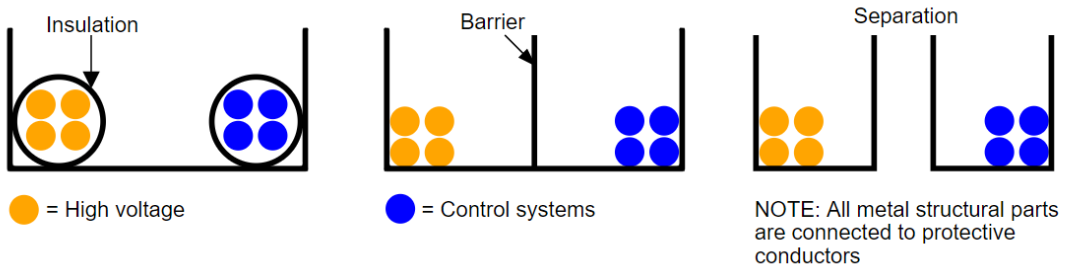


Figure 9. *Examples for protective separation (adapted from [19] and [23])*

The duct or barrier depicted in Figure 9 must also be connected to the equipotential circuit. Similarly, as with cables the space between other electric parts must also be evaluated.

The induced currents, or high current ripple in VDC-bus, might if not considered, also affect the control systems of the machine. As many of the components are packed together as tightly as possible the EMC limitations must be carefully inspected so that the required safety distance between the components can be designed. Usually component manufacturers provide their own evaluation results how much EMI can the component hold.

As these factors listed are of high importance in terms of machine safety, ISO has created standards for testing the EMC properties of EMMs. Standards ISO 13766-1 and 2 hold information on what type of stress the EMMs must be put under, and how it must perform in order to pass the tests [24]. Similar tests are run on electric motors and inverters by their manufacturers and their manuals should hold information if they correspond with the EMMs requirements. For electrically propelled vehicles EMC tests can be found in ISO 11451-1 [21]. In the future, when functional safety standard ISO 19014 for EMMs is completed, it will provide information on the EMC requirements as well [25].

The EMC test are usually performed by independent laboratories as the equipment utilized are expensive and complex to use. For electric drives the IEC 61800 provides test methods for clearance levels for EMC levels. Other generic test methods can be found in IEC 61000 series [19].

3.1.4 SUMMARY

The most important electric safety related requirements from the standards were the constant insulation and isolation monitoring between high voltage and electric chassis. This limits the possibility for electric shock when operator touches the surface of the machine. The challenges that arise from these floating systems are the need for return wires and possible filtering for electric systems. As the high voltage cables could induce interference to other cabling routes for example control signals, the cabling routes and insulation is required to be properly designed and all conductive parts connected in series.

These important factors must be considered when designing the implementation of ZH powertrain in systems that carry these high voltages. The complete design for actuator must include methods for connecting the system to chassis, clear design on the produced and shielding of EMI, proper routing for low and high voltage systems, protection against unexpected start-up, monitoring for multiple factors, and protection again external stress such as mechanical of environmental.

The high voltage related hazards can be the most dangerous ones and are therefore covered in higher value. However, reliability of lower voltage level control system is also important part of the design. Other important safety values and limitations for ZH are listed in Table 3, for more intelligible presentation.

Table 3. *Summary of requirements from standards [12, 16, 20, 26]*

Topic	**Requirement**
Components	Specified in corresponding IEC standards IEC 60664 for creepage and clearance, or pass hipot (high potential test)
Conductors and cables	Conductor and cable insulation, hazardous environments to be considered, flexing, winding, tensioning, protection for friction. Isolation between high voltage, and electric chassis are required to be monitored.
Controls	Control circuit supply/protection, interlocks, function in event of failure, operator interface, control gear, enclosures, access.
Disconnection of power	Complete engine stop acceptable, required disconnect characteristics, battery disconnect required. Up to designer, if multiple de-energization points are designed.
Electric motors and generators	Overcurrent, overload, overspeed protection, General design, and selection criteria's in section 3.3.
EMC	ISO 19014 series (when released) Tests: ISO 15998, ISO 13766, ISO 11451, IEC 61000, IEC 61500
Enclosure IP rating (not in cabin)	Must be adequate: IP 22 for control gear or IPXXB at minimum. All components exposed to environment must to have IP 55.
Equipotential bonding	Protective conductors, bonding circuit, connections, high leakage currents, functional bonding, continuity for the protective circuit. Markings and central bonding terminal are required. Measuring circuit to provide feedback on the continuity.
Manuals and technical documentation	List of information on items is required as well as service manuals
Markings	Shock hazard: Figure 6, Arc flash/blast: ISO 9244 Hot surface: ISO 9244, Magnetic field: ISO 70110-W006 Residual voltage warning, nameplate requirements, marking required if leakage > 10mA VAC or VDC systems
Non-motor loads	Overcurrent protection required.
Overcurrent protection/ equipment protection	By a circuit breaker, control system, or a fuse. Motors, over temperature, over speed, earth or chassis fault, overvoltage.
Prevention of unexpected startup	Required, usually with multiple actions are to be performed by operator for machine start up.
Protection against electric shock hazards	By enclosure, insulation, isolation, residual voltage protection, barriers, placing out of reach, class II design, automatic disconnection or PELV.
Tests	Automatic disconnection, Bonding continuity, insulation resistance (ISO 14990 $\geq 1M\Omega$, ISO 6469-3 $\geq 100\frac{\Omega}{VDC}, 500\ \Omega/VAC$) Hipot (2 times supply voltage, or 1000V) Residual voltage (less than 60 V in 10 s)
Vibration	ISO 15998 currently recommended
Wiring	Connections, routings, identification of wires, flexing, concealed or exposure, plug/socket, ducts, boxes, conduits.

3.2 HYDRAULIC SAFETY OF ZONAL HYDRAULICS

Even though the high voltage electrical safety is emphasized in the thesis, there are still requirements and limitations posed on hydraulic systems. When creating the ZH systems, the following hydraulic factors must be taken into consideration [27]:

- Pressures: working and maximum operating ranges
- Temperature: environmental and operational ranges
- Utilized hydraulic fluids
- Flowrate
- Lifting capabilities
- Requirements for safety and energy isolation, (accumulator)
- Painting, protective coating, and casing for the piping

The main safety related requirements are to design the complete hydraulic system to withstand the created pressures. The requirements are usually matched by creating the hydraulic systems to be able to withstand two times the maximum pressures without rupturing the piping [9]. In every actuator's hydraulic circuit, there should be a pressure relief valve, to decrease the risks of sudden increase in system pressure [27].

One of the benefits of ZH is the factor that hydraulic piping's are generally kept short and located close to the actuator. This naturally follows safety measures mentioned in ISO 20474 [26], where the high pressure hydraulic parts are expected to be at least 1 m away from operator. The positioning of the said system is still required to be carefully designed to limit the deterioration of hydraulic parts. The hydraulic parts should be located far from hot surfaces, sharp edges, possible collisions and other factors that might limit the use life.

Another important safety factor is to design the acceptable vibration limits from actuator and include methods of damping for both electric and hydraulic parts [27]. As all the high frequency inverter, high speed motor, and hydraulic pump induce vibration which, if left unchecked, could lead to hazards in form of fluctuation in the hydraulic system or loosening electric connections.

The designed system must still be able to handle fluctuations and pressure surges from the hydraulic systems. As ZH control is directly manipulating flow for individual hydraulic actuators, the fluctuations at times can be rather high and sudden pressure spikes can emerge [27].

During normal operation, while holding the load, the drift or creep in hydraulic system must not pose a hazard [26]. This could be included in the hydraulic design or the lowering control device might be implemented. ISO 8643 [28] was composed specifically for the lowering device limitations and tests. The criteria for the design is that when lowering, raising, or holding position, the allowed vertical drop should be less than 100 mm in duration of 10 s. The other specification is that if there is internal leakage, the vertical drop is required be less than 10 mm in 1 second.

Another important safety measure can be noticed under fault conditions [26]. If the complete machine, or individual actuator becomes de-energized, it must be possible to safely lower the affected part down. Once lowered, the residual pressure must be able to be released, from the hydraulic system and accumulators.

3.3 ELECTRIC MOTOR AND MOTOR DRIVE SELECTION

When selecting the electric motor utilized to drive the pump in ZH there are many factors to considered. The manufacturer in charge of creating the control systems for ZH must consider mainly between synchronous or asynchronous motors. The team designing the size and compactness of the complete actuator must also investigate the EMC and safety requirements. At least these requirements must be considered in the designing process [9] [12]:

- The type of the motor
- Duty cycle
- Maximum acceleration and load conditions
- Maximum overshoot
- Motors speed operation range, (for variable speeds, alternative cooling method)
- Environmental requisitions for IP classes and degradation in extreme conditions
- Resistance for external electromagnetic interference
- Mechanical vibration limits
- Motor control type, (with rotation speed or current)
- Effects of alternating waveform of voltage or current from adjustable speed drive to temperature rise
- Effects of variating counter-torque
- Effects of large inertia loads on the motor
- Effects of constant power and torque operations on the motor
- Requirements for inductive reactors between motor and electronic adjustable speed drive
- The desired behavior under fault conditions: control system, power source, or other relevant system failures

Alternative protection methods for motors should be designed. They include overheating, as well as overspeed in addition to over voltage, and current protection [19]. All these protection methods must be designed either in case of complete machine de-energize or individual path to individual actuator. The de-energization can also depend on the desired sequence for power loss. It must be thought out should the machine retain some

power or have the possibility for slower drive control. Also, the possible scenarios of restarting the actuators must be considered to not accidently create another hazard.

In Annex A there is a selection sheet for electric parts of the NRMM which should be applied when designing the complete structure for ZH in this application case. This should be used to select the possible frequency converter as well as individual safety functions.

3.4 RECHARGEABLE ENERGY STORAGE SYSTEM

The improvements in the RESS technology is one of the reasons why hybrid and fully electric NRMM are considered as viable options and can compete with conventional machines. The improvement in battery chemistries, especially with lithium, has managed to produce higher power and energy densities suitable for NRMM. The increase in production size for lithium-ion batteries has also been large driver in lowering the €/kWh price, that decreases the payback times for the machines.

Secondary battery should be implemented in NRMM to provide power for control and safety functions. This acts as a protection method in case of main battery failure or shutdown, as many safety functions require power to work. This is also common practice in modern electric vehicles, as if only the lower voltage is present in the operator cabin, the electric systems are not required to follow extra strict requirements.

The high voltage, high power RESS can be said to be one of the most dangerous components if not handled properly. The current safety requirements for NRMMs RESS are not highly specified so it is recommended for designers to look into the electrically propelled road vehicle standards, for example ISO 6469-1 [29], which was created precisely for this application. The closest relevant standard from NRMM for the power source is ISO 14990 and the requirements from there include [16] [12]:

- Disconnection device for each on-board power source,
    - that responds to engine key switch and engine stop feature
    - and in proximity of the RESS mains a switch, relay, plug, connector, or similar device, that is safe to remove, without exposing service person to live circuits.

The ISO 6469-1 [29] goes into more detail concerning the requirements for safe implementation of the RESS. At times, the safety information is rather self-explanatory. The general safety requirements include to not use the machine if the RESS has signs of leakage, spew flames, or has evidence of rupture.

Usually the RESSs are provided by other manufacturers and therefore, the designer can trust that the safety measures are applied and can worry more regarding the physical constraints. Few important ones are listed below [29]:

- RESS must possess protection class minimum of IPX7
- RESS must include protection against short-circuit either by being able to withstand the short-circuit currents (I^2t) or with additional over current protection devices.
- RESS must include overcharge and overdischarge protection

For installation of the RESS, especially in case of NRMM, the height requirement should be followed [29]. In vehicle case for machines over 3,5 ton if the RESS is installed higher than 0,7 m, from the ground to bottom of RESS, it is deemed to be safe in a vehicle crash situation. For external fire hazard protection, the RESS should be located higher than 1,5 m. As the machine in question is less than the required weight limit, external protective cases should be considered.

The level of available energy that can be used has to be taken into consideration when deciding the battery management system (BMS) [21]. If sized too small, the voltage bus might have fluctuations, that depending on the utilized control system, might create hazards.

Similarly, as with RESS the inherent safety measures used in charging should be left for the manufacturers. The designer should still be aware of the methods applied and know to ask for them. The main decision left for the NRMMs designer is to decide if the machine has an internal or external charger. The benefit of internal is that the charging does not depend on charge stations, but internal increases the complexity and costs of the machine. Both chargers are mostly developed by other companies and have their own safety requirements and standards.

Both charging methods are still connected to an external charger or voltage source. ISO 17409:2015 [30] states the safety requirements:

- The charger must be connected to the electrical chassis of the machine through the protective conductor
- Or connection to exposed conductive parts of the vehicles power supply, while the exposed parts themselves are connected to the electrical chassis, thus fulfilling the requirements for protective conductive connection
- The overall resistance of the protective conductor must be less than 0.1 Ω.

- If connected to external power, source the machines ability to move must be restricted [21]
- Risk assessment should be conducted for external electrical charging and take into account machine, electrical burn, and thermal hazards [12]

When also designing the insulation measurement system, it should be taken into account that external chargers can possess their own similar measurement system, and in many cases interference might be occurring between the two [30].

The manufacturer of the NRMM should follow the same rules and requirements posed by the high voltage system in both cases, but especially in the case of internal charger. The latter poses new EMC hazards that must be taken into consideration in form of insulation between other power electronics or control signals.

3.5 RISK MANAGEMENT WITH FUNDAMENTAL PROTECTION METHODS

Few fundamental faults, such unexpected startup and an emergency stop function, have their own standards to assess them. This section goes into detail regarding these faults and their prevention methods.

3.5.1 PREVENTION OF UNEXPECTED STARTUP

The unexpected startup is one of the most hazardous situations possible for NRMM with both electrified and conventional powertrains. The standards provide requisitions for power supply, stored energy, and external influence startups. Unexpected startup can occur from multiple sources. For example, if the hydraulic systems have residual pressure and the safety valves are released, the machine can start moving without commands. Or the electric systems might be under a fault, thus giving a command to the system to move even when it is supposed not to. For these reasons, it is one of the faults that are required to be defined in its own standard ISO 14118 [31].

ISO 14118 [31] lists few possible alternatives on prevention of unexpected startup mentioned, but the main solutions are isolation or energy dissipation. The isolation can be applied on multiple levels, but the main method is by control switches directly on power sources or actuators. The main concept is to be able to completely stop the power from actuating hazardous faults, by disconnection. With dissipation, the energy contained by hydraulic accumulators, electric capacitors, or mechanical movement is dissipated prior to the machine being restarted and the stored energy causing actuation. Both isolation or dissipation are possible to realize with either manual or automatic methods if proper functional safety requirements are followed. IEC 60204-1 [19] explains in more detail the electric and ISO 4413 [27] hydraulic protection methods. Other protection methods are demonstrated in Figure 10 found in ISO 14118.

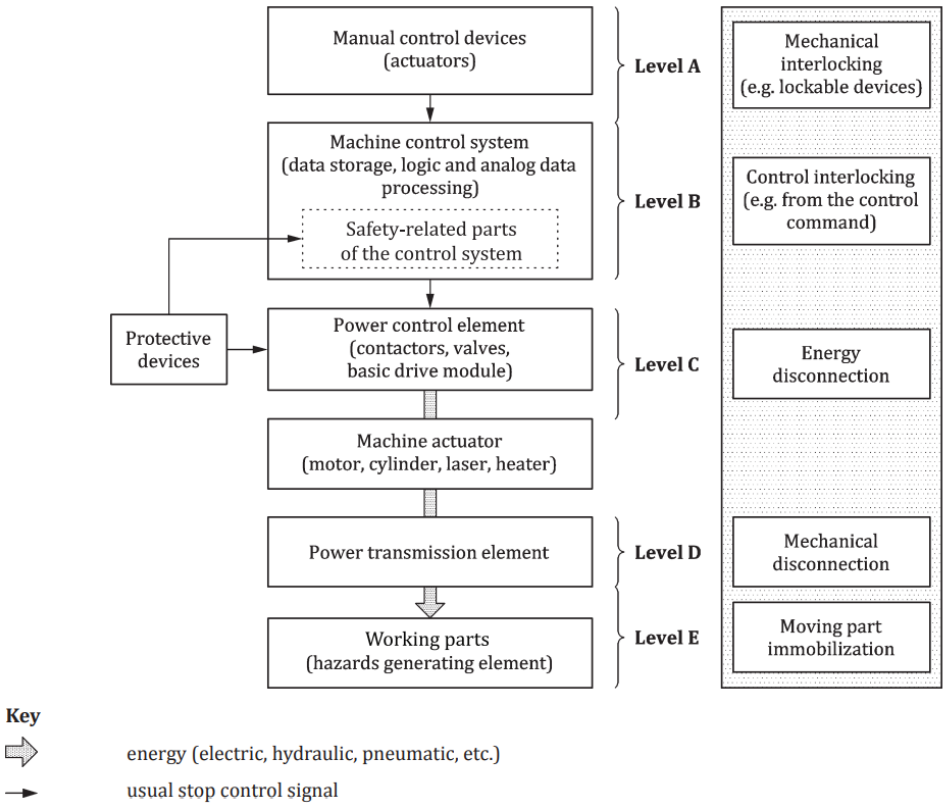


Figure 10. *Alternative methods in place of isolation and energy dissipation for preventing unintended startup [31]*

Figure 10 provides names, and example for individual protection methods that are placed in machine to prevent the self-actuation. One simple method for protection is left out from the figure which is providing audible or visible warning from the operated machine in startup to let the people around the machine know there is possible risk for self-actuation [31].

In all cases, when the method is chosen as a prevention for the fault, the ISO 12100 risk assessment standard as well as ISO 13849-1 functional safety standard should be followed. The ISO 12100, further explained in chapter 3.6, is a type A standard that provides conceptual information on the risk assessment to be applied when designing a machine, actuator, or action. ISO 13849-1 is a functional safety standard for all systems, for example electric, hydraulic, and mechanical that provides methods for assessing and creating safety systems.

3.5.2 EMERGENCY STOP

Emergency stop is complementary protective device and a method to avoid already occurred or about to occur emergency that was caused by unexpected hazardous event or

actions of persons. Similarly as in previous chapter the emergency function has its own dedicated standard, ISO 13850 [32].

Emergency stops are used in industry, mobile machines, and other strict environments. When assessing the necessity of the safety function the designer must evaluate whether the stop function could cause additional hazards for the system. For the complexity of the function it was decided that the emergency stop can have two levels of functionality [32]:

- **Category 0:** instantaneous removal of power from the machine or from the actuators.
- **Category 1:** Driving the machine actuators and operations to stop, followed by immediate removal of power.

There are still factors shared by the two categories. Firstly, the operator must be able to initiate the emergency stop function by a single action [19]. This allows the response to hazards be more immediate. Another requirement is that the function must be available and operational at all given times. The function can override all other functions expect the other protective functions in all operating modes. Moreover, subsequent to the actuation the state must be maintained until manually stopped by operator, and the restarting can only permit the start of the machine, not to restart the machine [32]. The differences in design of electric, IEC 60204-1, and hydraulic, ISO 4413, actuator can be found in the corresponding standards. The emergency stop warning label can be viewed Figure 11.

Figure 11. *Emergency stop symbol, IEC 60417-5638 [32]*

Emergency stop function designed to be implemented alongside ZH in electrified NRMM, should follow the category 1. Machines that have multiple heavy movable parts have possibility of someone ending up being between the machine and hard surface, it should be possible to move the weight off the person in question when the machine is shutting

down. It should prove to be helpful that the shutdown path for the machine can be predetermined by the design team, and there is no definite requisition for the actuation, expect that the safety level should be of c, which is explained in more detail in the next chapter, section 3.6.4 ISO 13849 [32].

3.6 FUNCTIONAL SAFETY

Electrification is known to create more complex systems not only for the actuators but for the control systems required for them. Implementation of ZH is not an exception, rather confirmation of the rule. Especially since the system is a combination of electric and hydraulic parts and is to be installed in mobile machinery that usually has strict rules and regulations surrounding them.

The safety is still something for designers to strive for rather than avoid with their design. The benefits of well operating machine outweigh the difficulty of assessing the safety design. And there are many methods provided from multiple standards for reducing the risk of hazard within operations.

If an inherently safe machine cannot be created or area of operation for NRMM where the possibility for risk cannot be neglected, functional safety evaluation is the correct method to move forward with [33]. Functional safety provides, based on safety related parts of control system (SRP/CS), method for decreasing the risk level for the operation of the machine. Standards provide information on the required safety levels for the actuators and functions under evaluation. The explanation of the safety levels differs a bit depending on the standard in question, but the main concept is to gain knowledge of the frequency and possibility of fault occurring during operation that can pose danger to the user and those around the machine.

Usually safety system designers in teams select the most suitable safety standard to start the evaluation process from multiple standards, that exist from both IEC and ISO organizations, that can be applied for the process. This of course complicates the designer's choice as there is overlapping and limited differences between the methods. Therefore, it is important that they possess appropriate knowledge on all the methods and can provide proper reasoning for their chosen method.

It is still important to acknowledge the fact that neither the gained performance level (PL) from ISO 13849, nor the safety integrity level (SIL) from IEC 61508, provide information on absolute safety nor strict risk levels. Instead they offer relative information about the levels of risk reduction provided by the safety functions that are under evaluation or cre-

ation [33]. However, from risk reduction level gained can the inherent risk level be observed. As greater the risk, greater the safety functions ability to respond to it without a fault.

In the next sections the main safety standards and their sub standards are gathered and explained. Also, the most important safety standards for NRMM are selected and utilized in the hazard analysis chapter 4, and safety system design chapter 5. The first standard to be introduced is ISO 12100 which can be categorized as a risk assessment standard.

3.6.1 ISO 12100

ISO 12100 [34] is a special standard in regards that it can be applied together with the chosen functional safety standard to help the process of risk management. It is also one of the harmonized safety standards, that are applied as methods for attaining safety ratings from European government bodies [33]. The term risk and its relation to hazard is important and frequently utilized factor in all safety related standards, therefore it is depicted in Figure 12 below.

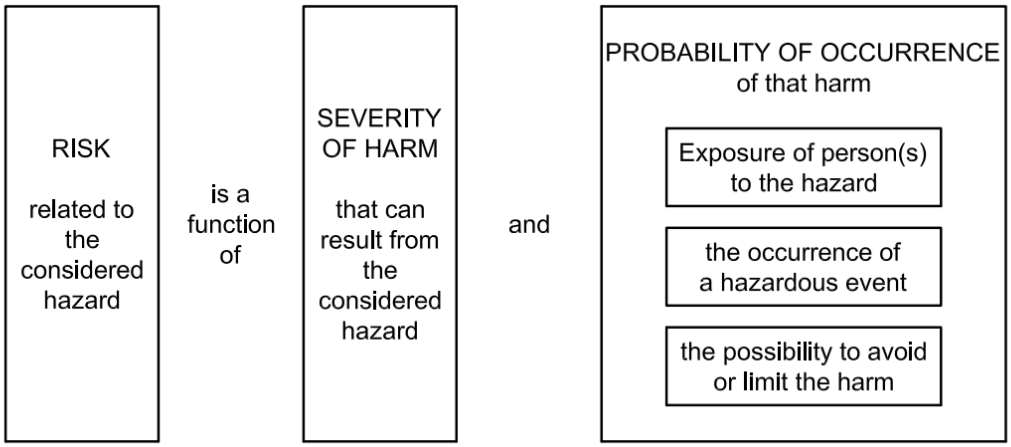


Figure 12. *Definition of risk from ISO 12100 [34]*

Risk is defined as the probability for the hazard to occur, as well as the predecessor for harm. The safety standards do not remove the risk but propose methods to mitigate the hazard.

The ISO 12100 was created to help perform risk assessment for hazard identification. It holds a useful annex that lists large array of possible hazards to help in the evaluation process [33, 34].

It imposes a strategy for safety designers to apply in the risk assessment and risk reduction [34]:

- Select the machinery limits, intended use, and possible misuse
- Identify the hazards and situations that might cause hazards
- Evaluate the risk for each individual hazard and the hazardous situations
- Create risk reduction plan
- Remove the hazard or limit the risk with created protection measures

The introduced process can be examined in Annex B in detail. There are three separate methods proposed for risk reduction [34]:

1. Risk reduction with inherent safety design
2. Risk reduction with added safeguarding's and by implementing added protective measures
3. Or risk reduction with provided information

The method that provides the most safety would be the first, inherent safety of the machine or function. By creating a safety design where the faults don't occur within specified limits allows full range of operation with the machine. The third method, however, can only be as effective as the machine operator.

The standard ISO 12100 [34] then goes into detail regarding the individual steps in assessing the risk related issues. Firstly, the limitations of the machinery are governed from machine, function, person and from a random occurrence point of view. After which, the risk reduction methods are explained. The standard is created for larger complex machines and can be quite tricky for simple systems, where the other specified standards might prove more helpful. However, as it is not limited to only specific type of machinery or function it can prove to be useful in the evaluation of NRMMs when implementing and creating safety systems for ZH.

3.6.2 IEC 61508

Functional safety as a concept was firstly introduced in this standard, IEC 61508 [35]. It is recognized, by other standards and safety designers, as the generic standard for functional safety. It was created by electricians back when the complex control systems were

becoming increasingly more utilized in safety systems [33]. This required the self-evaluation for the applied safety systems as well as to ensure the ability to respond in case of faults and hazardous situation.

The IEC 61058 was strictly created for electric/electrical and electrically programmable safety-related systems. The SIL method provides information on the frequency of possible dangerous failures. The safety levels can be identified from Table 4.

Table 4. *Safety integrity levels – failure rates for proposed safety functions [35]*

Safety integrity level (SIL)	**Low demand mode: Average probability of a dangerous failure on demand of the safety function (PFD_{avg})**	**High demand mode: Average frequency of a dangerous failure of the safety function [h^{-1}] (PFH)**
4	$\geq 10^{-5}\ to\ < 10^{-4}$	$\geq 10^{-9}\ to\ < 10^{-8}$
3	$\geq 10^{-4}\ to\ < 10^{-3}$	$\geq 10^{-8}\ to\ < 10^{-7}$
2	$\geq 10^{-3}\ to\ < 10^{-2}$	$\geq 10^{-7}\ to\ < 10^{-6}$
1	$\geq 10^{-2}\ to\ < 10^{-1}$	$\geq 10^{-6}\ to\ < 10^{-5}$

Expressional values of the safety levels are demonstrated in Table 4 can be gained through calculative methods provided by IEC 61508. The safety levels are also applied in other functional safety standards that are specified for electric systems. These general or main functional safety standards are usually utilized as base for more specific safety information standards. As this standard is meant only for electric systems, it might not be the most suitable as complete functional safety standard for ZH.

3.6.3 IEC 62061

To link functional safety and machinery directive, the European harmonized standard IEC 62061 and ISO 13849 were created. IEC 62061 is a more common derivative of IEC 61508. Both standards are focused on the electrical control systems and use SIL system to define the safety levels [33].

If the electric safety systems are created based on SIL, the methods can be found in this standard. In 2015 project COMPSOFT [36] was finished that investigated the preferred functional safety methods and the differences of results gained from it. The standard in question was applied the second most with 27 % of preference rating from the participants.

IEC 62061 is mainly utilized by designers for complex machinery systems that utilize programmable controllers, PLCs, and fieldbus methods in their safety systems [33]. As well as designers, who create softwares and complex programmable safety systems that prefer to apply methods stated in IEC 61508.

Even though IEC 62061 is dedicated for the electrical safety system, if the manufacturer's utilizing ZH are planning to create every subsystem themselves, it can be applied as part of the complete safety process. In Figure 13 the relations between IEC 62061 and other functional safety standards can be observed.

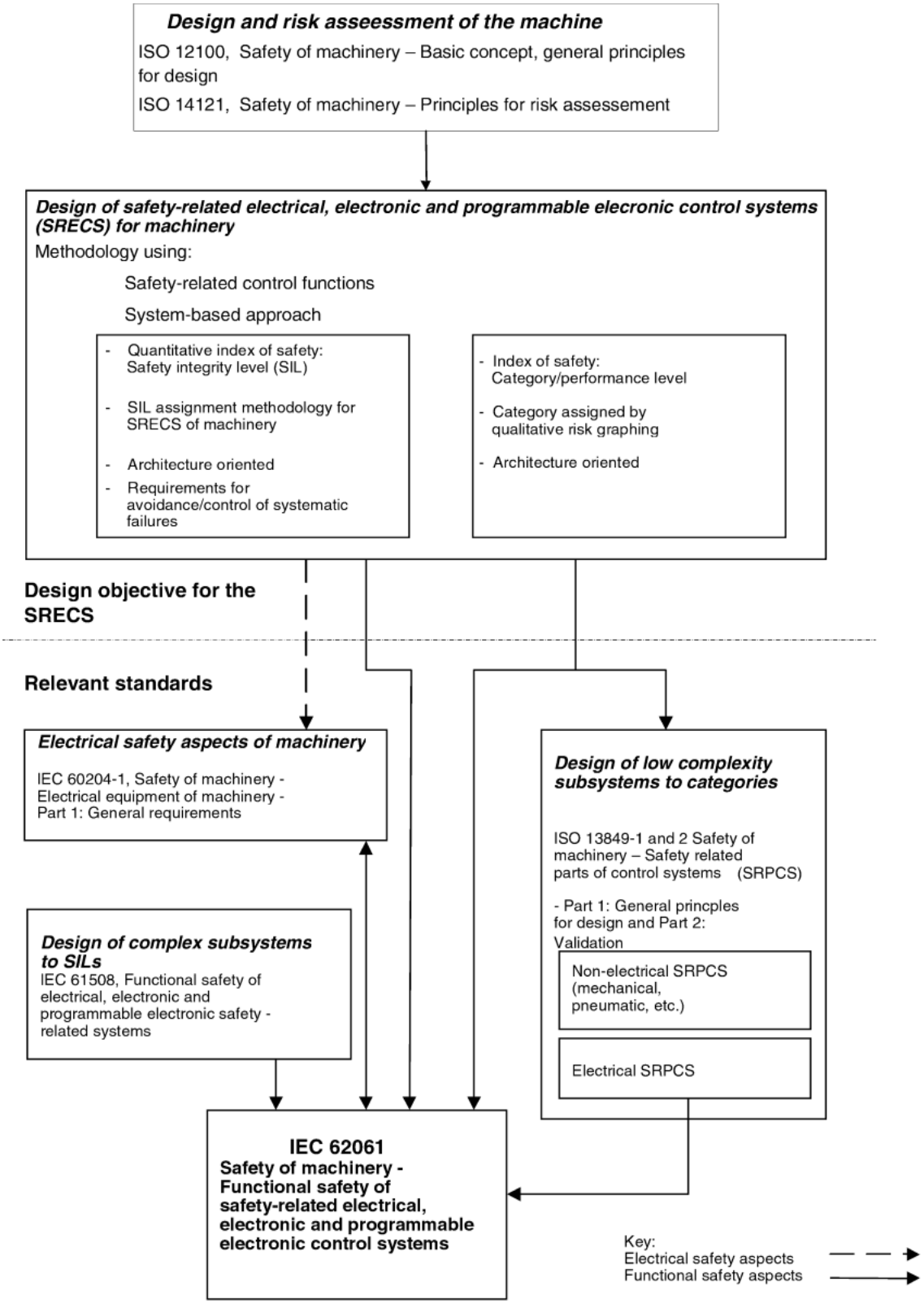


Figure 13. *IEC 62061s relation to other functional safety standards [37]*

IEC 62061 is divided into six main categories in assessing the specifications for safety-related control functions [37]:

- Functional safety management
- Requirements for specification
- Design and integration
- Specified information to be provided
- Validation
- Modification

The process of assigning SIL can be examined in Figure 14 below. The SRCF stands for safety related control function.

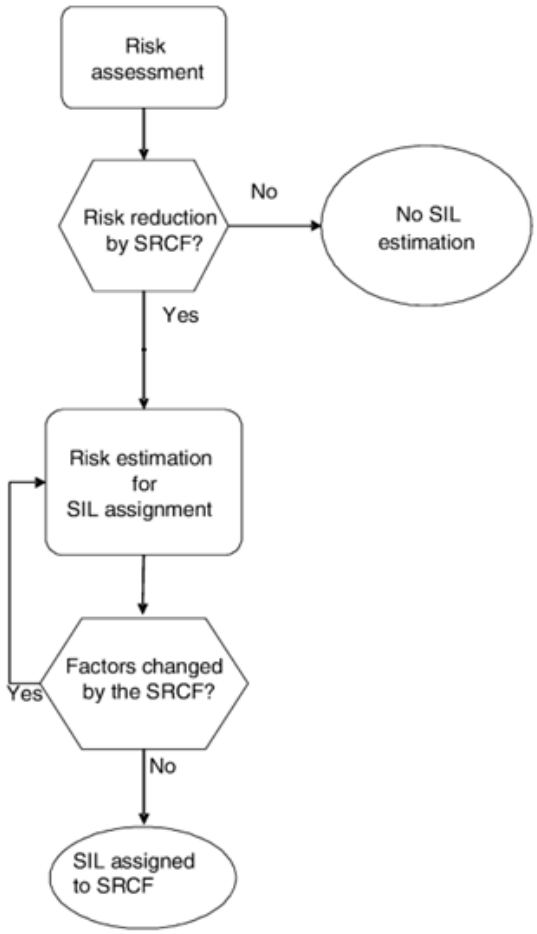


Figure 14. *Workflow for assigning SIL [37]*

The methodology for approaching the necessary safety levels works in similar fashion as in every other functional safety standard. Therefore, for the designer the general methods are easy to follow in all the standards, but the equations to attain the possible

results differ quite a bit. The Finnish standardization organization SFS has created guidance document for the application of IEC 62061 and ISO 13849, SFS 5974 [38]. From the document Table 5 was adapted.

Table 5. *Relation between PL and SIL [38]*

Performance level (PL)	Average probability of a dangerous failure per hour (1/h) (PFH_d)	Safety integrity level (SIL)
a	$\geq 10^{-5} \ldots < 10^{-4}$	-
b	$\geq 3 \cdot 10^{-6} \ldots < 10^{-5}$	1
c	$\geq 10^{-6} \ldots < 3 \cdot 10^{-6}$	1
d	$\geq 10^{-7} \ldots < 10^{-6}$	2
e	$\geq 10^{-8} \ldots < 10^{-7}$	3

Table 5 demonstrates clear relation between the results gained from the two main functional safety standards. Therefore, it is up to the designer to choose between the harmonized standards [39].

As this standard is still mainly focused on completely electrical and programmable electric methods, it is not the most suitable method for ZH.

3.6.4 ISO 13849

The most commonly utilized functional safety standard is ISO 13849. From the study mentioned in the earlier chapter, the amount of safety experts that preferred to apply this standard amounted to roughly 69 % [36]. The reason for this is that ISO 13849 is designed for more simplified systems, and for all systems not only electric [33]. The standard includes guidance on not only the electric, but also on the mechanical, hydraulic, pneumatic and other [40].

The most suitable safety standards were deemed to be ISO 19014 and ISO 13849 for the adaptability of the standards. The ISO 19014 is the sub-standard of ISO 13849, which applies the same methods and equations but is more specified for EMMs. In future when ISO 19014 is completely created it will include its own methods for specification of the safety system but currently only holds methods for assessing the requirements. Therefore, it is important for the safety designer to also learn to implement the methods from ISO 13489. Other important aspect is that for ZH conceptual safety design, the methods used should be kept as simple as possible, as it can be implemented in various applications including stationary and mobile.

ISO 13849 employs same risk assessment methods and methodologies as ISO 12100. Therefore, risk reduction process from ISO 12100 is an important tool and a logical process to follow and can be examined in Annex B. It is in fact so important, that ISO 13849 developed it a bit further to demonstrate which part of the process is the appropriate safety function to implement. In the latter method is depicted in Annex C.

The ISO 13849 begins, subsequent to deciding the safety method, with iterative process of determining the requisitions and levels. Figure 15 introduces the process.

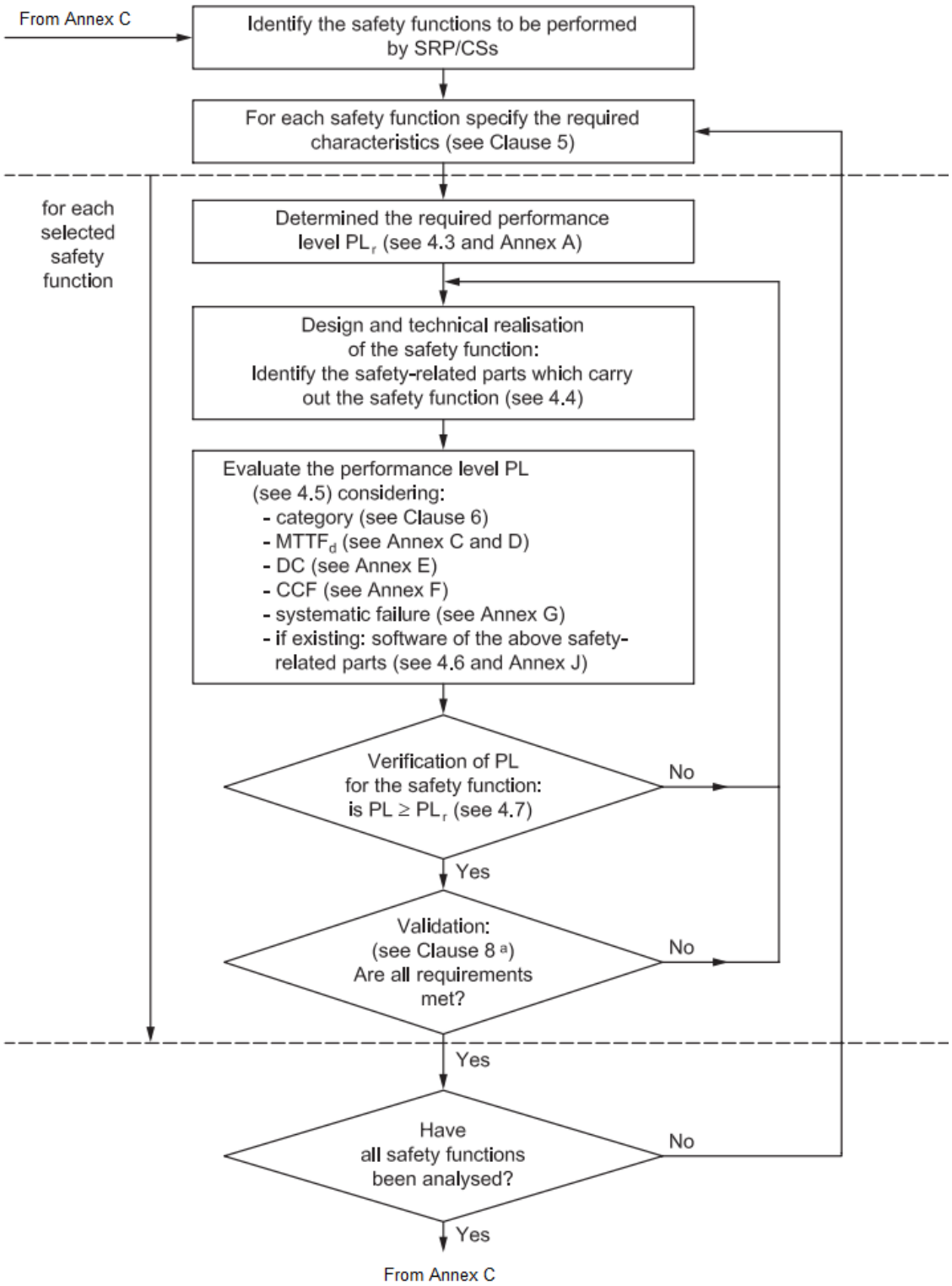


Figure 15. *Design process for safety-related parts of control systems (SRP/CS) [40]*

The approach for the ISO 13849 to move towards functional safety consists of six steps [33]:

- Risk assessment and evaluation of the proposed safety functions
- Analyzing the required performance levels for all safety functions
- Identifying the combination of all safety related parts which respond to the safety function
- Evaluation for the category that is applied in the safety related parts, assessing the mean time to dangerous failure ($MTTF_d$) for individual components, the diagnostic coverage (DC) and common cause failures
- Verification for the achieved PL of the safety related part of the control system (SRP/CS)
- Validation

SRP/CS mentioned is either a part of the safety function or the main method of achieving the safety output. It can be from any technology and actuated in any method possible. This is the main benefit in comparison of the earlier IEC 62061, as the safety functions design is completely left for the designer. The basic function of the SRP/CS is rather simple. According to [40], it consists of:

- Input (SRP/CS_a)
- Logic or processing element (SRP/CS_b)
- Output or power control elements (SRP/CS_c)
- And interconnections (i_{ab}, i_{bc})

The representation can be viewed in Figure 16.

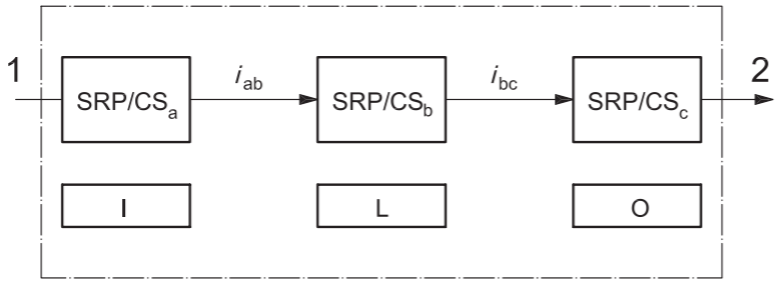


Figure 16. *Typical SRP/CS as safety function representation [40]*

The typical representation can be applied in the designing process for the functional safety. The design still holds multiple other parts that must be solved. As the designer

starts the process of assessing PL for the SRP/CS, the following aspects must be gained first [40]:

- The mean time to dangerous fault, $MTTF_d$
- The diagnostic coverage
- The common cause failure (CCF)
- The structure

The $MTTF_d$ is a method of providing information on how frequently individual component is expected to break in complete systems. It is divided into three levels: low, medium and high. The lowest provides values from 3 to 10 years, while highest represents from 30 to 100 years between failures. The relation between $MTTF_d$ and PFH_d is

$$PFH_d = \frac{1}{MTTF_d \cdot 8760} \qquad 1,$$

where, the PFH_d is measured in faults per hour while the $MTTF_d$ is in years [40].

The diagnostic coverage provides information on the ability to detect faults within the system itself, or a ratio between detected faults and dangerous failures [33]. It is divided into four categories, from no coverage to high coverage. The values differ from the lowest less than 60 % coverage to highest up to 99 % [40].

The CCF is a method for checking the created control system for basic design faults. It can be found in ISO 13849 [40] and is usually performed for the complete SRP/CS.

SRP/CS, depending on the required performance level, has few separate architectures to choose from. Architectures represent the designated level of safety attainted through either proven and well-tried components or possibly with constant monitoring inside the logic circuit. The safety design categories are: B, 1, 2, 3, and 4. The B represents lowest requirement and 4 highest [33, 40].

Category B represented in Figure 17, that at maximum represents PL b, shall be designed and constructed according to relevant standards and utilize either basic or well-tested safety principles. It must provide safety in expected operations and from environmental stress, such as mechanical vibration, electromagnetic interference or power supply fluctuations. The category has no diagnostic coverage, and the $MTTF_d$ shall be either low or medium. CCF is not relevant in this category.

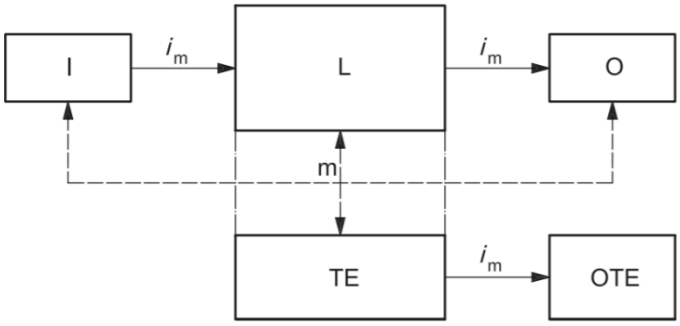
Key

i_m	interconnecting means
I	input device, e.g. sensor
L	logic
O	output device, e.g. main contactor

Figure 17. *Basic architecture for category B and 1 [40]*

The same architecture as before, can also is applicable for category 1 as it also does not include diagnostic coverage. The main difference between the two categories is that the category 1 must be designed to employ well tried methods, components, and safety principles while category B can be novel. The maximum achievable PL is c [40].

For the next category the all previous requirements apply, but there is a new element introduced. It is required from category 2 that the safety functions monitored and tested at decided intervals, by the machine control system. The check-up can be performed when the machine is started, prior to any possible hazardous actuation or periodically. If fault is detected, either the safe state is initiated (PL = d) or proper warning and possibility for the safe state actuation is provided (PL = c). The DC value shall be at least low and $MTTF_d$ depends on the wanted PL. The is representative of category 2. [40]



Key

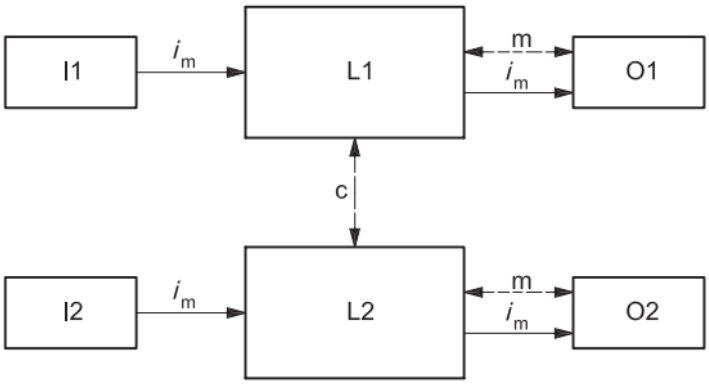
i_m	interconnecting means
I	input device, e.g. sensor
L	logic
m	monitoring
O	output device, e.g. main contactor
TE	test equipment
OTE	output of TE

Dashed lines represent reasonably practicable fault detection.

Figure 18. *Basic architecture for category 2 [40]*

Category 3 is the first of the introduced categories that can retain the possibility to respond to safety hazard even under single fault case. This is achieved through redundant

system architecture where two or more similar functions are copied to achieve the necessary output under the mentioned single fault. The category's basic structure is demonstrated in Figure 19.



Key

i_m	interconnecting means
c	cross monitoring
I1, I2	input device, e.g. sensor
L1, L2	logic
m	monitoring
O1, O_2	output device, e.g. main contactor

Dashed lines represent reasonably practicable fault detection.

Figure 19. *Basic architecture for category 3 [40]*

The final SRP/CS category in ISO 13849 is the fourth one. In similar fashion as with B and 1 the main difference between the 3 and 4 category is that latter utilizes higher DC and $MTTF_d$ values for higher PL. As now the highest attainable PL is e [40]. Category 4 system is categorized by its ability of continued performance in the presence of single fault, an ability to detect and to stop faults that might affect the safety function. The system is capable of taking multiple faults into consideration.

As all necessary functions have been considered, the simplified evaluation of PL can be formed. The relation between all the previously mentioned is demonstrated in Table 6.

Table 6. *Process for evaluating PL for SRP/CS [40]*

Category		**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC_{avg}		None	None	Low	Medium	Low	Medium	high
$MTTF_d$								
	Low	a	Not covered	a	b	b	c	Not covered
	Medium	b	Not covered	b	c	c	d	Not covered
	High	Not covered	c	c	d	d	d	e

ISO 13849 proves to be suitable tool to design the required safety systems, until ISO 19014 standard gets released. ISO 13849 also holds information on how to assess the required PL, but as the earlier mentioned ISO 19014 is the newest and most aimed for micro-excavator case equip with ZH, it is deemed to be the most suitable. Next section goes through the basic information on the standard as the hazard analysis chapter provides example case on the assessing process.

3.6.5 ISO 19014

ISO 19014 [41] is one of the functional safety standards which can be used to define necessary performance level for the analyzed function or actuator. This standard is created especially for safety evaluation of EMMs, and therefore is included in this thesis.

The standards for functional safety define safety control systems (SCS) in a way which could lead the designer to think of external protection methods. The standard [41] has a list of possible SCSs for EMMs. This list consists of variety of methods such as braking, steering, individual implements, propulsion, hazard mitigation systems, and more. The SCS can be either inherent to the design of actuator or also completely external protection method.

The standard defines all necessary terms and methods for determining machine performance level required (MPLr), which helps the system designers to plan either inherently safe actuator or the additional protection methods described in ISO 12100. The standard does not explain further how to create the system to match the required safety levels. In future, when the complete series for ISO 19014 is released, the methods will be published as well. Currently the best method for safety system designer for EMM is to apply ISO 19014 standard for the evaluation of the required safety level and then the ISO 13849 for the design.

The most important parts for the evaluation of MPLr are:

- Exposure
- Severity
- And controllability

Exposure is one of the values that is required to calculate the MPLr for the specific SCS. It represents the estimation of how exposed the risk group in question is to a hazard, which could lead to injury. The equation is according to [41],

$$E = A \cdot H \cdot P \quad , \quad 2$$

where the A is the application case, H is the hazard time, and P is the person group exposure. The exposure in ISO 19014 is in three levels which are represented in Table 7.

Table 7. *Exposure levels [41]*

E0	E1	E2
$E < 1\ \%$	$1\ \% < E < 10\ \%$	$E \geq 10\ \%$

Application case informs the efficiency of the analyzed task. More simply put, from 0 % to 100 % how much the machine or function is being utilized during that task. For normal digging actuation it usually is 90 %.

Accordingly to [41], hazard time is calculated for the person group under evaluation. While (2) is simplification of the exposure, when performing hazard analysis, the evaluation is typically performed for specific person group, for example an operator or a bystander. The equation for hazard time for the specific person group is,

$$H_{\text{Person Group}} = H_{\text{Stage}} \cdot (100\% - t_{\text{idle}}) \quad \text{[41]}, \quad 3$$

where the H_{Stage} states the amount of time in the work cycle the hazard is present and t_{idle} the percentage of the cycle that the machine cannot operate. Example how to calculate hazard times defined in ISO 19014 can be examined in chapter 4 table 12.

Next in the evaluation process for MPLr is severity. To ensure that the highest level of safety is achieved, the severity of fault should be assumed to be as high as possible. The severity levels and their examples are depicted in Table 8.

Table 8. *Severity levels and examples of injuries [41]*

S0	S1	S2	S3
Least dangerous scenario and requires at most first aid	Injuries might be inflicted that require medical attention. No loss in work capacity as total recovery is expected.	Severe injury inflicted that will afflict a permanent loss in work capacity.	The most severe case, fatality of the person in question.

The severity levels are estimations of the possible damage the fault could cause to the recipient. They are divided to four levels from least (S0) to highest (S3). They range from first aid, medical attention, permanent loss in work capacity, and death.

Final factor for MPLr is controllability. Controllability is one of the aspects that requires analyzing for the hazard in question to achieve the MPLr. Similarly, as well as exposure also controllability consists of multiple factors, but while E is defined with (2), C is defined with the matrix, demonstrated in Table 9 below. The factors are: alternative control, ability to react, awareness of hazard, and controllability.

Table 9. *Classification of controllability [41]*

		AR0	**AR1**	**AR2**	**AR3**
AC0		C3	C3	C3	C3
AC1	**AW0**	C3	C3	C3	C3
	AW1	C3	C3	C3	C2
	AW2	C3	C3	C2	C1
	AW3	C3	C2	C1	C0

In Table 9 alternative control (AC) is defined as a completely alternative path for control in case of a hazardous situation. It has only two levels, AC0 and AC1, which respectively state that there are either no possible controls or 1 or more alternative controls.

Awareness of hazard (AW) is divided to four levels as demonstrated in Table 9. AW3 is the highest level of awareness and means the action is known prior it has even occurred. Example for this would be seeing low levels of fuel in the gauge system, and later the vehicle engine dying for the lack of fuel. AW2 is medium level of awareness, which

means that when the function occurs, the operator immediately notices it. AW1 means the operator might notice the action occurring and AW0 means that the operator has no knowledge of the hazard occurring.

Ability to react (AR) in Table 9, states the level of control the operator has over the fault. AR3 means that operator can naturally react to fault and has already hands or feet on the alternative control methods. AR2 is rather similar, but in this case, operator must move arms or feet to another control method but can still do so instinctively. AR1 demands for unnatural response from the operator but is still possible to avoid the hazard. And AR0 refers to situation where operator is unable to respond in time even though there might be alternative control system in place.

By using the selected AC, AW, and AR values, the controllability factor can be gained from Table 9. Controllability has four levels, from lowest (C3 – no controllability) to the highest (C0 – high controllability).

After the exposure, severity, and controllability has been selected and estimated, the MPLr can be solved from Figure 20 below.

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

Figure 20. *MPLr matrix [41]*

Through hazard analysis the factors S, E, and C can be gained, and the corresponding requirement level can be achieved. The safety levels are demonstrated in Table 10.

Table 10. *Performance level with corresponding dangerous failure [40]*

Average probability of a dangerous failure per hour (1/h)	**Performance level (PL)**	**Safety requirement**
$\geq 10^{-5}$ ... $< 10^{-4}$	a	lowest
$\geq 3 \cdot 10^{-6}$ ... $< 10^{-5}$	b	
$\geq 10^{-6}$ ... $< 3 \cdot 10^{-6}$	c	
$\geq 10^{-7}$ ... $< 10^{-6}$	d	
$\geq 10^{-8}$ ... $< 10^{-7}$	e	Highest

These safety levels Table 10 are the same as in ISO 13849. Therefore, as currently ISO 19014 has yet to release part 4, the SCS can be designed using tools and requirements found in the ISO 13849. At this stage, it is even possible to apply any other safety standard for example IEC 62061, to design the electric control if the designer chooses.

3.6.6 SUMMARY

In this chapter the main functional standards were gathered and explained. The proposed and harmonized standards were,

- ISO 12100
- IEC 62061
- ISO 13849

The selected standards for this thesis were ISO 13849 and the sub-standard derived from it, ISO 19014. These are applied in the chapters 4 and 5, where ISO 19014 is utilized to analyze the required safety level for ZH and ISO 13849 to investigate how the requirements are defined for the system.

The next chapter is meant to provide insight how to implement the methods found in these standards and how to perform machine control system safety analysis (MCSSA) or also known hazard analysis from ISO 19014. The hazard analysis is performed for six actuation faults to ensure most of the hazardous situations are covered.

4. HAZARD ANALYSIS FOR MICRO-EXCAVATOR CASE

Hazard analysis is part of a functional safety process for safety control systems (SCS), where various operational cycles are analyzed, and the machine performance level required (MPLr) is gained. In this thesis the safety system analyzed is the EHA, and the functional safety method is applied from ISO 19014 [41]. The analysis was performed on the movement of a single actuator. This is the normal process in hazard analysis as even single fault is rare in most cases, and therefore two faults occurring at the same time is not considered. This chapter explains methods of assessing required safety levels for micro excavator based on the ISO 19014. Firstly, the work scenarios and specific safety factors are explained.

4.1 MICRO-EXCAVATOR MISSION HOURS

The first step in functional safety is to define the mission hours for one year. The study case selected is electrified JCB 8008 cts 1-tonne micro excavator. The machine can be operated in confined spaces where additional risks are involved and must be analyzed.

The annual work mission hours must be analyzed with help of experts. Typical large-scale excavator has roughly 10 000 h of operation or 6 years, which means around 1700 h per year [42] and 1000 hours a year for operation was recommended for micro excavator [43]. The results can be examined in Table 11.

Table 11. *Micro-excavator work mission hours/year*

Operation	hour/year	% of total time
Digging/grading	520	40
Truck loading	390	30
Idling	195	15
Travelling	130	10
Being loaded for transport	65	5
Total	1300	100

From Table 11 can be observed that the machine is operative for 1300 h per year. This was a rough estimate on machine's life cycle.

4.2 THE DIGGING CYCLE

To analyze required MPLr for actuators the cycle must be selected. The reason for this is to help with the visualization and assessment process for hazardous situations. The selected cycle was created based on Japanese digging cycle (JCMA07). The only difference between Japanese and created digging cycles is the fact that micro-excavator will consider possibility of being operated in confined spaces. The machine operated in confined spaces is demonstrated in Figure 21.

Figure 21. *JCB 8008 cts micro-excavator (from JCB website)*

The modified Japanese digging cycle is presented in Figure 22, where it has been in the operational sections. The operational sections are:

A. Conventional digging cycle where only boom arm and bucket are controlled
B. Moving the arm sideways for unloading and dumping the bucket
C. Returning the arm to initial position.

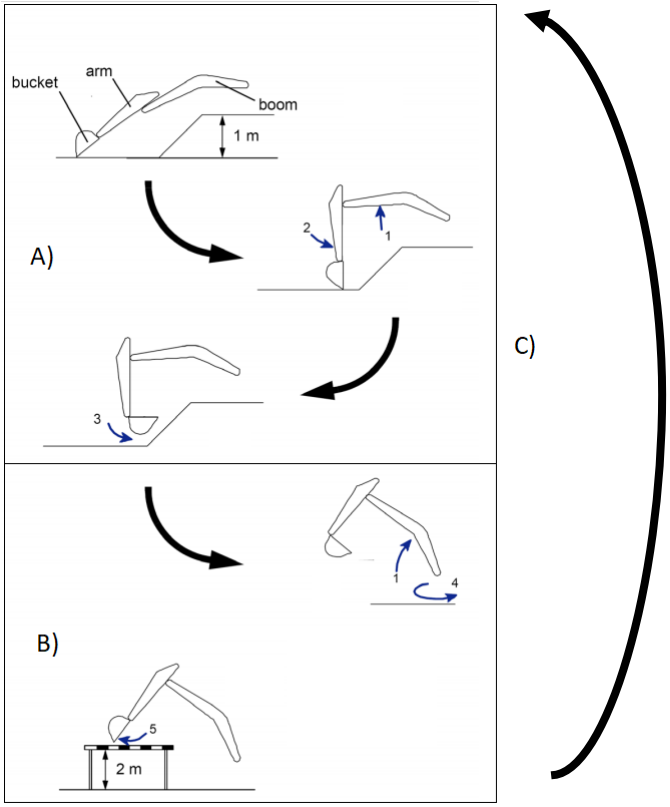


Figure 22. *Modified Japanese excavator digging cycle (JCMA07) utilized in hazard analysis [44]*

The digging cycle was modified to involve confined spaces to represent the most hazardous situation for operator. It was divided into three operational cycles to help the assessment process in hazard analysis. As was observed from Figure 21 this type of excavator does not require cabin to protect the driver. Therefore, under right fault conditions, there is possibility of the arm to hit walls or rafters, thus creating hazardous condition if something were to fall over the operator. For coworkers, it is assumed that there should not be naturally occurring hazardous situations as all personnel should stay clear of operated machines. There are still operations that could prove to be hazardous even while taking precautions. In the machine control system safety analysis (MCSSA), found in the next section, these hazardous situations are considered and analyzed.

4.3 HAZARD ANALYSIS FOR UNCOMMANDED ACTUATION

This section includes MCSSA for the specific failure type that is performed for actuators in micro-excavator. In this section the process is presented step by step but later in the other fault conditions mainly the results are listed. The first failure type is uncommanded actuation demonstrated in 4.3.1. This means that from stopped position, one of the actuators starts moving, creating possible hazards for operator and those around him. The

sections subsequent to that are divided for arm, bucket, rotation, swing, and traction respectively.

4.3.1 BOOM'S UNCOMMANDED ACTUATION

The first step is to determine the hazardous outcome of the failure. The first case scenario is when the boom's actuator starts moving either up or down, from stationary position. Possible outcomes, for:

- Operator: possible hard jerk motion when machine hits ground or ceiling in tight spaces, possible hazard of objects falling from rafters over the operator
- Coworker: Ending up being hit with the lowering machine arm.

Then the severity is defined from Table 8,

- For operator S1, Minor jolt
- For coworker S3, loss of life

The analysis applies values that remain the same throughout the hazard analysis. These are application use case and person group exposure. Application use case for digging cycle is defined in the standard ISO 19014, Annex C [41], to be *A* = 90 %. It meant that machine is operational and performing the digging operations 90% of the cycle. The rest is for waiting or evaluation of work process. Person group exposure is also estimated for the digging cycle, therefore, is not dependent on the failure or actuator position. The following assumptions are applied,

- for the operator $P_{\mathrm{Operator}} = 100\ \%$ (always present in excavator)
- and for coworker $P_{\mathrm{Coworker}} = 5\ \%$ (should not be near excavator except in special situations).

Hazard time is defined for both, operator and coworker cases. The results can be examined from Table 12 and Table 13 below. The percentages are estimations of how long the hazard is present during the movement.

Table 12. *Operators exposure to hazard expressed as a % of time: boom, uncommanded actuation*

Stage of Work Cycle (from diagram in Figure 22)	**Time (%)**	**Percentage of Stage Hazard Present (%)**	H_{stage} **= Time (%) x (percentage of stage Hazard present)**
A	50 %	$66\,\% \cdot 50\% \cdot 20\,\% = \mathbf{6,6}\,\%$	$50\,\% \cdot 6{,}6\,\% = \mathbf{3,3}\,\%$
B	25 %	$33\,\% \cdot 50\,\% = \mathbf{16,5}\,\%$	$25\,\% \cdot 16{,}5\,\% = \mathbf{4,125}\,\%$
C	25 %	$80\,\% \cdot 50\,\% = \mathbf{40}\,\%$	$25\,\% \cdot 40\,\% = \mathbf{10}\,\%$
		total	**17,425**%

From the left-most column in Table 12, the individual parts of the cycle can be identified. The hazards in this first case are the possibility for the arm to hit ceiling and causing something to drop on top of the operator, dropping down to ground causing sudden jolt, and dropping down the arm when it is moving sideways. The next column then informs the percentage of how long the machine stays in that corresponding part of the cycle. Second column from right then gives estimation on how long the hazard is present in that specific part of the cycle. The right-most column in Table 12 demonstrates the information for how long the hazard is present during the complete cycle.

For the cycle part A, the hazard is present for $\mathbf{6,6}\,\%$. This was estimated for the possibility of fault causing dangers in only one direction. The hazard is only present if loose material is present in the rafters of the confined work area. In cycle part B, the hazard is present only when moving the machine sideways and if the arm was to drop down. In the cycle part C, the situation is the same but now as it is not used for dumping the hazard is present longer.

Then the (3) is applied and idle time taken into consideration. The idle time was estimated to be 10 %. The idle time was gained when taking the machine size and tight operation spaces into consideration. The operator requires time to become familiar with the safe working premises and how to move within those limits. The H_{Operator} is then calculated to be $16{,}68\,\%$.

The same estimations were then performed for the coworker's case. Table 13 was formed of these results.

Table 13. *Coworkers exposure to hazard expressed as a % of time: boom, uncommanded actuation*

Stage of Work Cycle (from diagram in Figure 22)	**Time (%)**	**Percentage of Stage Hazard Present (%)**	**H_{stage} = Time (%) x (percentage of stage Hazard present)**
A	50 %	**5** %	$50\,\% \cdot 5\% = \mathbf{2,5}\,\%$
B	25 %	**0** %	**0** %
C	25 %	**0** %	**0** %
		total	**2,5** %

Similarly, as with the boom the cycle is divided, and estimations are given. In part A, the hazardous scenario is: if the coworker is examining something in the dug hole and the machine arm was to drop down. In parts B and C there is no hazard present as there should never be personnel under the moving arm, especially when moved sideways. In part A, it is estimated that hazard is only present for 5 %, as from complete operational cycle the amount of time coworker is under the arm is very low. The total H_{stage} was then calculated and (3) was applied to attain the hazard time for coworker, with the result of $H_{\text{Coworker}} = 2{,}25\%$.

The percentage of exposure was then calculated by applying (2) from section 3.6.5. The equation applies the application use case, hazard times for operator and coworker, as well as person group exposure values that were calculated and estimated earlier in Tables 12 and 13. Using the Table 7 the exposure values can be gained. The values are,

- $E_{\text{Operator}} = A \cdot H_{\text{Operator}} \cdot P_{\text{Operator}} = 90\,\% \cdot 16{,}68\,\% \cdot 100\,\% = 15\,\%$, E2
- $E_{\text{Coworker}} = A \cdot H_{\text{Co-worker}} \cdot P_{\text{Coworker}} = 90\,\% \cdot 2{,}25\,\% \cdot 5\,\% = 0{,}11\,\%$, E0

The factors needed to estimate the controllability function (Table 9) are AC, AW, AR. The resulting values can be viewed from Table 14.

Table 14. *Controllability factors: boom, for uncommanded actuation*

	Alternative control	**Awareness of Hazard**	**Ability to react**
Operator	AC1	AW2	AR2
Coworker			AR3

The alternative control was selected to be AC1 as the operator can try to lessen the impact using either swing or arm movement even if the boom actuator loses control. The awareness of hazard is AW2, as the operator notices immediately if the boom were to move without command. For ability to react AR2 was selected for operator as the operator cannot avoid hitting the ground or ceiling, only to lessen impact. But for coworker, the operator can try to use other parts of the machine, such as swing to avoid hitting

them. With the selected values from Table 14, the controllability factor can be achieved by following the corresponding paths from Table 9. And they are,

- $C_{\text{Operator}} = C2$, low controllability
- $C_{\text{Co-worker}} = C1$, medium controllability

Controllability, severity, and exposure levels are then applied to select the required performance level from Figure 20. By following the corresponding lines, the MPLr can be gained from the matrix in Figure 20.

- $(S1, E2, C2) \rightarrow MPLr_{\text{Operator}} = \text{b}$
- $(S3, E0, C1) \rightarrow MPLr_{\text{Coworker}} = \text{a}$

The gained MPLr values represent the safety level that the designed system must achieve. In practice this value is then applied when the SCS is designed with the help of ISO 13849. The higher value b provides information how frequently dangerous fault can occur. Table 10 demonstrate the average probability for dangerous fault occurring is around $\geq 3 \cdot 10^{-6}$ ... $< 10^{-5}$ per hour, or once per 11 to 38 years.

The complete process from this section is then applied to arm, bucket, swing, rotational movement and traction actuators respectively. The process is also applied for other faults such as uncommanded actuation, undesired deactivation, unexpected failure of activation and unexpected failure to deactivate.

4.3.2 ARM'S UNCOMMANDED ACTUATION

When performing hazard analysis, one should start with the most dangerous hazards to ensure high enough MPLr is achieved but should still check all actuator cases to ensure that no higher level of requirements is involved. In the micro-excavator case, the larger movements such as the movement of the boom, are deemed more dangerous.

Now as the failure is occurring on the arm, some of the factors are different. The mass falling is lower and movement range shorter. Nevertheless, the failure still creates a hazardous situation, but for another area. The results are demonstrated below.

Similarly, as earlierly the S, E, AC, AW, AR, C, and MPLr variables are chosen and estimated, and then added to Table 15.

Table 15. *MCSSA, arm, uncommanded actuation results*

	Hazard time	S	E	AC	AW	AR	C	MPLr
Arm, operator	16,68 %	S1	E2	AC1	AW2	AR2	C2	b
Arm, coworker	1,125 %	S3	E0	AC1	AW2	AR3	C1	a

Because the main difference between boom and arm actuation is the lesser hazard time, the MPLr's is the same. The highest required performance level is b.

4.3.3 BUCKET'S UNCOMMANDED ACTUATION

Bucket actuator poses the least danger in comparison of arm and boom as its movement is the most limited. If the bucket would become actuated while coworker is stuck under the arm, the movement would most likely not hit the person. However, in the case of operator it is still possible that the bucket might hit the roof and drop something over the driver if the arm would be positioned high enough. Table 16 demonstrates the analyzed MPLr results.

Table 16. *MCSSA, bucket, uncommanded actuation results*

	Hazard time	S	E	AC	AW	AR	C	MPLr
Bucket operator	0,9 %	S1	E0	AC1	AW2	AR3	C1	QM
Bucket coworker	0,45 %	S1	E0	AC1	AW2	AR3	C1	QM

Table 16 illustrates the results of calculations in similar manner as in boom actuator's case. The bucket failure poses little to no risk because of the limited movement range, and therefore lower possibilities of collision. The coworker can only be hit with the bucket if standing directly under it. This differs heavily from the earlier cases as the range is noticeably limited. For the operator, the only possible risk scenario is if the bucket were to push something down from the rafters. However, even then, the operator can control boom, or arm to lower it enough to avoid impact. The results gained are defined as Quality Measure (QM). In practice it means no extra safety measures are to be taken, only by following the quality measured posed by standards until the actuation reaches the safety levels necessary.

4.3.4 ROTATION OF THE CABIN, UNCOMMANDED ACTUATION

As the sideways movement poses completely new possible hazards and is inherently different to vertical movement of the boom and arm, similar complete analysis is performed for the rotation of the cabin (in larger machines called swing). For the swing movement only, the results are gathered in the corresponding Table 20.

The hazardous outcomes for cabins rotation are:

- Cabin starts to rotate in either of the two directions, from stationary position.
- Operator: Possible collision with either of the walls in tight confined spaces or losing balance in the sudden jerk motion
- Coworker: Impact with the arm of the excavator

The severities are of the same level as in the boom case. The sudden movement or stop poses mainly discomfort for the operator, but the worst-case scenario for coworker could be loss of life. The hazard time analysis was performed for operator and coworker in Tables 17 and 18.

Table 17. *Operators exposure to hazard expressed as a % of time: rotation of the cabin, uncommanded actuation*

Stage of Work Cycle	**Time (%)**	**Percentage of Stage Hazard Present (%)**	H_{stage} **= Time (%) x (percentage of stage Hazard present)**
A	50 %	$20\,\% \cdot 30\,\% = \mathbf{6}\,\%$	$50\,\% \cdot 6\,\% = \mathbf{3}\,\%$
B	25 %	$50\,\% \cdot 20\,\% = 10\,\%$	$25\,\% \cdot 10\,\% = \mathbf{2,5}\,\%$
C	25 %	$0\,\%$	$\mathbf{0}\,\%$
		total	$\mathbf{5,5}\,\%$

Now in part A and B, the most hazardous scenario is hitting the wall with the machine arm. As the fault activates the sideways rotational movement suddenly is mostly dangerous if the machine is located close to walls, the arm is lifted high enough. The only difference between the cycles is that the B has the hazard present when dumping the load. In part C, the rotational movement is constantly used so hazard cannot materialize.

Compared to previous results, in sections 4.3.1, 4.3.2, and 4.3.3, the H_{stage} is more limited as the machine is constantly in motion. The H_{Operator} is solved by using (3) and the result is $4{,}95\,\%$. For the coworker the results can be observed below in Table 18.

Table 18. *Coworkers exposure to hazard expressed as a % of time, rotation of the cabin, uncommanded actuation*

Stage of Work Cycle	**Time (%)**	**Percentage of Stage Hazard Present (%)**	$\boldsymbol{H_{\text{stage}}}$ **= Time (%) x (percentage of stage Hazard present)**
A	50 %	$5\,\% \cdot 50\,\% = 2{,}5\%$	$50\,\% \cdot 2{,}5\,\% = \mathbf{1{,}25}\,\%$
B	25 %	$50\,\% \cdot 50\,\% \cdot 20\,\% = 5\,\%$	$25\,\% \cdot 5\,\% = \mathbf{1{,}25}\,\%$
C	25 %	$0\,\%$	$\mathbf{0}\,\%$
		total	$\mathbf{2{,}5}\,\%$

The most hazardous situations present are is in part A if the coworker is standing next to the arm while examining something in the dug whole and in part B if the person stands too close of the dumping pile and with sudden movement something from the bucket would hit him. In part C, the bucket has no load and coworker is assumed to not stand next to moving arm.

Now with the (3), the H_{Coworker} is solved to be $2{,}25\,\%$. The exposure can be solved with application time, hazard time and person group exposure similarly as in previous sections. Using Table 7 the exposure can be gained. For operator and coworker, they are respectively, E1 and E0. Next the controllability factors AC, AW, and AR are defined in Table 19.

Table 19. *Controllability factors, rotation of cabin, for uncommanded actuation*

	Alternative control	**Awareness of Hazard**	**Ability to react**
Operator	AC1	AW2	AR3
Coworker			AR2

Similarly, as previously the operator can immediately notice the faulty movement and react to it by lowering arm down. This removes the possibility of harm for the operator but in rare cases where coworker would be standing too close the operator might not be able to react in time.

By following the corresponding paths from matrix in Table 9, the controllability factors were solved to be,

- $C_{\text{Operator}} = \text{C1}$, medium controllability
- $C_{\text{Co-worker}} = \text{C2}$, low controllability

Subsequent to gaining controllability factor, the severity, and exposure are applied to solve MPLr from Figure 20,

- $(S1, E1, C1) \rightarrow MPLr_{\text{Operator}} = QM$

- $(S3, E0, C2) \rightarrow MPLr_{\text{Coworker}} = b$

Next section is for the swing movement. The movement is, similarly to bucket, inherently safer compared to rotational movement as it has limited range. Therefore, only the main results are provided.

4.3.5 SWING OF THE BOOM, UNCOMMANDED ACTUATION

This actuator can be noticed from Figure 21 at the base of the boom. The movement is like the rotation of the cabin, but with much more limited movement range. From Table 20 below the results of hazard analysis can be checked.

Table 20. *MCSSA, swing of the boom, uncommanded actuation results*

	Hazard time	**S**	**E**	**AC**	**AW**	**AR**	**C**	**MPLr**
Swing, operator	2,7 %	S1	E1	AC1	AW2	AR3	C1	QM
Swing, coworker	1,35 %	S3	E0	AC1	AW2	AR3	C1	a

Table 20 demonstrates that the highest requirement gained for actuators with swing in this case is *a.* For operator the requirements only are quality measures in the design.

4.3.6 TRACTION'S UNCOMMANDED ACTUATION

Traction includes one of the most important and dangerous actuators. The uncommanded movement is one of the issues that is well covered in standards as moving machinery can pose dangerous hazards for people around the machine. Even though standards include requirements for the movement, it is still important to evaluate the dangers posed by this movement.

The hazardous outcomes in this case for operator is collision with objects and for coworkers being run over. The severities are defined as S2 for operator and S3 for coworker. The hazard times are defined below in tables Table 21 and Table 22.

Table 21. *Operators exposure to hazard expressed as a % of time: Traction, uncommanded actuation*

Stage of Work Cycle	Time (%)	Percentage of Stage Hazard Present (%)	H_{stage} = Time (%) x (percentage of stage Hazard present)
A	50 %	$50\,\% \cdot 20\,\% = \mathbf{10}\,\%$,	$50\,\% \cdot 10\,\% = \mathbf{5}\,\%$
B	25 %	$50\,\% \cdot 20\,\% = \mathbf{10}\,\%$,	$25\,\% \cdot 10\,\% = \mathbf{2,5}\,\%$
C	25 %	$50\,\% \cdot 20\,\% = \mathbf{10}\,\%$,	$25\,\% \cdot 10\,\% = \mathbf{2,5}\,\%$
		total	$\mathbf{10}\,\%$

Hazard that is caused by malfunction in traction affects all parts of the cycle. In all parts, if the machine suddenly starts to move, especially in in tight spaces there is risks for hitting walls or objects. The same percentage was used for all parts of the cycles and were justified with the tight spaces and if the walls or objects were in close vicinity. The hazard time for operator was calculated with (3). The H_{Operator} is $9\,\%$ and therefore exposure is E1. Table 22 includes the same calculations but for coworker case.

Table 22. *Coworkers exposure to hazard expressed as a % of time: Traction, uncommanded actuation*

Stage of Work Cycle	Time (%)	Percentage of Stage Hazard Present (%)	H_{stage} = Time (%) x (percentage of stage Hazard present)
A	50 %	$50\,\% \cdot 5\,\% = \mathbf{2,5}\,\%$,	$50\,\% \cdot 2{,}5\,\% = \mathbf{1,25}\,\%$
B	25 %	$50\,\% \cdot 10\,\% = \mathbf{5}\,\%$,	$25\,\% \cdot 5\,\% = \mathbf{1,25}\,\%$
C	25 %	$50\,\% \cdot 10\,\% = \mathbf{5}\,\%$,	$25\,\% \cdot 5\,\% = \mathbf{1,25}\,\%$
		total	$\mathbf{3,75}\,\%$

In case A, the hazard was present if the coworker were examining something in the dug hole and the machine started suddenly moving forward. For the parts B and C of the cycle the hazard was mainly present if the coworker were to stand behind the machine and operator could not see him. $H_{\mathrm{Co-worker}}$ is calculated to be *3,375 %* and exposure E0. Controllability factors AR, AW and AR are presented in Table 23.

Table 23. *Controllability factors, boom, for uncommanded actuation*

	Alternative control	Awareness of Hazard	Ability to react
Operator	AC1	AW2	AR3
Coworker			AR0

The individual factors differed compared to the previous cases. Now if the machine starts to suddenly move it will be noticed immediately and it can be slowed down by lowering boom. But if in cycle part A, the coworker was in front of the machine, this would not be

possible as it would just create new hazard if the operator were to suddenly lower down the arm.

The controllability factors are calculated to be,

- $C_{Operator} = C1$, medium controllability
- $C_{Co-worker} = C3$, no controllability

by using Table 9. The MPLr is gained with Figure 20,

- $(S2, E1, C1) \rightarrow MPLr_{\text{Operator}} = a$
- $(S3, E0, C3) \rightarrow MPLr_{\text{Coworker}} = c$

The highest MPLr from this failure was *c*, in traction. Usually traction is designed to include other methods for stopping or keeping the machine stopped during work cycle. These extra methods lessen the safety requirements for the actuator itself.

4.4 HAZARD ANALYSIS FOR UNDESIRED DEACTIVATION

This failure represents situation, where either by fault or de-energization subsequent to the fault the actuator is deactivated and depending upon the design moves towards neutral position. Impact can be quite similar in comparison of uncommanded actuation, where the heavy arm drops down with high velocity. Usually there is counter measure in design, that either slows the fall or completely stops it in a faulty condition. Nevertheless, when creating hazard analysis only the movement of the actuator is evaluated, without any possible requirement from standards or from widely known protection methods.

Now similarly as in previous case, in section 4.3.1, for boom the most serious dangers posed to operator came from high velocity impact in confined tight spaces that might cause something to fall over from the rafters. In this case the only possible fault for the driver is the sudden stop of movement that might cause him discomfort or possible strains from falling off the seat. However, in coworker case the dangers posed are almost identical, as even if the motor itself does not increase the force of impact, the weight of boom, arm, bucket plus load is enough to cause irreversible damage. The evaluation of hazard times was concluded in similar way as in previous chapters. The results are included in Table 24.

Table 24. *Actuators case results, undesired deactivation*

	Hazard time	S	E	AC	AW	AR	C	MPLr
Boom operator	$(50 \cdot 0 + 25 \cdot 33 + 25 \cdot 80)\% \cdot 90\% = \mathbf{25,43}\%$	S1	E2	AC1	AW2	AR2	C2	b
Boom coworker	$50\% \cdot 0{,}5\% \cdot 90\% = \mathbf{0,225}\%$	S3	E0	AC1	AW2	AR3	C1	a
Arm operator	$(50 \cdot 0 + 25 \cdot 33 + 25 \cdot 80)\% \cdot 90\% \cdot 66\% = \mathbf{16,78}\%$	S1	E2	AC1	AW2	AR2	C2	b
Arm coworker	$50\% \cdot 2{,}5\% \cdot 90\% = \mathbf{1,125}\%$	S3	E0	AC1	AW2	AR3	C1	a
Bucket operator	$(50 \cdot 1 + 25 \cdot 1 + 25 \cdot 1)\% \cdot 90\% = \mathbf{0,9}\%$	S1	E0	AC1	AW2	AR3	C1	QM
Bucket coworker	$50\% \cdot 1{,}25\% \cdot 90\% = \mathbf{0,56}\%$	S1	E0	AC1	AW2	AR3	C1	QM

The results analyzed provide the same values for MPLr even though hazard time increases for the operator. The reason why the hazard time increases was as prior the movement had two possible directions, either up or down, in this case, the only movement in case of deactivation is downwards. This increased the hazard time in the cases where the arm was moving sideways. However, as in previous cases the hazard time was already over 10 %, which is the upper limit for exposure in Table 7, the class remains the same, level E2.

From Table 24 the rest of the estimations can also be identified. When the swing movements were analyzed, the sideways rotational movement was deemed inherently safe, if there was no possibility for collision. As there is no risk of violent stop by excavator arm hitting ground, or ending up crushed under heavy weights, the actuators utilized in terms of this fault should only be following quality measures.

Similar way of thinking applies for the traction, as the machines are usually designed to be stopped suddenly even without brakes. Therefore, even if the machine is suddenly stopped there should not be any new hazards for either cases.

4.5 HAZARD ANALYSIS FOR UNEXPECTED FAILURE TO ACTIVATE

This section is usually reserved for SCS that are already intentioned to act as a safety measure against hazards or faults. One of these would be braking systems utilized in road vehicles, that are meant to mitigate hazards of impact with objects. Usually the evaluation is also proposed for the brake system to ensure the safety level.

With the micro-excavator case and the work cycle that is being studied, there is no such single movement or actuator that could possess extra risk to people around the machine.

From Figure 21 can be analyzed that in no case, is the machine required to perform movements to lessen or avoid hazards caused by external variables.

4.6 HAZARD ANALYSIS FOR UNEXCPECTED FAILURE TO DE-ACTIVATE

This movement can pose similar hazards as uncommanded actuation or undesired de-activation. However, in the similar manner as in the latter case, this movement is more limited in comparison with the uncommanded movement. This could pose hazards for the operator as well as people around the machine. For this reason, this is a fault that should be investigated.

The hazards that pose the largest threats for the operator is again the machine arm hitting roof in the A part of the cycle for boom. In the movement, that is occurring sideways, the boom does not require activation, and therefore does not create possible hazards in parts B and C. For coworker the most hazardous cases are when there is a possibility of the boom or arm to drop down on them. The earlier cases evaluated situations if the arm were to drop down from stationary position. The fault in question requires the boom to be moving. Therefore, the only possible scenario of this hazard occurring would be if the operator were to lower the boom while the coworker was under it and that is a very unlikely scenario to occur. Table 25 below includes the calculated results for required performance level.

Table 25. *Actuators case results, unexpected failure to deactivate*

	Hazard time	**S**	**E**	**AC**	**AW**	**AR**	**C**	**MPLr**
Boom operator	$(50 \cdot 20 \cdot 33 + 25 \cdot 0 + 25 \cdot 0)\% \cdot 90\% = \mathbf{2,97}\%$	S1	E1	AC1	AW2	AR2	C2	a
Boom coworker	$50\% \cdot 0{,}5\% \cdot 90\% = \mathbf{0,225}\%$	S3	E0	AC1	AW2	AR3	C1	a
Arm operator	$50\% \cdot 20\% \cdot 33\% \cdot 33\% \cdot 90\% = \mathbf{0,98}\%$	S1	E0	AC1	AW2	AR2	C2	QM
Arm coworker	$50\% \cdot 0{,}5\% \cdot 90\% = \mathbf{0,225}\%$	S3	E0	AC1	AW2	AR3	C1	a
Bucket operator	$50\% \cdot 20\% \cdot 33\% \cdot 10\% \cdot 90\% = \mathbf{0,297}\%$	S1	E0	AC1	AW2	AR2	C2	QM
Bucket coworker	$50\% \cdot 0{,}5\% \cdot 10\% \cdot 90\% = \mathbf{0,0225}\%$	S1	E0	AC1	AW2	AR3	C1	QM
Rotation operator	$(25 \cdot 50 \cdot 20 + 25 \cdot 20)\% \cdot 90\% = \mathbf{6,75}\%$	S1	E1	AC1	AW2	AR2	C2	a
Swing operator	$(25 \cdot 50 \cdot 20 + 25 \cdot 20)\% \cdot 90\% \cdot 33\% = \mathbf{2,23}\%$	S1	E1	AC1	AW2	AR3	C1	QM

The analysis for the fault in question was not purposely created for coworker. With unexpected failure to deactivate, the rotation or swing movement should already be occurring in the direction of the risk group. In practice it means that the coworker should be standing next to the moving arm. Not only would this be irresponsible but also highly dangerous, and therefore not considered as proper practice and left out of this analysis. The other movement that is left out of analysis is the traction, as there is no traction movement occurring in this digging cycle and the fault is specified to be failure to deactivate.

4.7 HAZARD ANALYSIS FOR HAZARD ANALYSIS SUMMARY AND RESULTS

This chapter introduced results of the hazard analysis or MCSSA through proposed example scenario of micro-excavator. The results gained from this analysis are the basis for functional safety design that is required for all machines. The results are demonstrated in Table 26.

Table 26. *Collected MPLr results for all actuators and cases*

	Boom	Arm	Bucket	Rotation	Swing	Traction
Uncommanded activation: Operator	b	b	QM	QM	QM	a
Uncommanded activation: Coworker	a	a	QM	b	a	c
Undesired deactivation: Operator	b	b	QM	QM	QM	QM
Undesired deactivation: Coworker	a	a	QM	QM	QM	QM
Unexpected failure to activate: Operator	QM	QM	QM	QM	QM	QM
Unexpected failure to activate: Coworker	QM	QM	QM	QM	QM	QM
Unexpected failure to deactivate: Operator	a	QM	QM	a	QM	QM
Unexpected failure to deactivate: Coworker	a	a	QM	QM	QM	QM

The trend can be clearly seen from the Table 26. The coworker is present for shorter periods of times compared to the operator, and therefore requires lower safety requirements. For operator the average performance level is b which is reasonable as it in theory provides information on the average dangerous fault happening between 11 to 38 years of operation.

The next step is to investigate the requirements from either ISO 13849 or in the future ISO 19014. The standards also provide methods for achieving the safety system design. In the next chapter the basic safety system design is proposed based on the standards and MPLr. Conceptual methods for the evaluation of control systems is presented.

5. CONCEPTUAL SAFETY SYSTEM DESIGN

ZH system consists of individual EHAs as mentioned in section 2.2. This chapter provides information and methods to safely implement individual EHA to micro-excavator. As multiple of these individual actuators can be applied to complete ZH system, the proposed solution can also be applied to rest of the actuators in ZH.

Functional safety and how to approach it have been studied profoundly throughout the years. Example of such study is publication “Patterns for control systems” [45] which was part of J. Rauhamäki’s doctoral thesis [39]. In his work was proposed patterns to help in the development process. However, the initial step is to define the difference between control and safety systems.

Figure 23 presents the structure of EHA. It has been divided in four simplified block diagrams, with the concept of specifying the differences and relations of individual control systems to ease the process of the safety design.

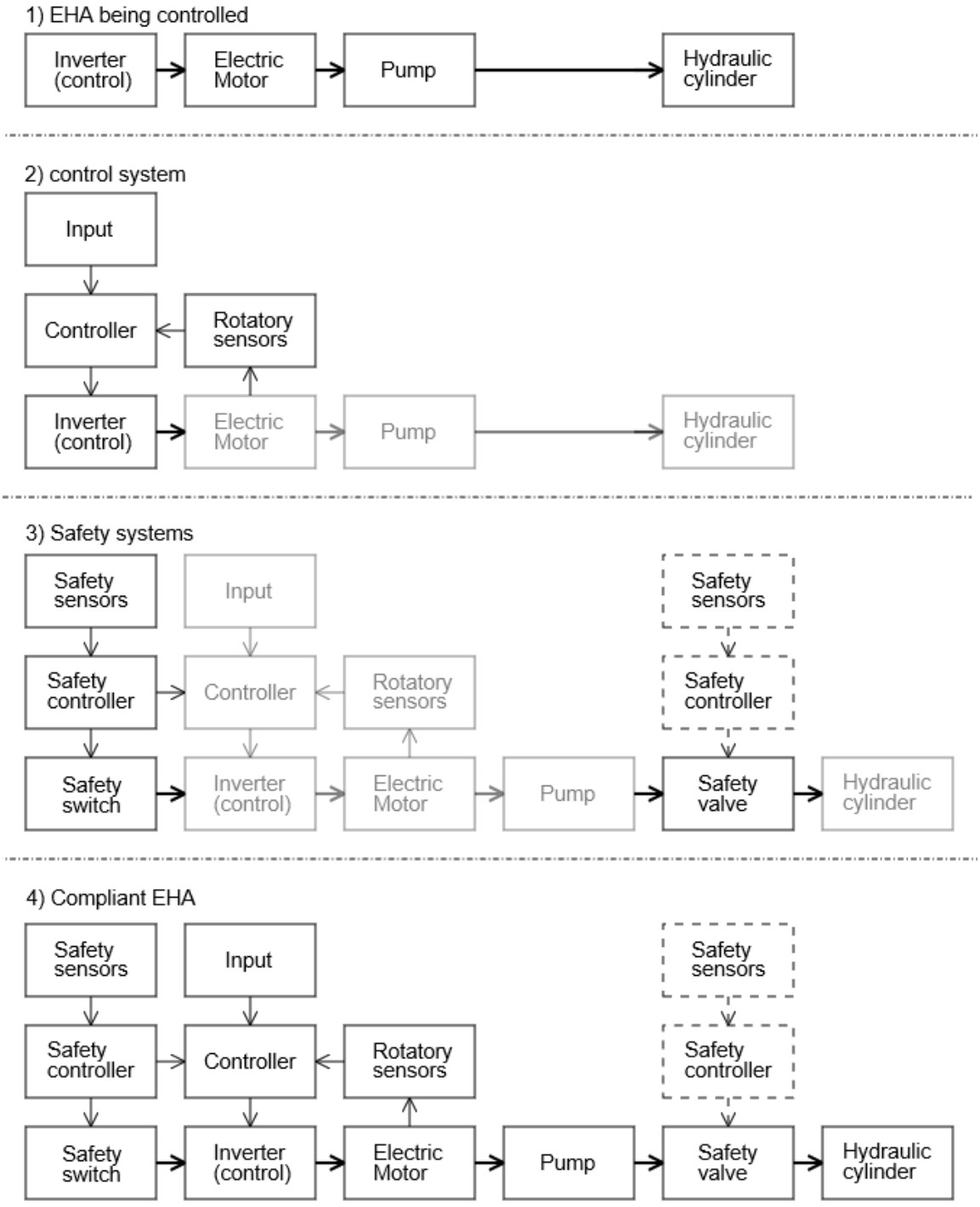


Figure 23. *EHAs control and safety system separation: 1. Simplified EHA, 2. control system, 3. safety systems, 4. compliant EHA structure*

The depiction of simplified EHA can be identified in section 1 of Figure 23. In its purest, it includes inverter, electric motor, pump, and hydraulic cylinder. Section 2 adds the control system for frequency converter, which takes the reference value of rotational speed from the motor and input from the user interface. Section 3 adds the required safety designs, such as the hydraulic safety valve and electric safety switch. The hydraulic control schematic was represented with a dashed line as it is controlled with the same systems as the electric. The electric switch involves either programmable logic controller (PLC) or alternative control systems. And lastly the section 4, demonstrates the compliant EHA structure, which follows the specifications introduced in standards.

The next sections demonstrate methods of implementing such systems within the limitations of standards and the process towards functional safety design can be performed with guidance of ISO 13849.

5.1 SYSTEM DESIGN REQUIREMENTS FROM STANDARDS

To design EHA to be compliant with the standards, it is important to consider all the requisitions for protection found in the multiple sources. These protection methods have been examined throughout the thesis. The important safety methods that are part of the control systems are:

- Over current protection, load, voltage, temperature protection
- High voltage chassis or earth insulation fault respond and monitoring
- Protective conductor continuation monitoring
- EMC challenges
- Emergency pressure relief
- Motor safety controls, i.e. overspeed and over temperature

Overcurrent protection can be achieved with circuit breaker, control system, or a fuse. Designer must decide on the possibility for multiple de-energization zones and isolation points. As an example, will the sensors placed in the input of the motor and the inverter trip the same safety switch in the dc-link or individual safety switches in the EHA for more robust protection system. The design should implement multiple protection methods that have similar outcomes, as that creates a more inherently safe system. It is recommended to implement safety switch in dc-link in the input of the inverter. The main reason is that it is able to respond to the multiple monitored values, such as the insulation, voltage fluctuations and high currents, before the hazard continues towards the actuator.

The hydraulic safety is usually realized with a passive safety valve to enable an immediate response to the fault. It is still possible to include a more complex safety valve that could provide safety in the case of de-energization of main power, or from an emergency switch.

The control system itself is also at times considered as a safety related part. And the control system has multiple requirements found in standards. The control system must be designed to limit the possibility for unexpected start-up. This is possibly realized with a designated sequence of actions by the operator for machine start-up and interlocking. The possibility of failure must be considered, and the machine movement identified in such an event. According to [12] [19], other important safety functions for control systems are:

- Load limitation
- Load lowering in case of fault
- Motor speed monitoring and over speed safety methods
- Fault detection, isolation, and response
- Recovery or protection against malfunction of control system
- Resilience against electromagnetic interference

The main safety control systems that are proposed for ZH are the hydraulic safety valve, electric safety switch and redundant control system for motor drive. In the next section the process is demonstrated for creating conceptual safety system design.

5.2 CREATING THE SAFETY SYSTEM DESIGN

Once the safety systems are decided and required performance levels gained, the next step would be the evaluation of the selected safety system. ISO 13849 as depicted in section 3.6.4, has the main design factors and requirements listed. Mainly the categories and the MTTFd are chosen for the EHA.

From Table 26 the results of hazard analysis can be observed. The highest MPLr is level c. The traction could be created more inherently safe with the added brakes, but to achieve higher overall safety for future implementations, the higher safety level is chosen for the conceptual safety system design. The level c corresponds to average dangerous fault per hour being $\geq 10^{-6}$ ... $< 3 \cdot 10^{-6}$, as examined from Table 10.

Presented in Table 6 are the categories and MTTFr values for performance level c. The factors and options are presented in Table 27.

Table 27. *Possible safety system designs based on ISO 13849 [40]*

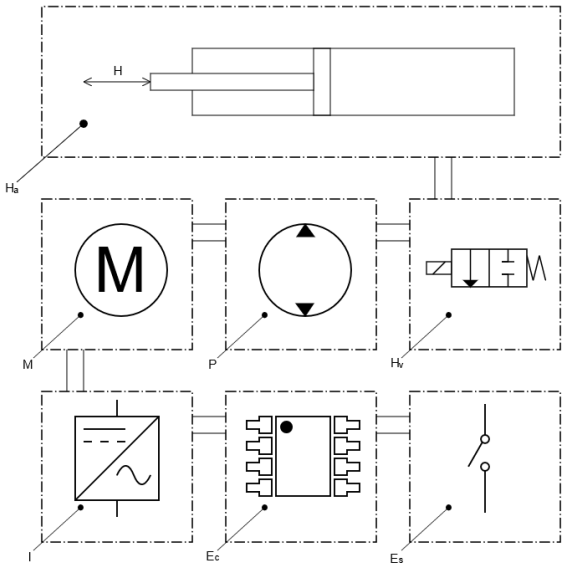
Category	**1**	**2**	**2**	**3**	**3**	**4**
DC_{avg}	None	Low	Medium	Low	Medium	high
$MTTF_d$						
Low = (3 – 10 years)	-	-	-	-	c	Not covered
Medium = (10 – 30 years)	-	-	c	c	d	Not covered
High = (30 – 100 years)	c	c	d	d	d	e

Other important factor to consider is by placing safety functions “parallel” it is possible to increase the safety level and redundancy with lower level safety systems. However, the system in this thesis is designed to be of level c or higher. Therefore, this is meant only for future consideration.

The MTTFd factor, as the name implies, provides information on average failure of the part or the system. The failure rates of the components can be gained from the manufactorers or from ISO 13849. The standard has methods for calculation individual components MTTFd based on the amount of actuations per year. This is an important factor when designing and selecting the correct safety switches and circuit breakers for the design, as it can lower the achiavable safety level. As the component selection is one of the most straightforward methods of increasing reliability, it is recommended to be kept as high as possible. In practise this means using and applying well tried components as stated in the standards.

The diagnostic coverage is difficult to design. ISO 13849 contains annex that will provide estimations of the diagnostic coverage for multiple components and systems. For the safety systems in ZH achieving safety level c, the highest diagnostic coverage value amounts only to low or medium. The low provides diagnostic coverage of 60 – 90 % and medium from 90 to 99 %. For example indirect monitoring by pressure sensor is rated at level medium and monitoring values of the circuitry is low. Therefore, using rather basic safety sensors the DC can achieve medium level. If multiple measurements for fault detection are utilized, the same annex E has an equation to calculate the average value.

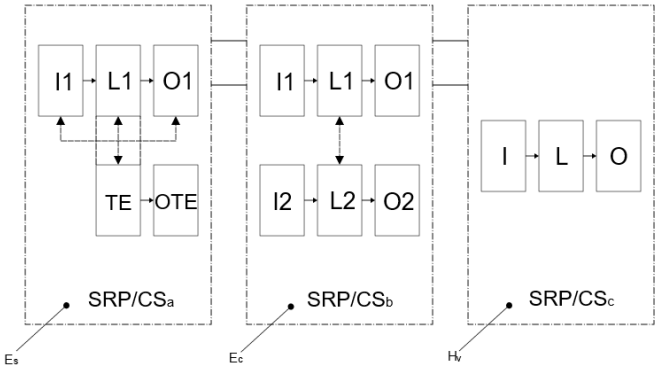
The safety system was illustrated in Figure 24 and it is meant to represent the combination of SRP/CS in EHA. Such system was designed to represent of the safety level c for EHA utilized in ZH.



H Hazardous movement
Ha Hydraulic actuator
Hv Hydraulic relief/safety valve, Category 1, PL=c
P Pump
M Motor
I Inverter
Ec Electronic control for motor drive, Category 3, PL=d
Es Electric safety switch, Category 2, PL=c

Figure 24. *EHAs safety related parts of control systems*

In Figure 24 the safety related parts are hydraulic safety valve (Hv), electric control (Ec), and electric switch (Es). From the pump, motor, and inverter safe design is expected from the manufactorers and should be designed to last as long as the lowest rated safety parts. The chosen performance levels can be examined in Figure 24. The lowest level is chosen to be level c but for the control system it was chosen to be d. This was mainly as the control system is chosen to be reduntand. The safety related parts and their control systems are presented in Figure 25.



Hv	Hydraulic relief/safety valve
Ec	Electronic control for motor drive
Es	Electric safety switch
I, I1, I2	Input devices, e.g. sensors
L, L1, L2	Logic
O, O1, O2, OTE	Output devices, e.g. main contactor
TE	Test equipment

Figure 25. *Selected categories for SRP/CS*

The categories chosen for the safety system can be examined in Figure 25. The definitions for the requirements can be found in section 3.6.4. The categories chosen for the safety systems were as follows:

- Category 1 for hydraulic safety valve
- Category 2 for electric safety switch
- Category 3 for the control system

Category 1, which can be examined in Figure 17, was selected for the hydraulic safety valve. Most systems employ passive relief valve, but the proposed solution prefers an active controlled valve. The safety level that can be achieved with well tried components and methods is also of level c without the requirement of monitoring.

Category 2 represents the electric monitoring and safety switch. The representation in Figure 25 depicts only the single input value, but in practise the required monitoring factors amount to a larger number of sensors. The factors that require monitoring were insulation, voltage fluctuations and drops, the current, and more depending on the design of control systems. The category now requires monitoring and test functions for itself. Depending on the required DC value, testing can be performed manually, or prior to dangerous movements to ensure proper operation in case of a single fault within the safety control system.

For the inverter drive or control system, category 3 was recommended for its inherent redundancy. By partially or wholly duplicating control systems safe operation can be assured for the operator and to people around the machine. Such inherently safe design provides safety even under single fault. In the next chapter the proposed design and combined category for the safety system is depicted.

5.3 PROPOSED SAFETY SYSTEM

The proposed safety system design based on standards is presented in Figure 26. The functionality of the design is to implement a redundant safety system with modern tools for individual EHA utilized in ZH. The safety features are operated by programmable logic controller (PLC) and motor control unit for frequency converter which has an integrated safety functions.

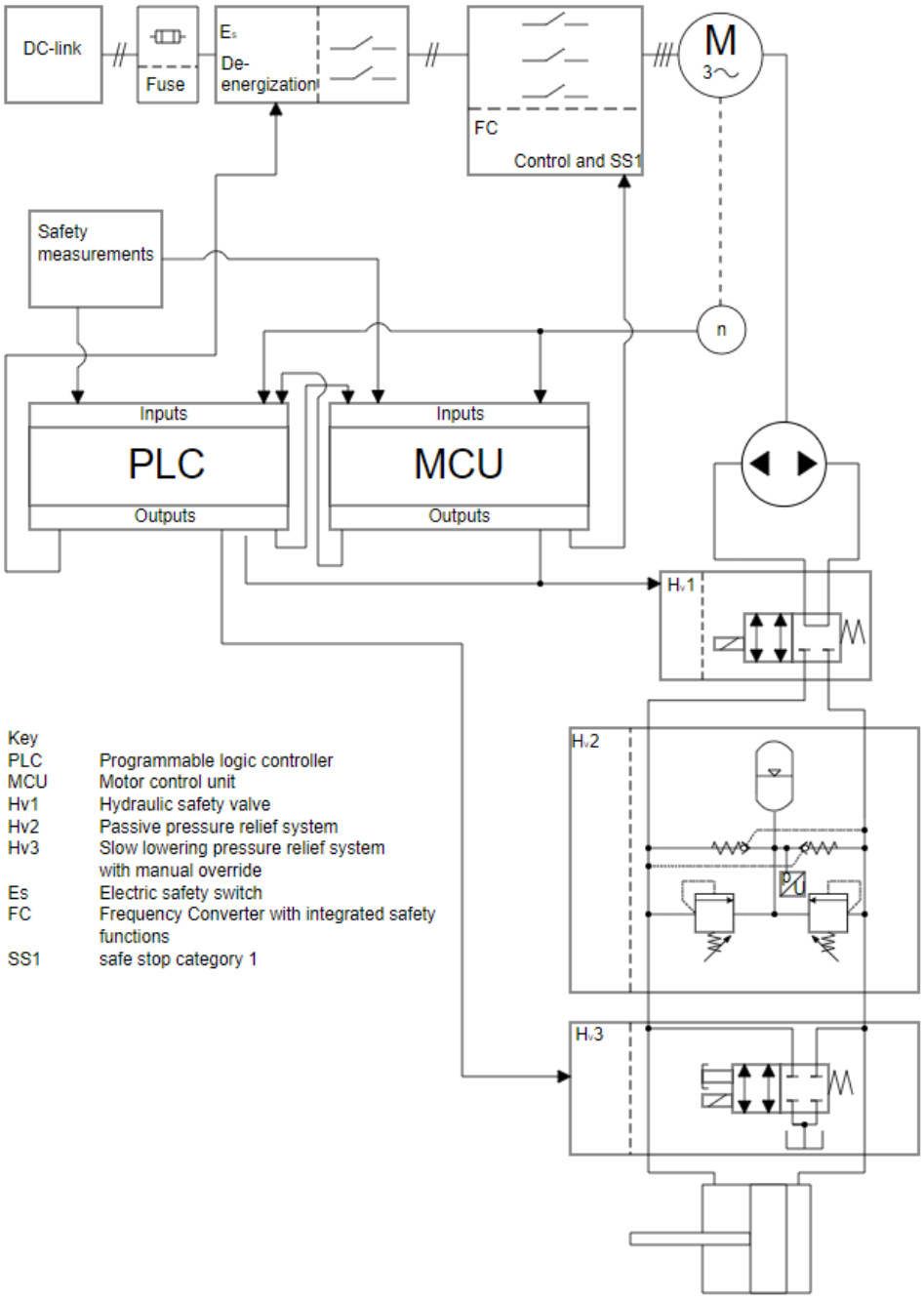


Figure 26. *Proposed safety system design*

The proposed design, from Figure 26, has two pathways to achieve safe state. The frequency converter applies stop category 1 explained in section 3.5.2. It issues a drive command to bring the motor to a stop after which the complete removal of power for the actuator is placed. It will also remove power from the hydraulic stop valve which will lock the hazardous movement in place. The alternative path reacts to more immediate hazards such as the lack of insulation between high voltage and chassis and voltage fluctuations. The PLC issues a command for a safety switch to open relays to cut down the power from DC-link to actuator. The response is immediate, and the motor shuts down abruptly. Therefore, it is necessary for the two safety control systems to have monitoring to ensure that if the inverter detects a fault and is driving the machine down, the PLC does not shut down the power in the middle of the process. After activated, the PLC also gives command, if deemed necessary, for hydraulic safety valve, Hv3, to open which then controllably lowers down any actuator. This is done to avoid any hazards that might be caused if the lifted part of machine were to stay in place.

Additional protection methods were passive relief valves for hydraulic system and an overcurrent fuse for DC-link. The safety lowering device Hv3 was also designed to have manual override in case of the safety measurements activated by Hv1.

Figure 27 represents the combined safety system proposed for EHA. In the figure I1 represents the rotational speed measurements while I2 and I3 represents all other possible input values that might trigger the safety systems. L1 depicts the motor control system while L2 the safety controller. O1 and O3 are the electric safety switches while O2 and O4 the hydraulic safety valves.

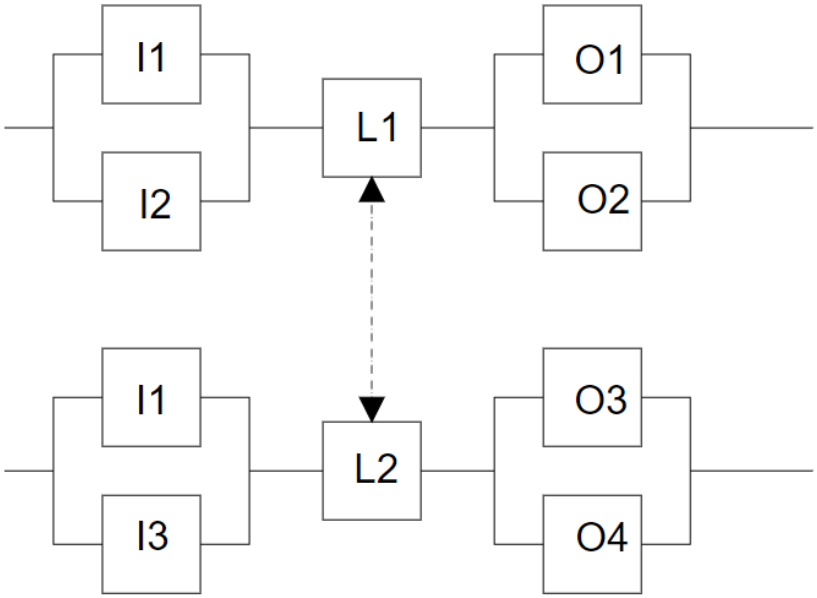


Figure 27. *Combined safety system architecture for EHA*

The proposed safety system provides redundant safety for the individual actuator. This is represented by the two paths linked with monitoring. The proposed complete is category 3. To achieve safety level of c, the diagnostic coverage for the complete system must be between 60% – 90% as can be noticed from Table 27. From the same table the value for average fault in single components is selected to be of 10 to 30 years.

6. DISCUSSION AND CONCLUSION

Safety in the modern NRMM environment is governed by standards and well tried and applied methods and products. Standards are created to ease the innovation process and to provide the same requirements for all machine manufacturers to level the competition. But as the systems and electric parts are becoming more complex and their responses more difficult to predict, the requirements get more difficult to specify. These factors lead to the machines becoming more complex to design and increase the number of standards and regulations for designers.

Nevertheless, the safety of the machine is of highest of importance and thus requires time and effort from the designers to investigate. This thesis was created to help the process by providing general safety requirements for NRMM and more specific ones for the analyzed micro-excavator case that includes ZH system and individual EHAs.

The requirements for the new systems were gathered from standards related to NRMMs, EMMs, high voltage, and hydraulic systems. From time to time requisitions and guidelines were borrow from standards aimed towards electrically propelled vehicles to ensure that the newest high voltage safety related knowledge was applied. The standards were proven to be borrowing and giving similar requirements throughout machinery and industry, and at times when various information was provided the ones aimed at NRMM were favored.

High voltage safety was proven to be a difficult concept for standardization organizations to provide strict and definite requirements, mainly for the novelty of the field. Many requirements were within the lines of must work, must have, without proposing well known methods for the designers. This also meant that compared to the traditional EMM, the number of requirements increased to respond with the more hazardous systems. This requires strict analysis and evaluation from the designers when considering all the requirements to ensure the compliance with standards.

The process for creating a hazard analysis can be found in multiple functional safety standards but the one chosen for the thesis was ISO 19014. It proved to be a useful tool to analyze actuators and hazardous movements. The gained safety level requirements were proven to be important when the safety system was designed. The average safety level for ZH system with EHA was evaluated to be of safety level b but when evaluating the traction for the machine the safety level requirement rose to c. The higher safety level

was chosen for the conceptual safety system design mainly to assure if the EHA is implemented in stricter machine environment but also for demonstrative purposes.

The conceptual safety system design for ZH was proposed based on the requirements found on multiple standards, through MPLr evaluation in ISO 19014 and safety system design based in ISO 13849. As the limitations and component selection differ depending on the manufacturer the complete safety design was not provided. The next step would be to evaluate and select all individual components or give the partnered manufacturers the design requirements. This is to demonstrate the acquired safety levels and for the future documentation.

Another important step would be the creation of a prototype. This way the possible communication between controllers in case of fault could be verified and designed. As the final designed had two paths of achieving safety, the interface between all safety features and wanted safety actuations need to carefully looked at. With excavators there are always risks involved either with the possibility to crush something or having the heavy arm apply constant pressure on object that it is not supposed to. Therefore, the application cases of stopping the hazardous actuator or safely lowering it down needs to be designed.

The results of this thesis are meant to provide information and clarity when implementing ZH. The requirements and functional safety are the modern tools for system designers to achieve inherent safety for novel machines.

REFERENCES

[1] I. Burch and J. Gilchrist, “Survey of Global Activity to Phase Out Internal Combustion Engine Vehicles.”

[2] A. Lajunen, J. Suomela, J. Pippuri, K. Tammi, T. Lehmuspelto, and P. Sainio, “Electric and hybrid electric non-road mobile machinery - present situation and future trends,” *World Electr. Veh. J.*, vol. 8, no. 1, pp. 172–183, 2016, doi: 10.3390/wevj8010172.

[3] T. S. Kwon *et al.*, “Power control algorithm for hybrid excavator with supercapacitor,” *IEEE Trans. Ind. Appl.*, vol. 46, no. 4, pp. 1447–1455, Jul. 2010, doi: 10.1109/TIA.2010.2049815.

[4] H. Yao and Q. Wang, “Development of Power Train of Hybrid Power Excavator,” 2013.

[5] H. Yao and Q. Wang, “Control strategy for hybrid excavator swing system driven by electric motor,” in *IFAC Proceedings Volumes (IFAC-PapersOnline)*, 2013, vol. 46, no. 5, pp. 109–115, doi: 10.3182/20130410-3-CN-2034.00065.

[6] A. ; Lajunen, P. ; Sainio, L. ; Laurila, J. ; Pippuri-Mäkeläinen, and K. Tammi, “Overview of Powertrain Electrification and Future Scenarios for Non-Road Mobile Machinery,” *Energies*, vol. 11, no. 5, 2018, doi: 10.3390/en11051184.

[7] P. Sainio *et al.*, “Technology road map for hybrid and electrical drivetrain of non-road mobile machinery.”

[8] T. A. Minav, J. E. Heikkinen, and M. Pietola, “Electric-driven Zonal Hydraulics in Non-Road Mobile Machinery,” *New Appl. Electr. Drives*, Dec. 2015, doi: 10.5772/61793.

[9] “ISO 22072:2011 Aerospace — Electrohydrostatic actuator (EHA) — Characteristics to be defined in procurement specifications.”

[10] K. Rajashekara, “Present status and future trends in electric vehicle propulsion technologies,” *IEEE J. Emerg. Sel. Top. Power Electron.*, vol. 1, no. 1, pp. 3–10, 2013, doi: 10.1109/JESTPE.2013.2259614.

[11] “SFS-EN ISO 16230-1:en Agricultural machinery and tractors. Safety of higher voltage electrical and electronic components and systems. Part 1: General requirements (ISO 16230-1:2015).”

[12] “ISO 14990-1:2016 Earth-moving machinery -- Electrical safety of machines utilizing electric drives and related components and systems -- Part 1: General requirements,” 2016.

[13] “Avain standardien maailmaan - Suomen Standardisoimisliitto SFS ry.” .

[14] J. Hagelund, J. Jerlang, A. Karppinen, D. Simunic, and N. Hampson-Jones, *A World Built on Standards: A Textbook for Higher Education*. 2015.

[15] G. P. Moreda, M. A. Muñoz-García, and P. Barreiro, “High voltage electrification of tractor and agricultural machinery - A review,” *Energy Conversion and Management*, vol. 115. Elsevier Ltd, pp. 117–131, 01-May-2016, doi: 10.1016/j.enconman.2016.02.018.

[16] “ISO 14990-3:2016 Earth-moving machinery -- Electrical safety of machines utilizing electric drives and related components and systems -- Part 3: Particular requirements for self-powered machines.” .

[17] C. Jung, “Power Up with 800-V Systems: The benefits of upgrading voltage power for battery-electric passenger vehicles,” *IEEE Electrif. Mag.*, vol. 5, no. 1, pp. 53–58, Mar. 2017, doi: 10.1109/MELE.2016.2644560.

[18] C. Mi and M. A. Masrur, *Hybrid Electric Vehicles : Principles and Applications with Practical Perspectives.* John Wiley & Sons, Incorporated, 2017.

[19] “SFS-EN 60204-1:2018 Koneturvallisuus. Koneiden sähkölaitteisto. Osa 1: Yleiset vaatimukset.”

[20] “ISO - ISO 6469-3:2018 - Electrically propelled road vehicles — Safety specifications — Part 3: Electrical safety.”

[21] “ISO - ISO 6469-2:2018 - Electrically propelled road vehicles — Safety specifications — Part 2: Vehicle operational safety.”

[22] A. Mathsyaraja, “Ground Fault Detection for Flexible High Voltage Power Systems,” *SAE Int. J. Commer. Veh.*, vol. 4, no. 1, pp. 185–197, Oct. 2011, doi: 10.4271/2011-01-2252.

[23] SFS 6000-4-44:2017, “Pienjännitesähköasennukset. Osa 4-44: Suojausmenetelmät. Suojaus jännitehäiriöiltä ja sähkömagneettisilta häiriöiltä.” .

[24] “SFS-EN ISO 13766-1:2018:en Earth-moving and building construction machinery. Electromagnetic compatibility (EMC) of machines with internal electrical power supply. Part 1: General EMC requirements under typical electromagnetic environmental conditions (IS.”

[25] “SFS-EN ISO 13766-2:2018:en Earth-moving and building construction machinery. Electromagnetic compatibility (EMC) of machines with internal electrical power supply. Part 2: Additional EMC requirements for functional safety (ISO 13766-2:2018).” .

[26] “ISO 20474-1:2017 Earth-moving machinery — Safety — Part 1: General requirements.”

[27] “SFS-EN ISO 4413 Hydraulic fluid power. General rules and safety requirements for systems and their components (ISO 4413:2010).”

[28] “SFS-ISO 8643:2017:en Earth-moving machinery -- Hydraulic excavator and backhoe loader lowering control device -- Requirements and tests.”

[29] “ISO - ISO 6469-1:2019 - Electrically propelled road vehicles — Safety specifications — Part 1: Rechargeable energy storage system (RESS).”

[30] “SFS-EN ISO 17409:2017:en, Electrically propelled road vehicles. Connection to an external electric power supply. Safety requirements.”

[31] “SFS-EN ISO 14118:2018:en Safety of machinery. Prevention of unexpected start-up (ISO 14118:2017).”

[32] “SFS-EN ISO 13850 Safety of machinery. Emergency stop function. Principles for design (ISO 13850:2015).”

[33] Torben Jespen, *Risk Assessments and Safe Machinery*. 2016.

[34] “SFS-EN ISO 12100 Safety of machinery. General principles for design. Risk assessment and risk reduction (ISO 12100:2010).”

[35] “SFS-EN 61508-1 Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements.”

[36] T. Malm, O. Venho-Ahonen, M. Hietikko, T. Stålhane, C. de Bésche, and J. Hedberg, “From risks to requirements Comparing the assignment of functional safety requirements,” 2015.

[37] “SFS-EN 62061:en Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems.”

[38] “SFS 5974 Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery.”

[39] J. Rauhamäki, “Designing Functional Safety Systems: A Pattern Language Approach,” Tampere university of technology, 2017.

[40] “SFS-EN ISO 13849-1:en Safety of machinery. Safety-related parts of control systems. Part 1: General principles for design (ISO 13849-1:2015).”

[41] “SFS-EN ISO 19014-1:2018:en Earth-moving machinery. Functional safety. Part 1: Methodology to determine safety-related parts of the control system and performance requirements (ISO 19014-1:2018, Corrected version 2019-02).”

[42] H. Inoue, “DEVELOPMENT OF HYBRID HYDRAULIC EXCAVATORS,” 2014.

[43] EUROMACH, “Käyttö- ja huolto-opas.” .

[44] S. Zarotti, R. Paoluzzi, G. Ganassi, F. Terenzi, P. Dardani, and G. Pietropaolo, “ANALYSIS OF HYDRAULIC EXCAVATOR WORKING CYCLE.,” *11th Eur. Reg. Conf. Int. Soc. Terrain-Vehicle Syst.*, 2009.

[45] J. Rauhamäki and S. Kuikka, “Patterns for control system safety,” in *ACM International Conference Proceeding Series*, 2015, vol. 10-14-July, doi: 10.1145/2739011.2739034.

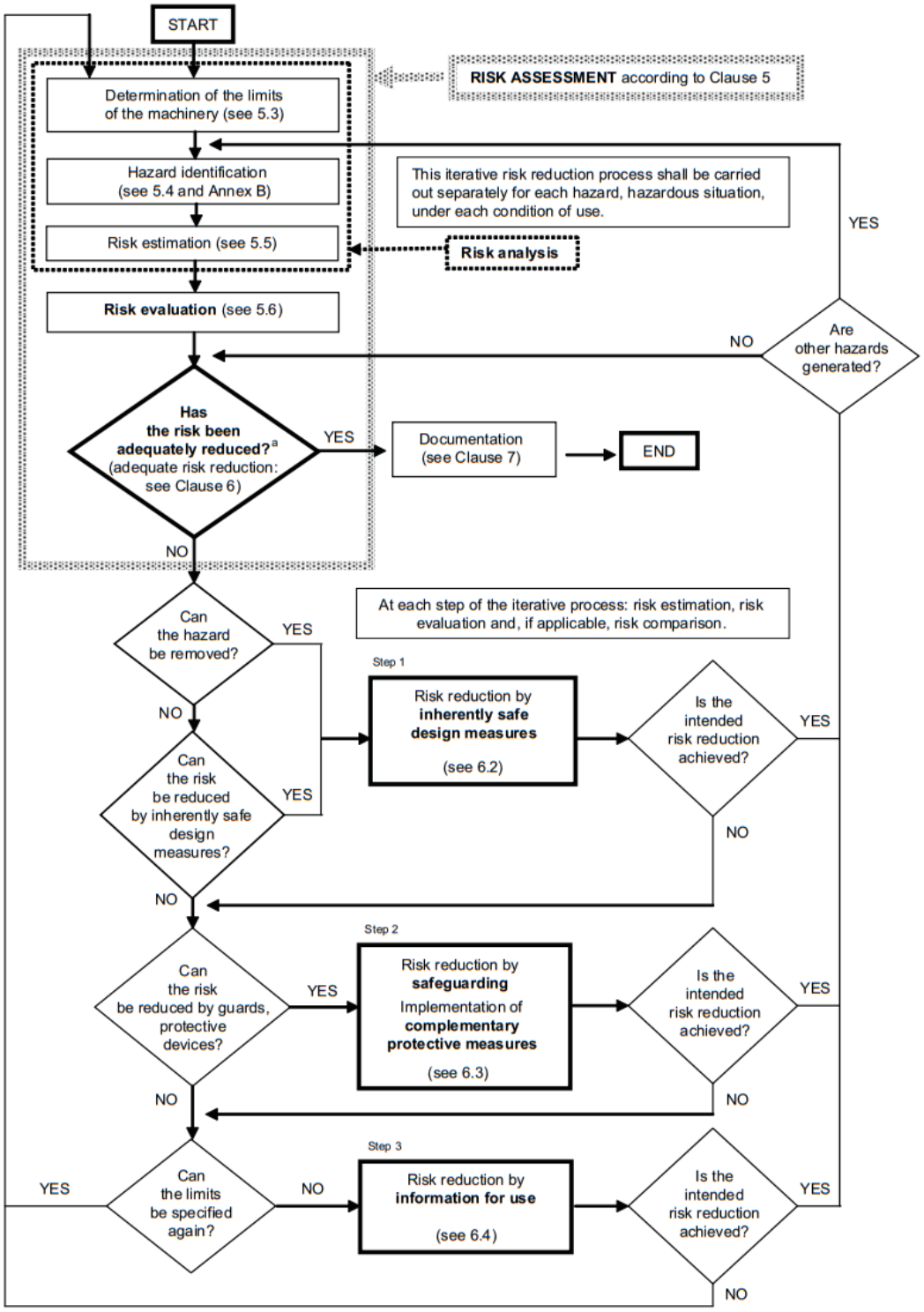
ANNEX A

Enquiry form for electrical equipment of self-powered machines (From ISO 14990-3 [16])

Item of information	Response
Date	
Quotation number, order number, etc.	
Name of manufacturer/supplier	
Name of purchaser/end user	
Type of machine	
1. Special concerns	
1.1 a) Will the machine be used in production or processing of explosive or flammable materials?	Yes/No
b) If yes, the specific nature of the materials	
1.2 a) Might the machine be used in explosive or flammable atmospheres?	Yes/No
b) If yes, the specific nature of the atmospheres	
1.3 a) Are any materials to be worked by the machine likely to give rise to special hazards?	Yes/No
b) If yes, specify the nature of the materials and hazards.	
1.4 a) Will the machine be used in mines?	Yes/No
b) If yes, specify the type of mine and material mined.	
1.5 Might the machine be exposed to more severe conditions during transportation or storage (e.g. temperatures beyond the normal operating range, etc.)	
1.6 Indicate any special limitations on the transport of the machine to the worksite	
1.7 Indicate any special aspect to facilitate maintenance and repair	
1.8 Indicate any special aspect to improve reliability and ease of operation	
2. Operating environment	
2.1 Indicate the worst-case EMC environment (note likely sources of interference)	
2.2 Maximum altitude	
2.3 Ambient temperature range	
2.4 Humidity range	
2.5 Special conditions (e.g. high dust level, very wet, corrosive atmosphere, etc.)	
2.6 Will the machine be used a) outdoors only?	Yes/No
b) indoors or within enclosed areas?	Yes/No
2.7 Will the machine be exposed to radiation?	Yes/No
2.8 Indicate the electrical competence of persons who would have access to the interior of electrical enclosures during normal use of the machine (untrained, instructed, skilled, etc.)	
2.9 Can safe access into electrical enclosures be reasonably ensured if such enclosures are supplied with removable keys or special tools to open them?	Yes/No
2.10 a) Is a particular degree of protection (sealing) desired for electrical and control enclosures?	
b) If so, specify.	
3. Controls	
3.1 If wireless controls will be used, what is the desired time delay before automatic machine shutdown is initiated in the absence of control signal?	
3.2 Are special colours desired for any operating controls? (e.g. such as may be in use on existing machines)	
3.3 Special environmental requirements	
3.4 Any special conditions relating to control devices, visual indicators, and displays?	
4. Miscellaneous electrical	
4.1 a) If convenience socket-outlets are to be provided, is a particular type desired?	Yes/No
b) If yes, what type?	
4.2 Are convenience socket-outlets to be provided with residual current protective devices (RCD)?	Yes/No
4.3 If there is a preferred or maximum voltage for lighting circuits, specify	
4.4 Special safety requirements, e.g.: Fire suppression system is required	
5. Markings	
5.1 a) Is a third-party certification mark desired?	Yes/No
b) If yes, specify.	
5.2 Specify any special markings to be placed on electrical equipment	
5.3 Specify the language to be used in markings	
6. Technical documentation	
6.1 Specify the language to be used in technical documentation	
6.2 Specify the media to be used for technical documentation (e.g. print, CD, DVD, etc.)	
6.3 Is a certificate of operating tests to be provided?	Yes/No

ANNEX B

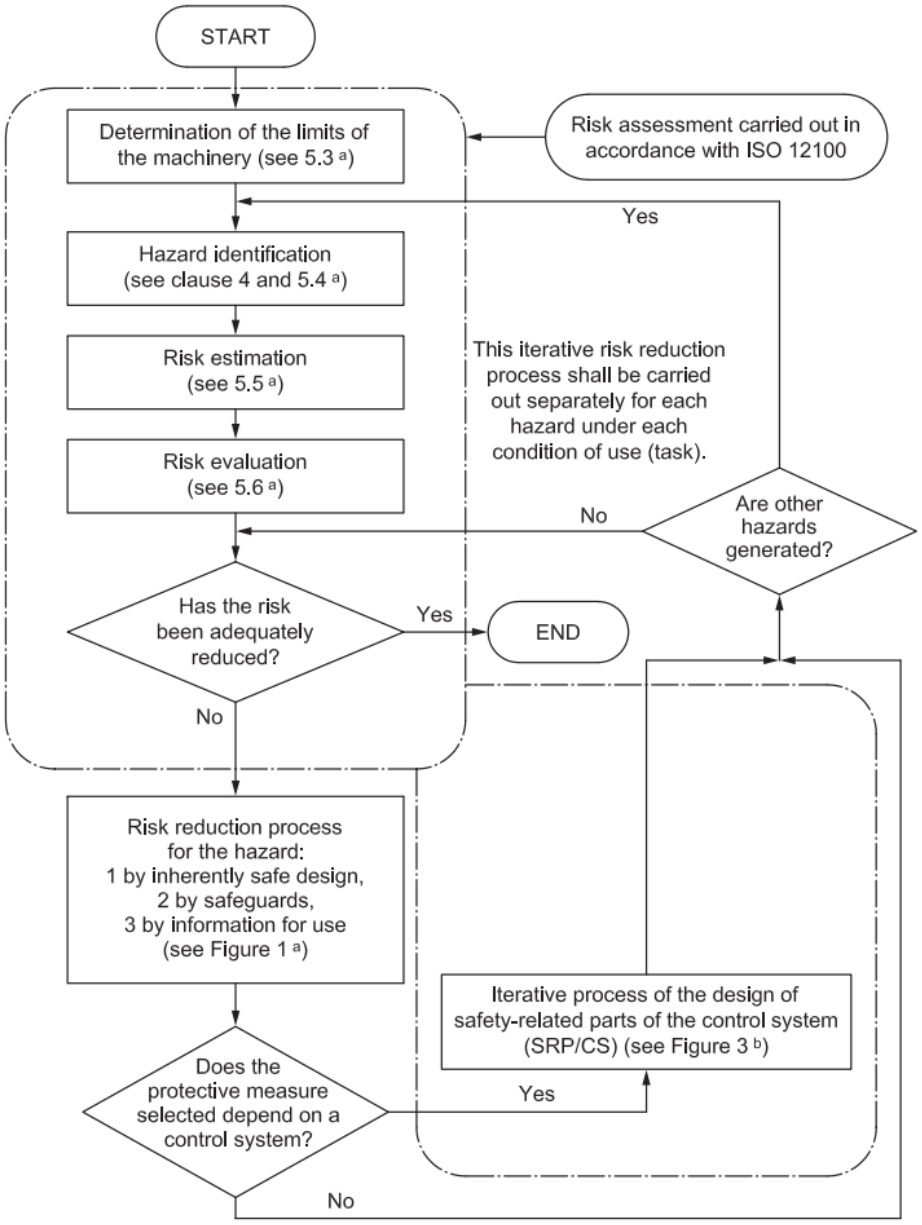
Risk reduction process introduced in ISO 12100 [34]



a The first time the question is asked, it is answered by the result of the initial risk assessment.

ANNEX C

Overview of risk assessment/risk reduction [40]



a Refers to ISO 12100:2010

b Refers to this part of ISO 13849