Politecnico di Torino

DEPARTMENT OF MECHANICAL AND AEROSPACE ENGINEERING

Master of Science in Mechanical Engineering

Design, evaluation and possible alternatives for AGV safety systems

Tutors:
Prof. Alessandro Rizzo
Dipl.-Ing. Jan Stefan Zernickel

Author:
Antonio Misuraca

Contents

Abstract

The present Master Thesis is focused on the topic of industrial safety, and has been developed in collaboration with InSystems Automation GmbH. Despite being a well-established practice, industrial safety is still to be consolidated when working with Automated Guided Vehicles, since these are constantly growing in number due to the improvements that take place when moving towards Industry 4.0. When dealing with the safety of people, the most important aspect is clarity and documentation. For this reason, norms like EN 1525 "Safety of industrial trucks - Driverless trucks and their systems" [6] are presented in the second chapter of this document, after a general introduction to the host company. The same chapter contains a thorough explanation of the main features of a safety system, as well as a walk-through of the norm ISO 13849 "Safety of machinery - Safety related parts of control systems", describing the workflow that is necessary to design a safety system.

Chapter 3 goes more in depth on the technological aspects of the safety systems deployed on mobile robots, namely the proANT 436 and proANT 490 robots that are manufactured by the host company. Here, the different aspects of safe components are discussed. More specifically, on the first subsystem described, the complete calculation of the safety performance is carried out step by step. Then, the other safety functions are described alongside with an in-depth description of the electronic and electro-mechanical components that are used to achieve a safe system. The breakdown of the system ends with a cost analysis and various suggested solutions to improve the cost-effectiveness.

Since it is not admissible to try to improve a system without studying the other solutions used by other manufacturers, chapter 4 presents the state of the art for AGV safety systems. The starting point is a description of the functionalities that the system needs to have. Then, the technology currently used by competitors is analysed, dividing the AGVs into four different types that generally have different requirements: forklift, differential drive, omni-wheel platform, magnetic or wire guided. A total of 13 manufacturers have been studied, finding a common thread among all of them.

Chapter 5 is the heart of the present work. All the knowledge gained by studying the norms and the competitors allows to suggest different alternatives to improve the safety systems of the AGVs. Solutions like different laser scanners, cameras and ultrasonic sensors are discussed and analysed.

Finally, the last chapter gives some hints about the implementation of a new safety system and a brief introduction to the role of future technological improvements.

Chapter 1

Introduction

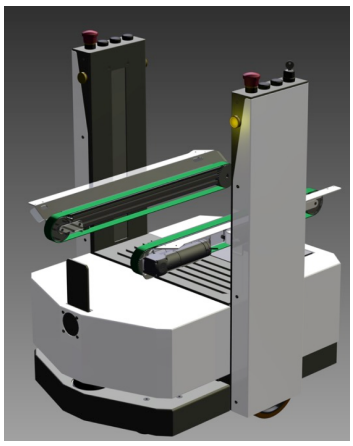
An AGV (Automated Guided Vehicle) is a mobile robot that navigates in an environment and it is mainly used to move a medium quantity of material (e.g. pallet loads) between shipping/receiving docks and storage racks, or to move semi-finished products between machine tools and stations. Usually AVGs travel speed is slower than the typical human walking speed, but due to their weight they could cause hazards for humans, and thus they carry several safety features. Some of them are obstacle detection, emergency bumpers, warning lights and warning sounds. In order to control AGVs, an industrial plant can use locator panels, color graphics displays, and central logging and report.

These machines can be used in various kinds of industries, such as pharmaceutical, chemical, manufacturing, paper and print, and in facilities like hospitals and warehouses. They can also be customized regarding the exact needs of the customers, allowing a great flexibility of the overall system.

The company: InSystems Automation GmbH

The thesis research took place at InSystems Automation GmbH in Berlin, Germany, from March 2019 to September 2019. InSystems Automation develops special machines for production, material flow and quality tests and it is specialized on the production of robots since 2012. The company was founded in 1999 by the managing directors Henry Stubert and Torsten Gast and grew constantly since. By now, more than 50 employees work at InSystems. The company is located in the science center Berlin-Adlershof and has offices, a workshop, an online shop and a showroom. Among the different activities carried out by the company, an important role is played by the manufacturing and constant development of a variety of AGVs. These are specifically designed according to customer demand and they can deal with loads of different weight, usually from 30 kg up to 1000 kg. The transport robots are developed under the name proANT, and the fleet is continuously growing with new models. The company features a certified competence since 2006, working with partners like Siemens and Wago.

proANT 016



proANT 436

proANT 485

proANT 490

proANT 576

Figure 1.1: The fleet of AGVs currently available from InSystems Automation

Chapter 2

Design of an AGV safety system

An Automated Guided Vehicle has to operate in an industrial environment without increasing the hazard levels of the plant. Especially when AGVs share their pathway with humans, their presence can't lead to any harmful or dangerous situation. To achieve this goal, the vehicles must be designed according to various norms that consider different aspects of their interaction with humans and with the plant itself. One of the most fundamental norms is the EN 1525-1998 "Safety of industrial trucks - Driverless trucks and their systems" [6], that will be briefly described below.

2.1 Safety according to EN 1525

This standard applies to all driverless industrial trucks [1], which are defined as "a powered vehicle, including any trailers, designed to travel automatically in which the safety of operation does not depend on an operator". The purpose of this standard is then to provide the technical requirements to minimize the hazards which can occur during operation or maintenance of the trucks. The first part of the norm consists in a detailed glossary (e.g. definitions of load, bumper, zones, path etc.) and a list of possible hazards (e.g. crushing, falling objects, lack of stability etc.). Then, in Section 5, the norm lists all the safety requirements for the autonomous guided vehicles, with cross-references to other norms.

Specifically, the truck must have:

- Protection against unauthorized use;
- Mechanical braking system that gets activated in case of potential hazard;
- Speed control system in accordance with EN 954-1 [7] category 1[2];

[1] Exception made for trucks solely guided by mechanical means (rails, guides, etc.) and trucks operating in areas open to persons unaware of the hazards.

[2] Categories are explained in the following section

- Protection against accidental contact with the charging connections of the trucks and their charging systems;
- Design of load handling systems that doesn't allow the uncontrolled movement of the load;
- Safety related parts of the steering system in accordance with EN 954-1 [7] category 1;
- Stability assured in all operating positions;
- Warning systems such as a flashing light, that must be activated when trucks are ready to move or moving, in accordance with EN 954-1 [7] category 1;
- Emergency stop devices complying with category 0^2, the actuators for emergency stop devices shall be easily visible and accessible;
- Safety related parts of the control system for emergency stop devices, in accordance with EN 954-1 category 3;
- Personnel detection systems that can trigger the emergency stop state;
- Safety related parts of the personnel detection system in accordance with EN 954-1 [7] category 3;

Section 6 gives procedures for verification and commissioning of the machines, whereas Section 7 gives the manufacturer detailed guidelines on how to produce maintenance instructions. Annex A establishes the minimum requirements for the preparation of the working environment, so that the automated vehicles can operate safely (for example a minimum safety clearance of 0.5 m wide for a height of 2.1 m on both sides of the truck).

The present norm was recently substituted by the more complete BS EN ISO 13489 [2]. However, the new norm covers a wider range of applications and doesn't give tangible tangible guidelines on the safety functions of AGVs. For this reason, it is a good idea to keep considering the older EN 1525 [6] when designing a safety system for driver-less trucks, especially when addressing the specific safety functions.

ISO 13489 describes in more detail the categories stated in the older EN 954-1. However, EN 1525 refers to EN 954-1, and for this reason a brief explanation of the above-mentioned norm is provided below.

EN 954-1 [7] safety requirements categories

- Category B: The safety-related parts of control systems shall withstand the expected operating stresses, the influence of transported material, and other relevant external influences e.g. vibrations or power supply interruption.

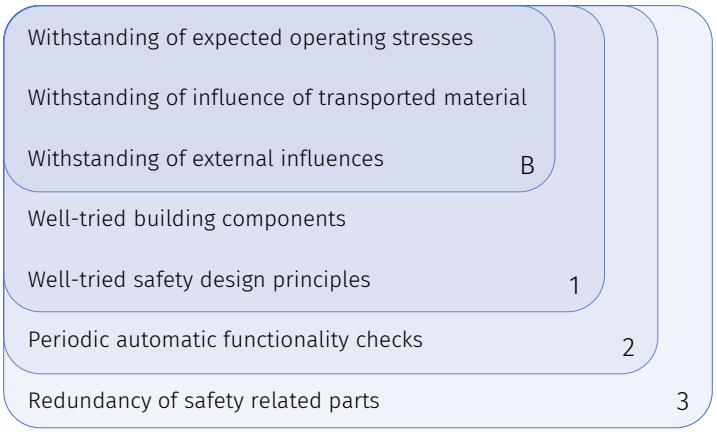


Figure 2.1: Features of the safety-related parts of the control system. Each feature belongs to its own category as well as the outer, more demanding categories.

- Category 1: The safety-related parts of control systems must fulfill all the requirements of category B. In addition, they shall be constructed using well-tried components and well-tried safety principles. Well tried components are components that have been widely used in the past with successful results or have been made and verified using reliable principles.

- Category 2: The safety-related parts of control systems must fulfill all the requirements of category 1. In addition, they shall be designed so that their functions are checked periodically by the machine control system. If the check has a negative result, the control system must not allow the truck to start.

- Category 3: The safety-related parts of control systems must fulfill all the requirements of category 2. In addition, they shall be designed so that a single fault in any of these parts does not lead to the loss of the safety function.

The relationship between this norm and the more recent and expanded ISO 13849 will be presented in section 2.3.

2.2 Scheme of a safety system

A safety system, in its most generic aspect, must reduce the hazard coming from industrial machines and equipment. An introductory example could be a system that protects the access to a restricted area of a machine to parts of the human body. This can be achieved through a light curtain that creates a virtual barrier between the hazardous parts of a machine and the outside, as represented in figure 2.2. In this application the human interaction is very frequent due to load/unload operations, thus a physical door would substantially reduce the efficiency of the operation.

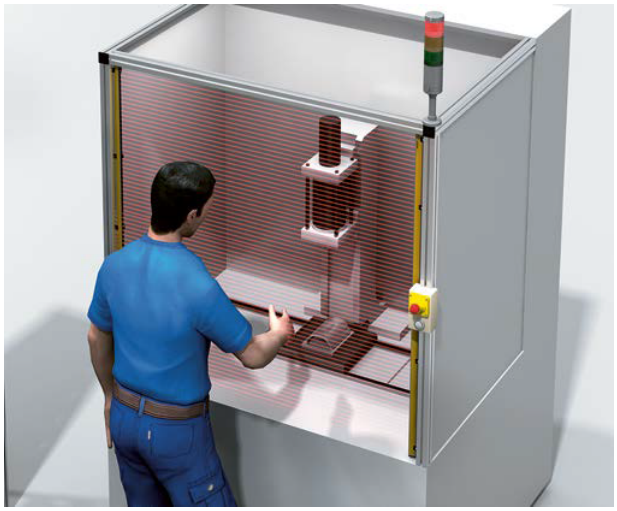


Figure 2.2: Application example of a light curtain in a tooling machine (Guide for Safe Machinery - Sick [23])

Now a clearer distinction must be done between the components of a safety system. At its simplest, a safety system consists of an input device, a logic device and an output device (figure 2.3). The light curtain in the previous example is the input device: it senses whether if the protected zone is free or obstructed, and constantly sends its result to the logic. The logic then interprets the signal sent by the sensing device and computes whether the machine needs to be stopped or not. If the sensing device's safety field is harmed, the logic will send a signal to the output device, whose aim is to put the machine in a safe state (e.g. stopping the operation). Usually the safe output consists of a relay that cuts off the current to the motor driver.

The main aspects of a safety system will be now introduced, namely the structure of the system, the reliability of components, the self-diagnostic functions and the resistance to common cause failures.

Figure 2.3: Fundamental backbone of a safety system.

Structure

To reduce the susceptibility of a safety component to fault by means of a better structure, the safety-related functions can be executed in parallel on more than one channel. Dual-channel safety components are common in the machine safety sector (see figure 2.8). Each channel alone can perform the intended safety function, so that a failure of one channel does not impair the safety system as a whole. The two channels can be of diverse design (e.g. one channel using electromechanical components, the other only electronics) [2]. Instead of a second equivalent channel, the second channel can also have a pure monitoring function (figure 2.7).

Reliability of the components

Any failure of a safety component will result in a disturbance the production process. For this reason the use of highly reliable components is crucial. The more reliable a component is, the lower the probability of a dangerous failure. Reliability is a measure of random failures within the life limit; it is normally provided in the following formats:

- B_{10} figures for electromechanical or pneumatic components. Here, life limit is determined by switching frequency. B_{10} indicates the number of switching cycles until 10% of components fail.
- Failure rate λ (lambda value) for electronic components. Often the failure rate is stated in FIT (Failures In Time). One FIT is one failure per 10^9 hours.

The trend of the failure rate follows the bathtub curve, shown in figure 2.4. The first part is a decreasing failure rate curve, known as early failures. The second part is a constant failure rate, known as random failures. The third part is again an increasing curve that represents the phenomenon known as wear-out failures [21].

Diagnostics for detecting faults

Certain faults can be detected by diagnostics measures. These include plausibility monitoring, current and voltage monitoring, watchdog functionality, brief function test, etc. Since all faults cannot always be detected, the degree of fault detection must be defined. A Failure Mode and Effects Analysis (FMEA) should be performed for this purpose [8]. For complex designs, measures and empirical values from standards provide assistance.

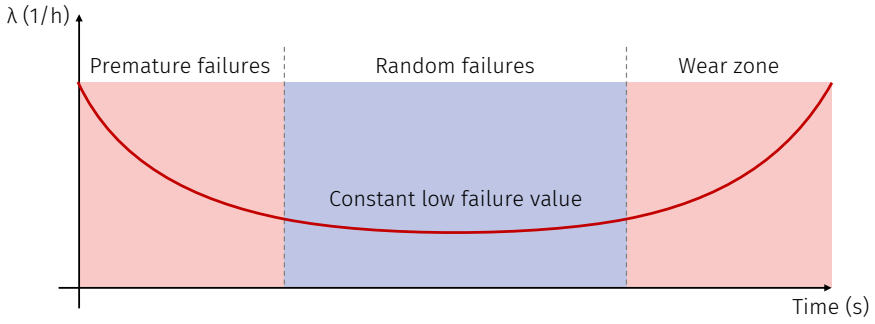


Figure 2.4: Bathtub curve, widely used in reliability engineering, is a combination of a decreasing hazard of early failure ("infant mortality failure") and an increasing hazard of wear-out failure , plus some constant hazard of random failure [21].

Resistance to common cause failure

The term common cause failure describes the situation in which, in a two-channel architecture, both channels fail simultaneously due to the same external factor [2]. For example, a failure in the power supply that leads to an over-voltage will impair the functionalities of both channels together. Appropriate measures shall be taken, e.g., isolated cable routing, suppressors, diversity of components, etc.

For an AGV, the safety system must allow the safe collaboration of the machine with the personnel and the whole industrial plant. In this case, the main hazard comes from the vehicle potentially crushing into something or someone, so the fundamental function that a safety system must perform is the detection of obstacles or personnel along the path of the AGV itself. Since it is safety-related, this function shall be performed with a sufficient reliability. This reliability is exactly the main topic of the ISO 13849-1-2015 "Safety of machinery - Safety related parts of control systems" [2], a standard that provides most of the tools and knowledge necessary to achieve the required safety levels in a machine, depending on the entity of the hazard that the machine itself intrinsically carries.

2.3 Design workflow of a safety system according to BS EN ISO 13849 [2]

The parts of machinery that are assigned to perform safety functions are called "safety related parts of control systems", abbreviated SRP/CS, and they can consist of hardware and software. The capability of the safety related parts of control systems to perform their function in a reliable way is defined in terms of *probability of dangerous failure per hour*. To each range of probability is given an associated Performance Level (PL), as described in table 2.1.

For every performance level the norm states not only a quantifiable aspect (that is PFH_d),

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

Table 2.1: Performace Levels

but also some qualitative aspects like the behavior of the safety functions under fault conditions, the safety related software or the systematic failure.

The design and assessment process is iterative and follows a flowchart displayed in figure 2.5. Considering the safety system of an AGV, the starting point is the definition of the safety functions, namely the "function of the machine whose failure can result in an immediate increase of the risk(s)", as stated in ISO 12100:2010, 3.30 [1].

2.3.1 Determination of the safety functions

The safety functions consider both the application and the hazard. In our case the hazard is the possibility of a heavy driver-less vehicle crushing on a human. This occurrence needs to be prevented using at least three safety functions, that are common in most AGVs:

- SF1 - Safe stop initiated by emergency stop button. This safety function is common in all industrial machines, and AGVs are not excluded.
- SF2 - Safe stop initiated by laser scanner. This function consists of detecting obstacles in front of the vehicle and reliably bringing the latter to a safe stop.
- SF3 - Dynamic safety field switch according to speed. This function enlarges or reduces the scanned area in front of the AGV according to its speed.

Each of the former is a different safety function and must be addressed separately, with its own safety system. At this point, the general characteristics of the safety function are known, e.g. the desired output (safe stop or field switch) and the action that is needed to trigger the system (emergency buttons, laser scanner or speed). More system-specific details about these safety functions are given in chapter 3.1.

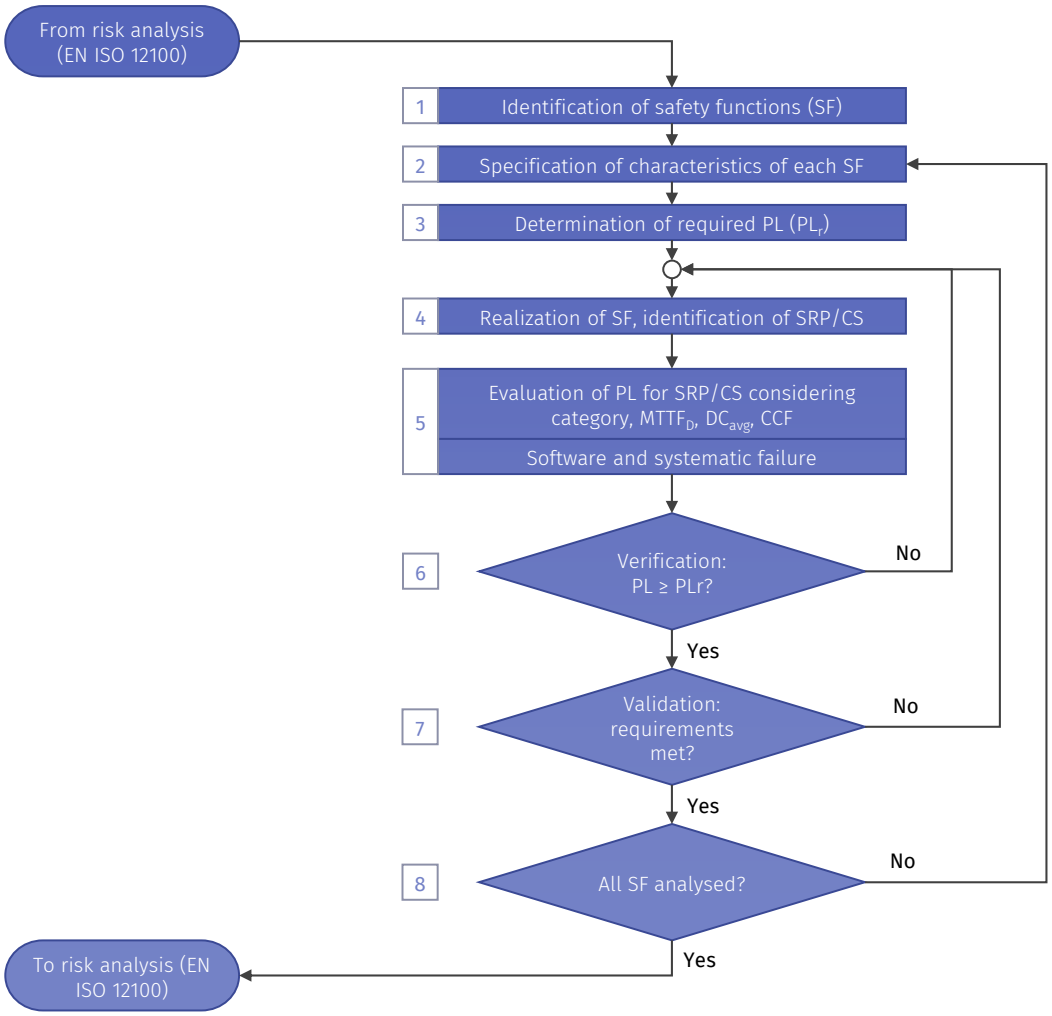


Figure 2.5: Iterative process for design of the safety-related parts of control systems.

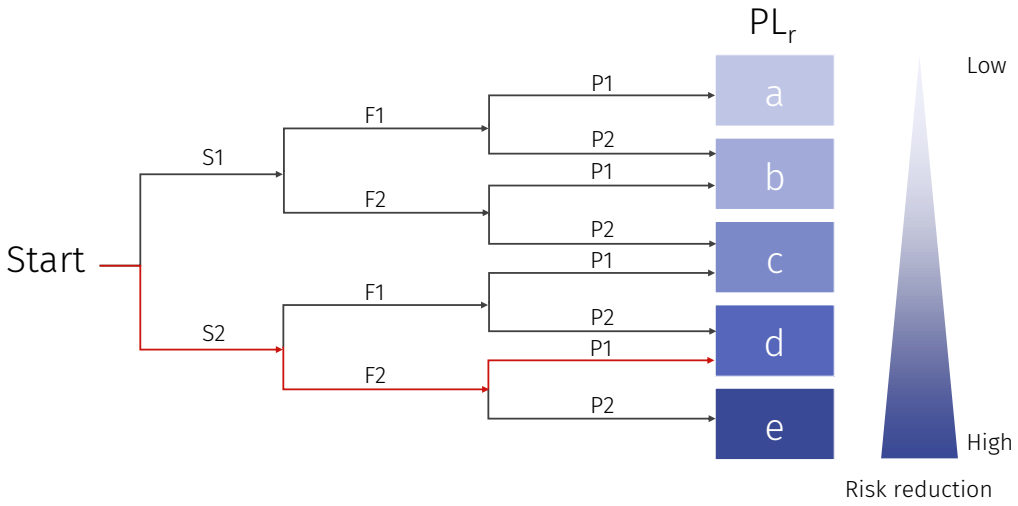


Figure 2.6: Graph for determining required PL_r for safety function.

2.3.2 Determination of the required performance level PL_r

It is of great evidence that the required Performance Level must be determined carefully *for each intended safety function*. The Annex A of the ISO 13849-1 gives guidance on estimating the PL_r for the safety system that performs the safety function. It is based on a risk estimation carried out by selecting the parameters S (severity of injury), F (frequency of exposition to the hazard) and P (possibility of avoiding the hazardous event). We will now focus on SF2, the function that detects humans or obstacles in front of the moving robot and stops the machine in a safe, reliable way. In our case, an AGV can bring serious injury to humans (S2), exposure is frequent (F2) and there is the possibility of avoiding hazard under specific conditions (P1). Thus, the required performance level is $PL_r = d$, as shown in the graph 2.6. The process here described depends on the risk assessment based on ISO 12100 [1].

The other safety functions follow the same path of the one discussed above, since the hazard is fundamentally the same, an AGV crushing into people. The result of the analysis of the other three safety functions is:

- SF1 - Safe stop initiated by emergency stop button: $PL_r = d$;
- SF2 - Safe stop initiated by laser scanner: $PL_r = d$;
- SF3 - Dynamic safety field switch according to speed: $PL_r = d$;

Although the previously discussed method is simple and allows a fast evaluation of the PL_r, a more robust evaluation when discussing AGVs can be carried out according to the

Required Category to EN 954-1:1996	Required Performance Level PLr and required Category to EN ISO 13849-1:2006
B	b
1	c
2	d, Category 2
3	d, Category 3
4	e

Table 2.2: Worst-case approach for conversion from a required Category in accordance with EN 954-1 to a required Performance Level PL_r [8]

EN 1525, described briefly in section 2.1. In the norm, each safety function (and thus its correspondent safety system) shall meet the specifications described in a Category of EN 954-1; for example, the safety related parts of the personnel detection system must be in accordance with EN 954-1 category 3. Anyway, EN 954-1 is older and less specific than ISO 13849, so it would be helpful to find a correlation between the Categories of EN 954-1 and the required Performance Level PL_r of ISO 13849. The German "Institute for Occupational Safety and Health of the German Social Accident Insurance" (IFA) provides a paper [8] in which the correlation between Categories and PL_r is discussed, and the resulting conversion table is shown in table 2.2.

According to the table, the required performance level for the personnel detection system is $PL_r = d$, equivalent to Category 3. This is the same result obtained with the simplified model, so both methods carry the same result. It is then confirmed that the system must complain with this parameter.

2.3.3 Design of safe control systems

Once the precise safety function and its required risk reduction (the PL_r) have been defined, the design of the *safety related parts of the control system* (SRP/CS) begins. The target of each activity during the design and integration of the SRP/CS is to develop and use products that are as free of faults as possible and which satisfy the safety requirements. Ultimately, the objective concerns the health of human beings and the avoidance of accidents. The motto for the design and development process must therefore be: *structured and well-documented*. For this purpose, chapter 10 of ISO 13849-1 gives guidelines the the minimum required information to be present in the documentation, including for example the exact safety function(s), the exact points at which the safety-related parts start and end, the PL, the software documentation etc.
Another fundamental document is the "Information for use". It must describe the limits of the system, the response time, the maintenance steps and other information all listed in chapter 11 of the above-mentioned norm.

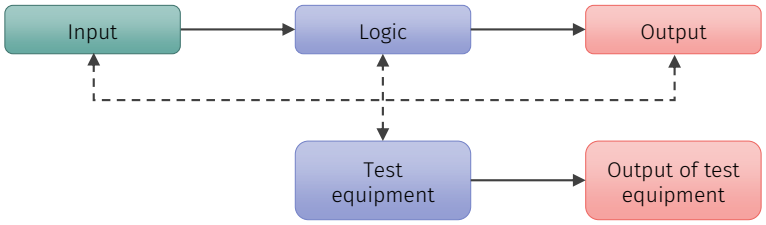


Figure 2.7: Designated architecture for category 2. Solid lines represent interconnection means, whereas dashed lines represent reasonably practicable fault detection/monitoring.

The determination of the PL is based upon the numerical quantification of the probability of failure. This value can be estimated through approximation with statistical methods or any recognized method, since the regulations are quite flexible in this regard. Such methods include reliability block diagrams, fault tree analysis, Markov modeling or Petri nets. However, a simplified approach described in ISO 13849-1 can be used for practical situations, with the only disadvantage of erring on the safe side, which could result in a greater estimated probability of failure. Below, this method will be used to describe the current safety system. It starts by defining one of the designated architectures.

Safety system architecture

The vast majority of all safety-related control systems can be classified in very few architectures. The least performing architecture is the single-channel untested system with components of differing reliability. It is represented in figure 2.3. This architecture allows a Performance Level up to PL c, which is too low to guarantee the minimum required safety specifications. An improved version is the same system enhanced by testing. The best performing system is however the two-channel system featuring high quality testing. Inside each of these architectures the components can also be divided into sensors level (input devices I), processing level (logic L) and actuator level (output O). Each Category described in ISO 13849-1 has quantitative requirements regarding:

- component reliability, represented by the mean time to dangerous failure MTTF_d
- diagnostic coverage of tests DC_{avg}
- resistance to common cause failure CCF

A basic requisite common to all categories is that the SRP/CS must be designed to resist the normal operating stresses and the influence of predictable disturbances (dust, chips...) and external influences like vibration or electromagnetic interference. These fundamental requirements are often met, since most components on the market must already fulfill these basic details.

The architecture of **Category 2** systems is shown in figure 2.7. In addition to the basic requirements, here well-tried safety principles must be applied; they are employed

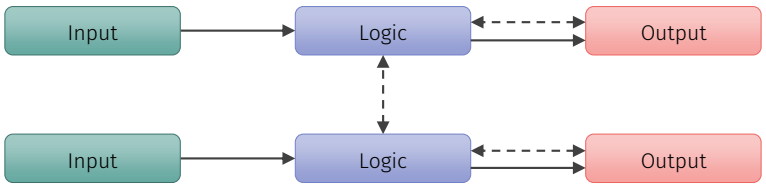


Figure 2.8: Designated architecture for category 3. Solid lines represent interconnection means, whereas dashed lines represent reasonably practicable fault detection/monitoring.

in order to minimize or exclude critical fault or failures that influence the safety function. For example, the avoidance of undefined states in the SRP/CS or the separation between non-safety and safety functions in order to prevent unanticipated influences. To minimize or exclude critical faults, well-tried components can be used. A component can be defined well-tried if it "has been widely used in the past with success in similar applications", or "has been manufactured and verified with the application of principles which indicate its suitability and reliability for safety-related applications" [2]. However, complex electronic components such as PLCs or microprocessors cannot be regarded as well-tried.

Another feature of Category 2 systems is that their safety functions are tested at reasonable intervals by the machine control system. Since the exposure to hazard is continuous in an AGV, the tests shall run periodically during operation. When a fault is detected, an output must be generated to initiate a safe state. This happens in the actual system by sending a true (1) value on the digital input for the STO (Safe Torque Off) present in the motor driver card.

A **Category 3** systems is shown in figure 2.8. The main feature is the two-channel configuration, that allows the system to withstand single faults without resulting in the loss of the safety function. The system is also monitored such as a single fault is detected at or prior to the next demand upon the safety function.
The requirement of single fault tolerance can be met even without a two-channel configuration if the employed components have a fail-safe design, that is they are tolerant of single faults. This tolerance can be met also with a highly monitored single-channel system, when a detected fault leads to an immediate entering of the safe state, before the next request upon the safety system. In other terms, an architecture as the one in figure 2.7 with a high testing frequency can be considered a Category 3 system.

Category 4 systems architecture is similar to the previous one, but the specifications to meet are higher in terms of failure detection and component reliability. Here, not only a single fault does not result in the loss of the safety function, but also the single fault is detected immediately and the safe state is entered. If this is not possible, multiple undetected faults must not result in loss of the safety function. In this Category, both

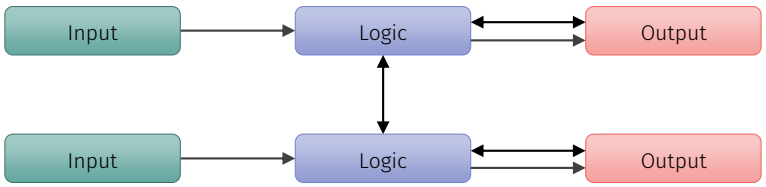


Figure 2.9: Designated architecture for category 4. The unbroken lines for monitoring symbolize the higher DC_{avg} with respect to Category 3.

MTTFd and DC_{avg} must be high. Scheme of a Category 4 system is represented in figure 2.9.

Every safety function in the AGV is however carried out by a system constituted by multiple subsystems, each one of them belonging to a certain Category. For example, the safety PLC is itself a Category 3, PL e subsystem. These subsystems will be then connected in a series fashion, to perform the required function. The combination of SRP/CS as subsystems is discussed in section 2.3.8.

2.3.4 Fault consideration and fault exclusion

In a control system there is no limit to the number of possible faults. However, some faults are more likely to happen than others, and some of them are so rare that their faulty behavior can be excluded. This is the case of technically improbable faults, or faults that do not result in a dangerous state. For example, most mechanical structures, mechanically linked elements and some hydraulic systems, have such a high reliability that their faults can virtually be excluded.

It could potentially happen that a fault in one component will generate another fault in a different component. The latter will be treated as a secondary fault, in the same way as multiple faults with a common cause (Common Cause Failure CCF). However, the occurrence of two or more faults with a *different* cause is extremely improbable, and should not be considered.

In conclusion, if a specific component (e.g. the mechanical actuation of an emergency stop device) is reliable enough, fault exclusion can be carried out, so that the component does not participate in the calculation of MTTFd and DC_{avg}. More on this topic can be found in Annex C of ISO 13849-2.

2.3.5 Mean Time To dangerous Failure - MTTF$_d$

This value characterizes the overall reliability of the component or the subsystem to which it's referred. The name itself, however, might need some preliminary explanation:

- Mean = statistical mean life of a component similar to the one under analysis. This is not a guaranteed minimum lifetime, but the *average* lifetime.
- Time = lifetime of the component or subsystem. MTTF$_d$ is usually measured in years (abbreviated "a"). Another notation can be the dangerous failure rate λ_d expressed in the unit "FIT" (10^{-9} failures per hour), with the relationship $\lambda_d = 1/MTTF_d$.
- Dangerous = failures that impair the safety function. Out of all possible failures, the Performance Level of the system is influenced only by those that lead to a dangerous state. To distinguish the dangerous failures among all of the possible failures, the subscript "d" is used. When no further information is available, the dangerous failures are assumed to be the 50% of all possible failures, thus $\lambda_d = 0.5\lambda$, for example.

Failure data can be given by the manufacturer or found in databases like Annex D of the ISO 13849-1, with conservative values erring on the safe side. Usually the data from the manufacturer expresses the failures without distinction between dangerous and safe, so it is assumed that on average just the 50% of the failures are dangerous.

Once the MTTF$_{d,i}$ is determined for every component, an FMEA analysis (Failure Mode and Effect Analysis) can be carried out to estimate the MTTF$_d$ of the entire system. This estimation, however, can be performed also by using the "parts count method", in which the failure rates are simply added together, erring on the safe side:

$$\frac{1}{MTTF_d} = \sum_{i=1}^{N} \frac{1}{MTTF_{d,i}} = \sum_{i=1}^{N} \lambda_{d,i}$$

This formula allows to combine the MTTF$_{d,i}$ for the components of a block and/or for the entire system (or channel, if the architecture exhibits multiple channels). Once the MTTF$_d$ for each channel is known, a further simplification is made in the form of a classification. The calculated values are assigned to three typical classes described in table 2.3.

2.3.6 Diagnostic Coverage of test and monitoring measures - DC

Effective self test inside the safety system allows to compensate for the poor reliability. According to ISO 13849-1 the quality of test is measured by the Diagnostic Coverage DC, namely the proportion of detected dangerous failures among all possible dangerous failures. To understand this concept it might be useful to look at the pie chart in figure 2.10, where is clarified the distinction between the different types of failures.

MTTF$_d$ of each channel	
Not acceptable	0 years $\leq$ MTTF$_d$ $<$ 3 years
Low	3 years $\leq$ MTTF$_d$ $<$ 10 years
Medium	10 years $\leq$ MTTF$_d$ $<$ 30 years
High	30 years $\leq$ MTTF$_d$ $\leq$ 100 years
Non-applicable	100 years $<$ MTTF$_d$

Table 2.3: Classification of the MTTF$_d$

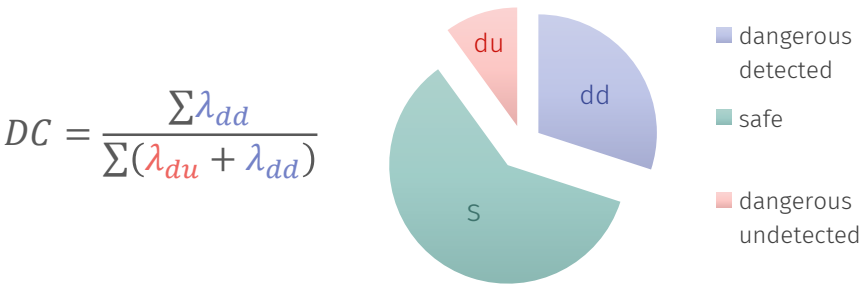


Figure 2.10: Classification of failures and definition of Diagnostic Coverage DC.

Diagnostic Coverage DC	
None	$DC < 60\%$
Low	$60\% \leq DC < 90\%$
Medium	$90\% \leq DC < 99\%$
High	$99\% \leq DC$

Table 2.4: Classification of the MTTF_d

The Diagnostic Coverage is thus defined as the rate of dangerous undetected failures divided by the rate of all dangerous failures, as figure 2.10 describes. The values of λ_{dd} and λ_{du} are determined through the FMEA analysis. Alternatively, a simplified method can be used:

Annex E of ISO 13849 contains a table that lists all the common detectable failures, and the tests needed to perform the detection. To each test is assigned a standard DC value (60%, 90% or 99%, see table 2.4), so that the block on which that test is performed takes on the corresponding Diagnostic Coverage. If no test is performed, the block has no Diagnostic Coverage and thus DC = 0%. Now, each block of the channel has a value of DC_j and $\text{MTTF}_{d,j}$, so the Diagnostic Coverage of the whole channel can be determined as a weighted average of the DC_j according to the formula:

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{d,1}} + \frac{DC_2}{MTTF_{d,2}} + \cdots + \frac{DC_N}{MTTF_{d,N}}}{\frac{1}{MTTF_{d,1}} + \frac{1}{MTTF_{d,2}} + \cdots + \frac{1}{MTTF_{d,N}}}$$

Other than the determination of the DC_{avg} value, some qualitative aspects must be also taken into account when dealing with the detection of failures, for example:

- After detection of a dangerous failure the safety system must initiate a safe state.
- The tests performed upon the SRP/CS must be initiated automatically.
- For Category 2 systems, the test must be performed with a frequency of at least 100 times greater than the frequency of the request upon the safety system. This enables to compensate for the single channel architecture.
- Each single block or component can be tested by several test procedures or test equipment (see Annex E of ISO 13849).

2.3.7 Measures against Common Cause Failure - CCF

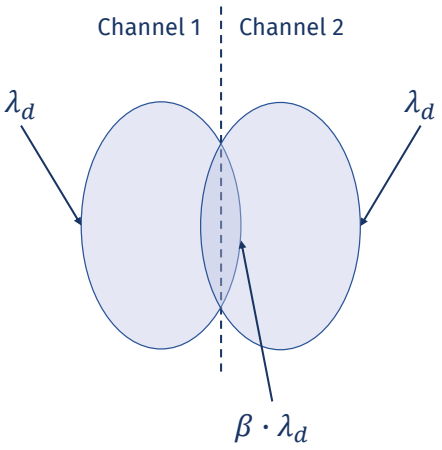


Figure 2.11: Illustration of Common Cause Failure (CCF) by means of the beta-factor model.

For a simplified quantification of the probability of failure, the final parameter concerns common cause failure, namely the failure of multiple channels due to the same initial event or situation. Given the probability of failure of two different channels, a portion of these failures has a common origin, as shown in figure 2.11. The rate of dangerous common cause failure in terms of failures per hour (1/h) can be calculated via the beta factor model, starting from the dangerous failure rate λ_d with the formula:

$$CCF = \beta \cdot \lambda_d \quad (1/h)$$

The β factor can be calculated via an FMEA analysis. When this would be too demanding for the task, another simplified approach can be used, for which a checklist is given in Annex F of ISO 13849. Each check gives certain points, the sum of which represents the resistance to common cause failure (with a maximum score of 100). With a score of 65/100 the β factor is estimated to $\beta = 2\%$, however the simplified procedure only requires that a minimum score of 65/100 is reached to consider the system resilient to common cause failure. An extract of the checklist is shown for clarity in table 2.5.

2.3.8 Combination of SRP/CS as subsystems

The safety function is often carried out by several SRP/CS arranged together in subsystems of different architectures and categories. Each subsystem is in turn very often part of a bigger system that comprises several subsystems, as shown in figure 2.12 (taken as an example from chapter 5.3).

In case the $\text{PFH}_{d,i}$ (Probability of dangerous Failure per Hour) of every subsystem is made available by the designer or manufacturer, the overall PFH_d of the whole system is calculated through the formula:

No.	Measure against CCF	Score
1	**Separation/ Segregation**	
	Physical separation between signal paths, for example: - separation in wiring/piping; - detection of short circuits and open circuits in cables by dynamic test; - separate shielding for the signal path of each channel;	15
2	**Diversity**	
	Different technologies/design or physical principles are used, for example: - first channel electronic or programmable electronic and second channel electromechanical hardwired; - different initiation of safety function for each channel (e.g. position, pressure, temperature); - components of different manufactures;	20

Table 2.5: Extract from table F.1 of ISO 13849-1, scoring process and quantification of measures against CCF.

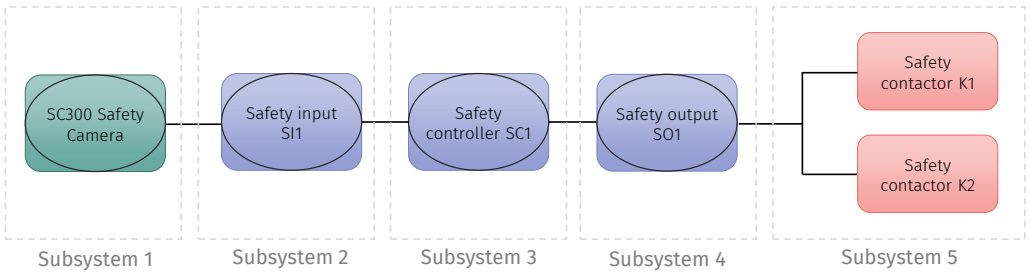


Figure 2.12: Example of combination of subsystems.

$$PFH_d = \sum_{i=1}^{N} PFH_{d,i} = PFH_{d,1} + PFH_{d,2} + \cdots + PFH_{d,N}$$

In case the $PFH_{d,i}$ is not available for every subsystem, a simplified approach can be used. It is based upon the Performance Levels PL of every subsystem, used as follows:

- the lowest PL of all subsystems is PL_{low}
- the number of subsystems with a Performance Level equal to PL_{low} is N_{low}
- the overall PL can be calculated with table 2.6 using PL_{low} and N_{low}

PL_{low}	N_{low}	Overall PL
a	≥ 4	No PL, not permitted
	≤ 3	a
b	≥ 3	
	≤ 2	b
c	≥ 3	
	≤ 2	c
d	≥ 4	
	≤ 3	d
e	≥ 4	
	≤ 3	e

Table 2.6: Simplified calculation of the PL for series arrangements of subsystems.

2.3.9 Computerization of the process

The simplified process here described can be automated by means of software applications or spreadsheets. One specific software however stands out for its completeness and ease of use. It is called SISTEMA (Safety Integrity Software Tool for the Evaluation of Machine Applications [25]) and it's developed by the IFA, an institute for research and testing of the German Social Accident Insurance in Germany. The IFA is also notified

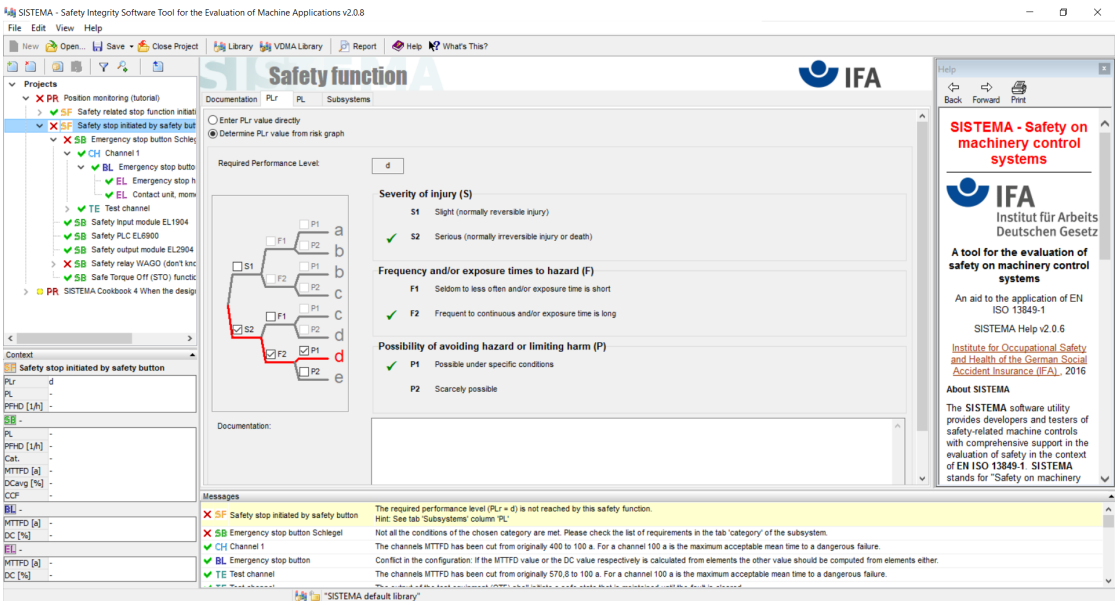


Figure 2.13: Screen capture of the graphical user interface of the software SISTEMA [25].

as testing and certification body for a number of test fields, for example the testing and certification of products and quality management systems for manufacturers [19].

The SISTEMA software utility provides developers and testers of safety-related machine controls with comprehensive support in the evaluation of safety in the context of ISO 13849-1. The tool enables to model the structure of the safety-related control components based upon the designated architectures, thereby permitting automated calculation of the reliability values with various levels of detail, including that of the attained Performance Level (PL).

Relevant parameters such as the risk parameters for determining the required performance level (PLr), the category of the SRP/CS, measures against common-cause failures (CCF) on multi-channel systems, the average component quality (MTTFd) and the average test quality (DCavg) of components and blocks, are entered step by step in input dialogs. Each parameter change is reflected immediately on the user interface with its impact upon the entire system. The final results can be printed out in a summary document. Particularly useful are the libraries, provided by the safety components' manufacturers, that contain all the useful data about the safety component or subsystem itself.

However, the software is made available free of charge, so the developers do not take responsibility for possible bugs or errors. A view of the software's user interface is shown in figure 2.13.

Chapter 3

The current safety systems

This chapter will describe the safety systems that are currently employed in two of the proANT AGVs, namely the proANT 436 and the proANT 490. The subdivision of this chapter follows the rule that every safety function must be considered independently. The main three safety functions (already presented in chapter 2.3.1) will then be introduced and described. For each safety function a block diagram of the safety system that performs the function will be created. Each component corresponding to a block of the system will then be described, stating all the necessary safety information and parameters. For the first subsystem of the first safety function, namely the emergency stop button subsystem, the calculation of the PFH_D will be carried out step by step. After the description of all the functions will be analyzed the cost of each safety component, leading to observations that will prepare the ground for the following chapters.

3.1 ProAnt 436 safety system

A safety system comprises of multiple safety functions, that need to be addressed separately as a standalone system (see section 2.3). The three safety functions that the basic version of proANT 436 carries out are:

- SF1 - Safe stop initiated by emergency button $PL_r = d$;
- SF2 - Safe stop initiated by laser scanner $PL_r = d$;
- SF3 - Dynamic safety field switch according to speed $PL_r = d$;

Every safety function has its own safety system that will be discussed below. However, some features are common to more than one function:

- On power failure, the engines stop and the AGV is halted.
- Both SF1 and SF2 bring the system into a safe state.
- The safe state corresponds to the activation of the Safe Torque Off (STO) performed by the servo driver card: the current to the motors is interrupted and the brakes are engaged.

Figure 3.1: Isometric view of the proANT 436. Emergency stop buttons are visible at the top of both columns.

SF1 - Safe stop initiated by emergency stop button

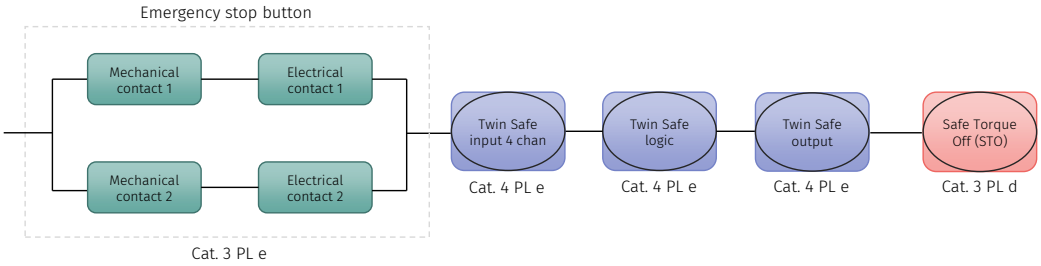


Figure 3.2: Safety system that performs the safety function 1

This safety function has a $\text{PL}_r = d$. The event that triggers the safe state is the actuation of one of the two emergency stop buttons present on both sides of the AGV, as visible in figure 3.1. The contacts of the buttons are monitored by a safety PLC (a Programmable Logic Controller with redundancy of elements and self-test functions) which triggers an output when the buttons are pushed. This output is connected to the servo drive card with the function of reliably stopping the motors. The following section will also have the secondary aim of giving an example of the simplified calculation of the PL in a subsystem.

Subsystem 1 consists of one emergency stop button. Despite the fact that two emergency stop buttons are present on the vehicle, the two systems are equal but independent from each other; for this reason, it is sufficient to analyze just one of the two. Each button is comprised of two components: an emergency stop head and a contact unit (figure 3.3). Also, each button has two electric contacts that are mechanically linked, so both the electrical and mechanical parts of each button can be seen as a two-channel configuration according to ISO 13849-1 2015 table C.1, note 3 "Each contact element (including the mechanical actuation) can be considered as one channel with a respective B10_D value". This architecture is congruent with Category 3 (when a single fault occurs, the safety function is always performed; some, but not all, faults will be detected; accumulation of undetected faults can lead to the loss of the safety function).

Both the emergency stop head and the contact unit are the two elements that constitute each channel of the first subsystem, namely the "emergency button" subsystem. To determine the performance level of this subsystem, the first step is to calculate the reliability of the single elements in terms of MTTF_d. This can be done for both the button head and the contact unit starting from the expected life B10, according to chapter C.4.2 of ISO 13849-1. For example, the manufacturer states that the life of the button head is $B_{10D} = 50000\ cycles$. Assuming that the buttons are pushed 10 times a day (extremely erring on the safe side) for 250 working days a year, the $n_{op} = 2500\ cycles/a$ can be used to calculate the MTTF_D with the formula C.1 of the norm:

Figure 3.3: Emergency-stop head for 16.2 mm mounting depth (Schlegel FRVKZ) and Contact unit (Schlegel PTSOOI) with 2 NC and 1 NO contacts.

$$MTTF_{D,E1} = \frac{B_{10D}}{0,1 \cdot n_{op}} = 400\ a$$

Similar calculations for the contactors result in $MTTF_{D,E2} = 4000\ a$. The next step is calculating the MTTF_D of the entire block, starting from the single elements. This can be done with the formula:

$$MTTF_{D,BL} = \frac{MTTF_{D,E1} \cdot MTTF_{D,E2}}{MTTF_{D,E1} + MTTF_{D,E2}} = 363\ a$$

Although it may not be immediately clear, this formula is simply the summation of the probability of failure of the two elements of the block. In fact, the MTTF_D has been introduced as the reciprocal of the probability of dangerous failure λ_D (failure per hour). These values can be summed up, thus for the whole block $\lambda_{D,BL} = \lambda_{D,E1} + \lambda_{D,E2}$, and applying the substitution $\lambda_D = 1/MTTF_D$ results in the above-mentioned formula.

Then, the $\text{MTTF}_{D,1}$ and $\text{MTTF}_{D,2}$ of the two channels are symmetrized into one value, that will be the final MTTF_D of the whole subsystem. In this case, being the two channels equal, symmetrization is not needed, and the calculated MTTF_D is capped to 100 years according to the norm. The formula for calculating the symmetrized MTTF_D is given for completeness:

$$MTTF_D = \frac{2}{3}\left[MTTF_{D,C1} + MTTF_{D,C2} - \frac{1}{\frac{1}{MTTF_{D,C1}} + \frac{1}{MTTF_{D,C2}}}\right]$$

The Diagnostic Coverage is also determined by a simplified method, following the indications of table E.1 "Examples of Diagnostic Coverage (DC)" in ISO 13849-1. In this case,

each of the two channels is cross-monitored within the PLC, giving a $DC = 90\%$ equal for both channels, that results in a $DC_{avg} = 90\%$ for the whole subsystem (according to the formula presented on page 19).

Next, Common Cause Failure is addressed. The subsystem is able to withstand the occurrence of CCF mainly through 5 measures, that score a total of 70 points:

- Physical separation between signal paths, separation in wiring, sufficient clearances and creepage distances on printed-circuit boards (15 points)
- Protection against over-voltage (15 points)
- Components used are well-tried (5 points)
- Prevention of contamination and electromagnetic disturbances (EMC) to protect against common cause failures in accordance with appropriate standards, e.g. IEC 61326–3-1 (25 points)
- Consideration of the requirements for immunity to all relevant environmental influences such as temperature, shock, vibration, humidity as specified in relevant standards (10 points)

Now, all the data for the calculation of the PFH_D is available. This can be done with table K.1 of ISO 13849-1, entering with Cat. 3, $\mathrm{MTTF}_D = 100$ and $\mathrm{DC}_{avg} = medium$. The result is a $\mathrm{PFH}_D = 4,29 \cdot 10^{-8}$, perfectly in line with the requirements.

The rest of the chain is made of enclosed subsystems, for which the manufacturer states all the safety performance levels and further safety details. This is particularly common when dealing with complex electromechanic machines such as AGVs, since the usage of safety-rated components saves time and money in the creation of a complex safety system.

Subsystem 2 is the input module of the modular Safety PLC, which meets the requirements of Cat. 4, PL e. The two different contacts of each emergency stop button are connected to this module, so that the built-in test functions can be used to detect random wiring faults. The specific module is the Beckhoff EL1904, shown in figure 3.4 with a description of the various contacts and LEDs.

Subsystem 3 is the logic of the modular safety PLC, complying with Cat. 4 PL e. The logic of all the safety system can be here programmed, using ready-made, pre-certified function blocks. This allows a very easy and fast programming of the PLC, as well as skipping the software validation, a procedure that can be very slow and expensive. In fact, safety functions such as emergency stop, safety door monitoring, two-hand control and more can easily be selected and linked. All blocks can be freely connected among each other and are complemented by operators such as AND, OR, etc. [26]. The required functions are configured via the TwinCAT System Manager and loaded into the EL6900 TwinSAFE Logic via the fieldbus. An image of this module, the Beckhoff EL6900 is

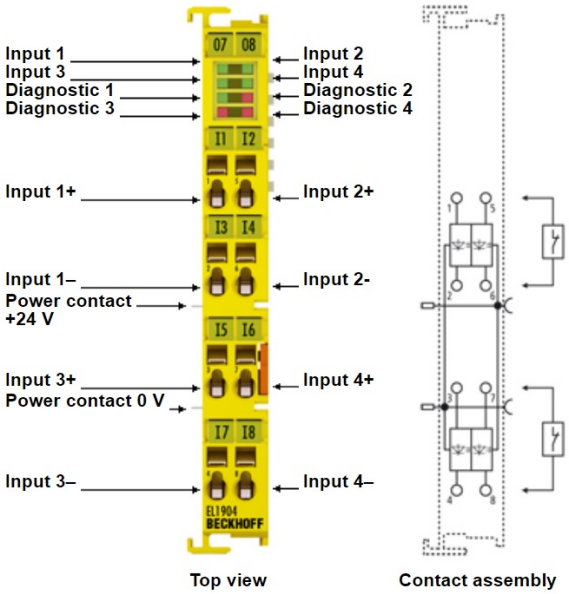


Figure 3.4: Beckhoff EL1904 input module

shown in figure 3.5.

These elements tend to be rather expensive, with prices higher than two or three times their non safety-rated counterparts. Such prices are due to the high reliability of the components, as well as the redundancy of internal connections and the self-testing functions implemented in the circuits. However, part of the cost is to be located within the various tests and certifications that make these products highly reliable in a safety system.

Subsystem 4 is the last module of the modular safety PLC, namely the output module. This is a Beckhoff EL2904, which meets, as all the other safety PLC modules, the requirements of Cat. 4 PL e. Similarly to the input module, here the built-in test functions can be used to monitor the state of the elements connected to it. Figure 3.6 shows this module.

Subsystem 5 is the last element of the safety chain. When an emergency stop is triggered, the output module of the safety PLC sends a digital signal that commutes the STO (Safe Torque Off) input of the servo drive card. It must be pointed out that the servo driver card is not safety-certified itself, but the whole STO system complies with Cat. 3 PL d, so that it is possible to treat it as an enclosed subsystem, as done with the safety PLC components. The Beckhoff EL7201 Servomotor terminal is shown in figure 3.7.

The Safe Torque Off function simply consists in cutting the power supply to the motors,

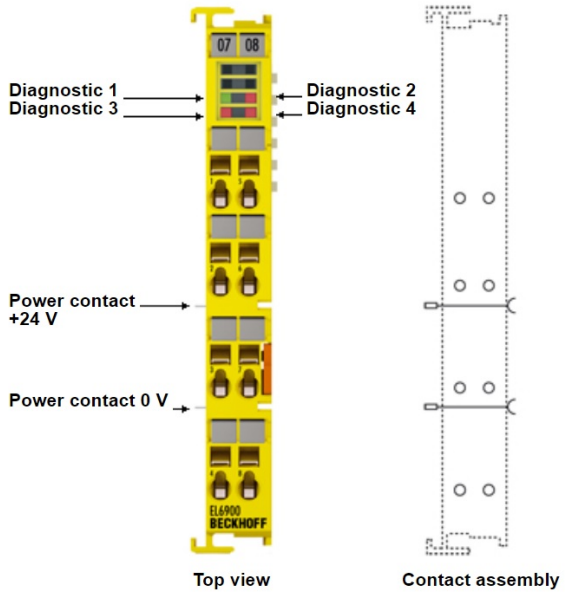


Figure 3.5: Beckhoff EL6900 logic module

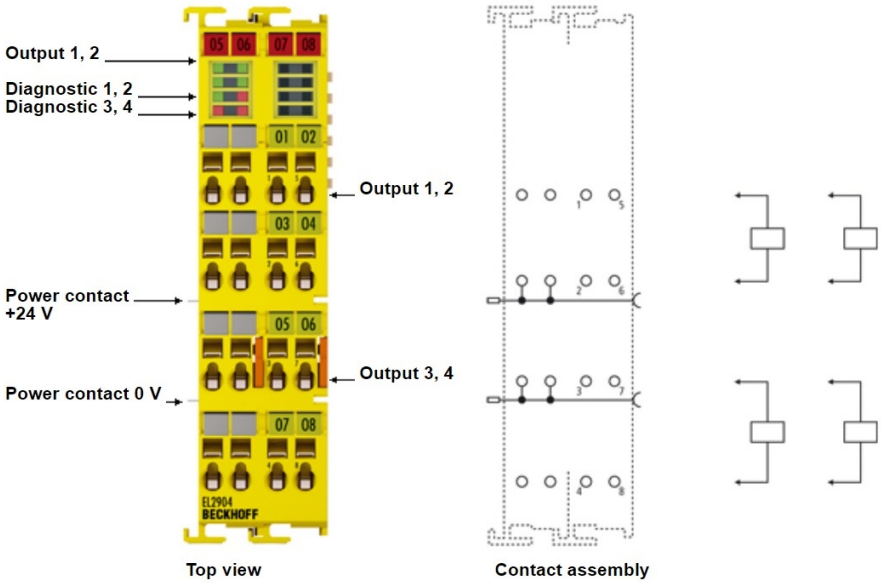


Figure 3.6: Beckhoff EL2904 output module

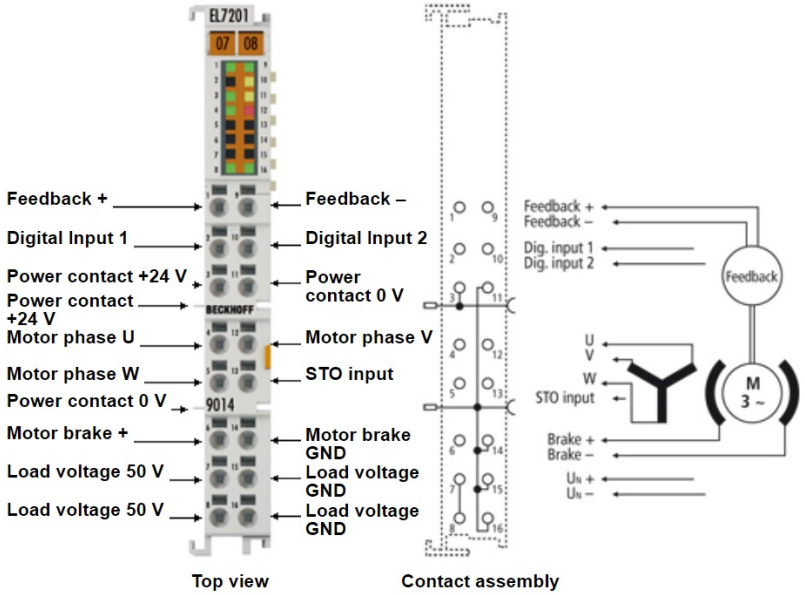


Figure 3.7: Beckhoff EL7201 - 9014 Servomotor terminal with OCT and STO.

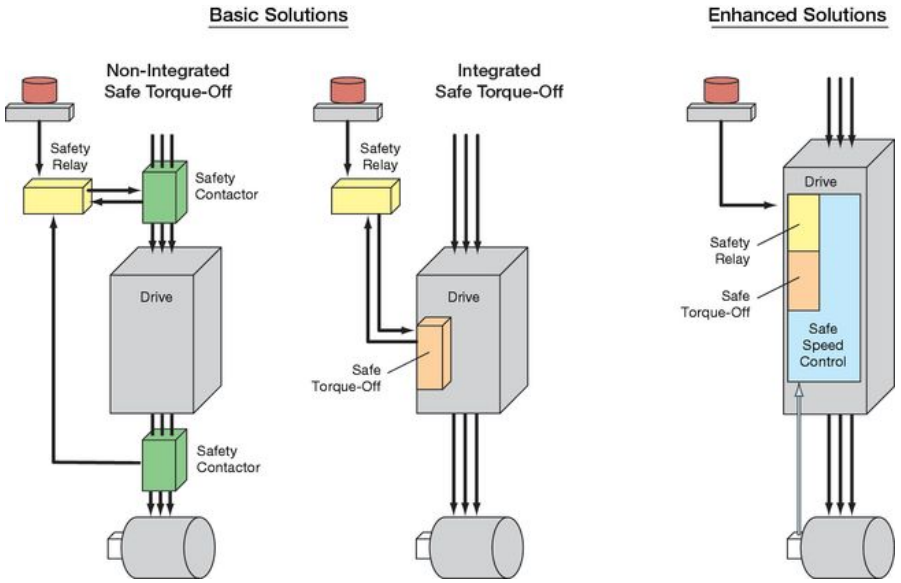


Figure 3.8: Scheme of the evolution of the STO function, from the most basic (left) to the most recent and advanced solutions (right).

making sure that no torque-generating energy can continue to act upon the actuators and preventing unintentional starting, in a reliable fail-safe way [4]. Originally this was done with two safety contactors actuated by a safety relay (figure 3.8) that took out the power of the motors. However, this method could bring to the loss of position data since the drive is shut down completely. Placing contactors between the drive and the motor solved this problem, but interrupting the power supply would sometimes cause the drive stage of the servo controller to blow up if the switch-off happened with the motor running and under high load. To solve this, current servo drives are manufactured with integrated safety relays, contactors and other components that make the STO function. Ultimately, STO is a state where the drive is reliably torque-free. A similar procedure subsequently engages the brakes, bringing the AGV to a stop.

After describing all the subsystems and calculating the PFH_D for each of them (or reading it from the manufacturer's datasheet) it is possible to calculate the PL reached by the overall system together with the overall PFH_D. This can be done simply by summation of the $\text{PFH}_{D,i}$ of every subsystem (formula in section 2.3.8), or with the simplified method based on the single PL of each subsystem, in case not all PFH_D values are available. In the end the system has a PL d and $\text{PFH}_D = 3.4 \cdot 10^{-7}\ 1/h$.

SF 2 - Safe stop initiated by laser scanner

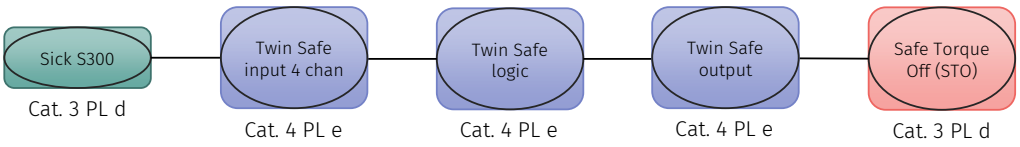


Figure 3.9: Safety system that performs the safety function 2

This safety function has a $\text{PL}_r = d$. If the safety field of the laser scanner is harmed, the system enters the safe state, removing the torque to the motors and halting the AGV. This is achieved via digital channels of communication between the Sick S300 Laser scanner and the safe PLC.

Subsystem 1 is then the laser scanner, namely the Sick S300 Expert shown in figure 3.10 [23]. This sensor belongs to the family of the Electro-sensitive protective equipment, specifically the active optoelectronic protective devices responsive to diffuse reflection. These are protective devices that use optoelectronic sender and receiver elements to detect the reflection of optical radiation generated by the protective device itself. This reflection is generated by an object in a predefined two-dimensional area. Detection is signaled by a signal change (OFF state) to its output signal switching devices (OSSDs).

These signals from the OSSDs are used as input to the safe PLC.

Figure 3.10: SICK 300 laser scanner (left) installed on the proANT 436

The scanner has a field of view of 270° and it's placed at a height of 12 cm from the floor, so it can scan the environment just at this height. For this purpose the laser scanner is mounted upside-down. This feature is of crucial importance since the safety system has to detect (according to EN 1525) the leg of a person laying down on the floor. Therefore, it is crucial that every object shorter than 12 cm is removed from the path of the robot, or added to the map. Also, hanging objects like forklift forks need to be removed from the path.

Additionally, the field of view of the laser scanner allows the sides of the AGV to be partly covered by the laser beams. This is possible since the space around the sensing head of the scanner is free, so the shape of the achievable safety field is shown in figure 3.11.

A safety laser scanner is an optical sensor which monitors a hazard zone on a machine or vehicle by scanning the area around it on a single plane with infrared light beams. It works on the principle of time-of-flight measurement, figure 3.12. The scanner sends very short light pulses (S) while an "electronic stopwatch" runs simultaneously. If the light strikes an object, it is reflected and received by the scanner (R). The scanner calculates the distance from the object from the difference between the send and receive times. A uniformly rotating mirror (M) in the scanner deflects the light pulses such that a sector

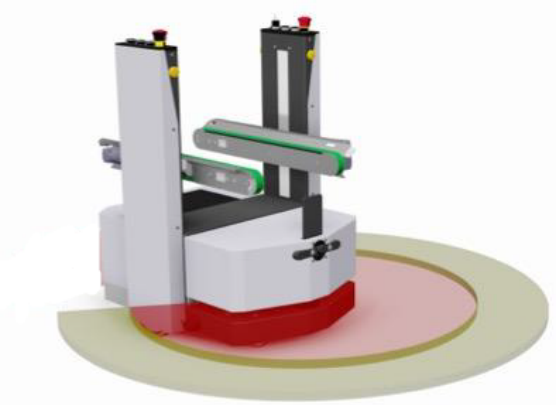


Figure 3.11: Shape of the achievable safety field

of a circle is covered. The scanner then determines the exact position of the object from the measured distance and the angle of rotation of the mirror.

Safety laser scanners use individually emitted pulses of light in precise directions and do not continuously cover the area to be monitored. Resolutions (detection capabilities) between 30 mm and 150 mm are achieved through this operating principle. With the active scanning principle, safety laser scanners do not need external receivers or reflectors.
The user can program the area in which object detection trips the protective field. State-of-the-art devices allow multiple areas to be monitored simultaneously and switching between these areas during operation. This feature will be used in this case to adapt the monitored area to the speed of the vehicle.

Due to their construction comprising high precision rotating parts, mirrors and internal sensors, these elements tend to be very expensive, as analyzed in section 3.1.1. Part of the cost is however to be attributed to the various tests and certifications that make these products comply with the requirements of DIN EN ISO 13849-1:2008 (Cat 4, PL e) and IEC 61508:2010 (SIL 3). As a matter of fact, not only high reliability, but also redundant architectures and self testing equipment make safety laser scanners suitable for purposes in which the lives of the people are at risk.

With the current developments in the field of autonomous driving vehicles, Lidar technology is experiencing a growing rate faster than ever, thus more and more companies bring their solutions to the table. A fundamental aspect to be considered is however the discrepancy between safety of machinery and safety on public streets, which is regulated differently. For this reason self-driving cars have a great redundancy of sensors and powerful computation systems that take care of blending together all the data from different sensors and sensor technologies.

As an example, figure 3.13 shows the setup used for autopilot function in new Tesla cars.

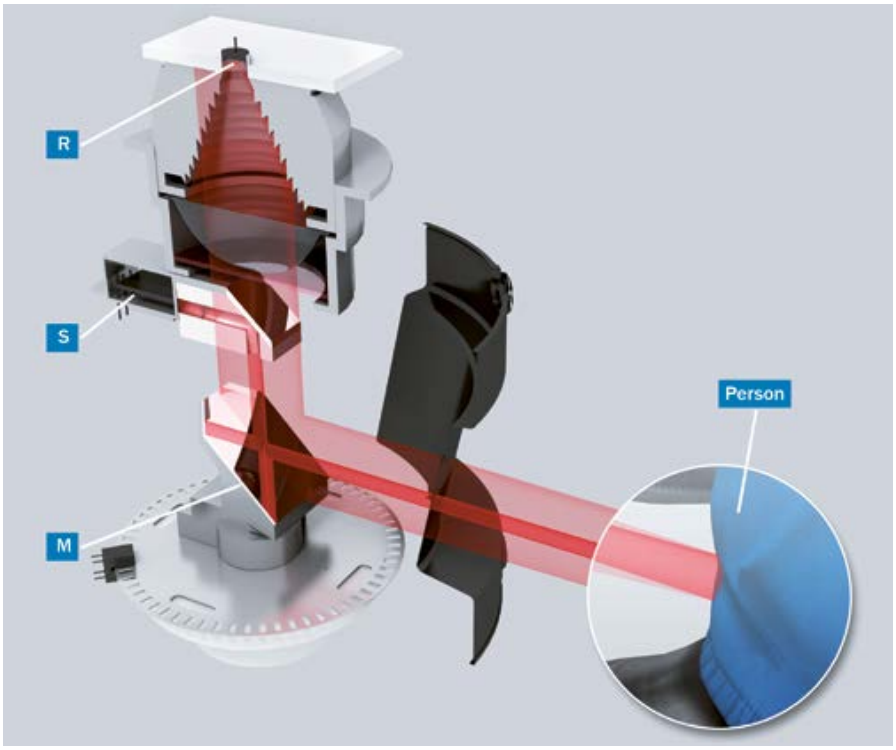


Figure 3.12: Basic structure of a laser scanner.

The autopilot hardware suite consists of 8 cameras, 1 radar, ultrasonic sensors and a new supercomputer to support its "Tesla Vision" end-to-end image processing software and neural net. The main forward camera covers a distance of 150 m with 50° field of view, aided by a narrow 35° camera, a wide 150° camera and a 160 m range radar. Two forward looking and two rearward looking side cameras complete the 360° visual coverage, enhanced by a wide angle 50 m range rear view camera. Finally, all-round ultrasonic sensors cover the proximity of the vehicle up to 8 m, allowing precise maneuvers in tight spaces [28].

Tesla is however one of the few car manufacturers that don't use Lidar in their autonomous driving systems.

Subsystems 2, 3, 4 and 5 are the same as the previous safety function. The laser scanner activates the safe state when triggered, similarly to how the emergency stop button triggers the safe state when pushed. In this case, every component is an encapsulated subsystem for which the manufacturer certifies all the required safety features, so that the overall performance level can be calculated according to section 2.3.8. In the end, a PL d ($\text{PFH}_D = 4 \cdot 10^{-7}\ 1/h$) has been reached.

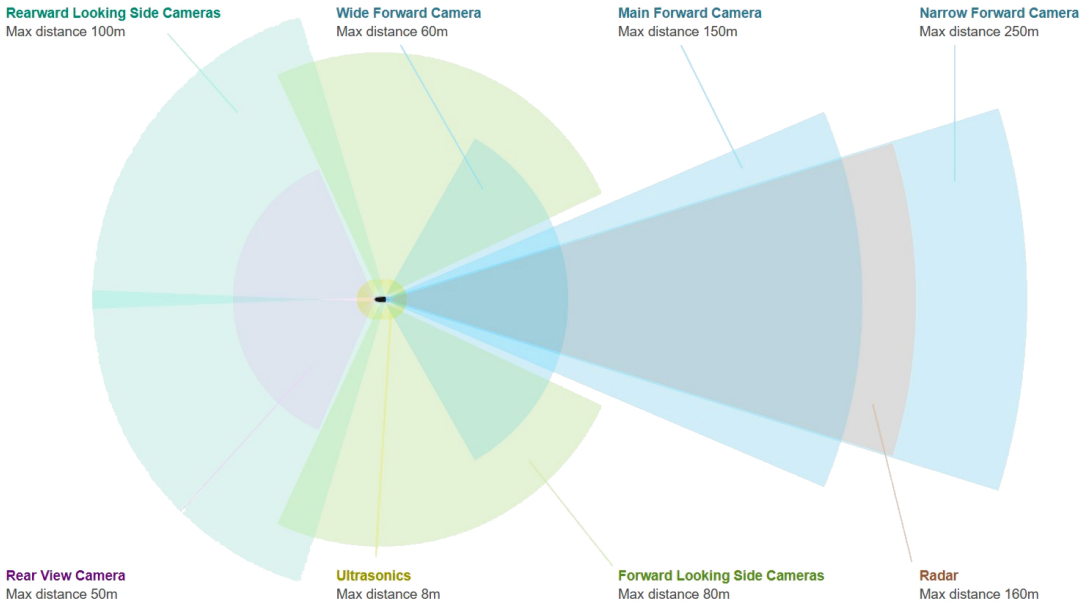


Figure 3.13: Sensor suite on newest Tesla cars.

SF 3 - Dynamic safety field switch

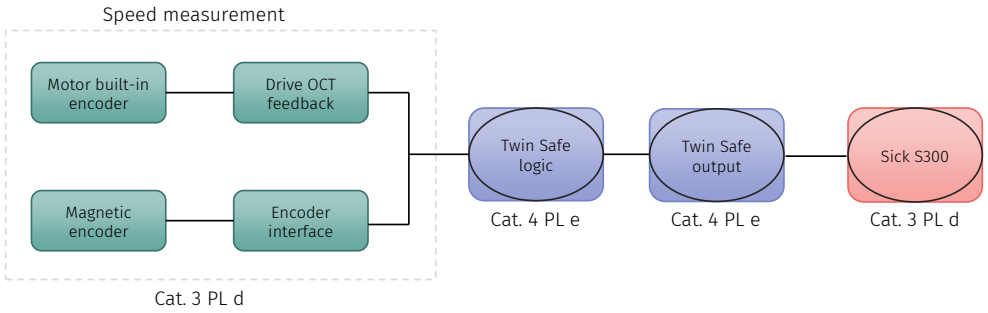


Figure 3.14: Safety system that performs the safety function 3

One of the main features of every proANT AGV is the advanced natural navigation system. When cruising through a plant and navigating naturally, the vehicle is subject to route changes, obstacles and twisty paths, thus the velocity of the robot is constantly changing. It is then of great importance that the safety field of the laser scanner discussed in the above chapter is switched dynamically according to the speed of the robot. This allows a greater flexibility and improved performance of the robot, due to the constant adaptation of the distance at which the laser scanner is triggered.

Additionally, without this feature it would be virtually impossible to perform, for ex-

ample, obstacle avoidance in narrow pathways, because the safety field would be easily harmed. This is better explained in figure 3.15.

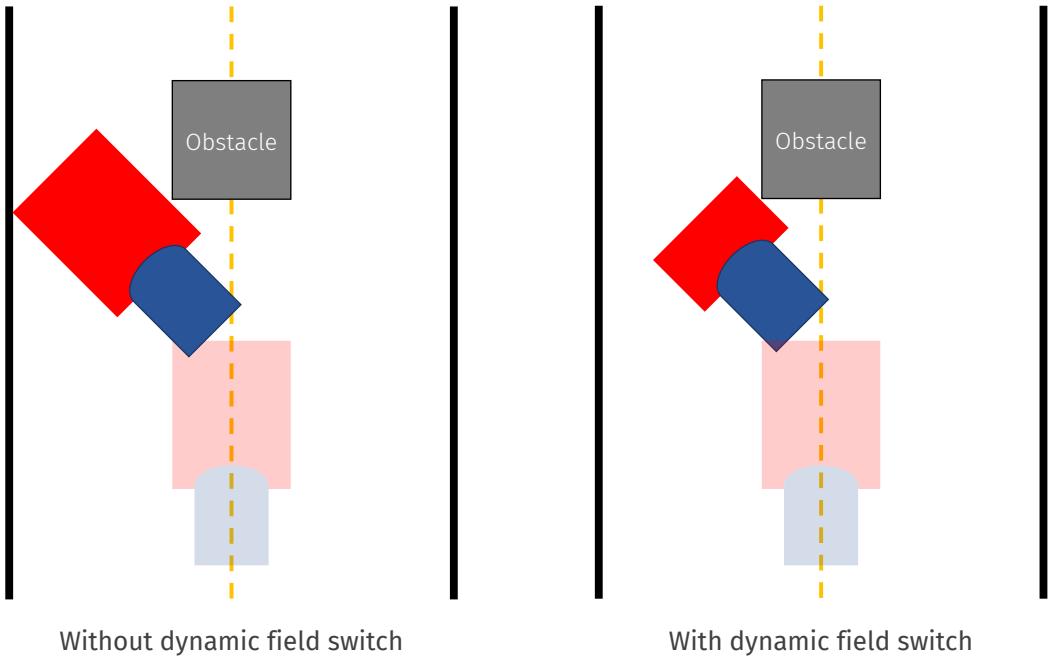


Figure 3.15: The capability of switching the safety fields of the scanner dynamically according to the speed allows the AGV to avoid obstacles in tight spaces.

The yellow dashed line represents the path of the robot (in blue), while the red area represents the safety field. Before approaching the obstacle, the robot cruises at a speed up to 1.5 m/s and the safety field covers a reasonably long area in front of the vehicle. When an obstacle is detected, the AGV slows down. Without the safety field switching, it would be impossible for the robot to navigate around the obstacle because its safety field would be triggered and the emergency stop would be activated. However, if the safety field is shortened when driving at lower speeds, the vehicle can easily skew the obstacle if there's enough room for the maneuver.

Subsystem 1 is then the speed measurement input. It consists of two channels arranged in a Category 3 subsystem, to calculate a safe speed measurement out of two unsafe signals. The first channel is the feedback of the servomotor: the AM8111 Beckhoff servomotor in figure 3.16 features the OCT (One Cable Technology), meaning that the built-in feedback system (normally an encoder) can be connected to the servo drive card. In our case, the Beckhoff EL7201-9014 servo drive card is used, as described in the previous systems and shown in figure 3.7. From here the speed value can be sent to the safe logic. The second channel consists of an external Magnetic incremental encoder from Kübler, shown in figure 3.17.

Figure 3.16: Beckhoff AM8111 three-phase servomotor with OCT technology.

Figure 3.17: Magnetic encoder Kübler RLI20.

An optical encoder uses light (optics) to identify unique positions for the encoder. A magnetic encoder uses the same principle to determine a position as an optical encoder, but it does it using magnetic fields rather than light. It consists of a rotating disk with a number of magnetized poles around its circumference, and a sensor that detects the changes in magnetic field. The poles in the disk, which is mounted on the rotating shaft, provide the code pattern useful to determine the position of the wheel and, in turn, its speed. A schematic representation of this principle is shown in figure 3.18.

The signal from the encoders is sent to the input channel of the Encoder interface module EL5101. The speed is calculated and then sent to the safe PLC for speed comparison.

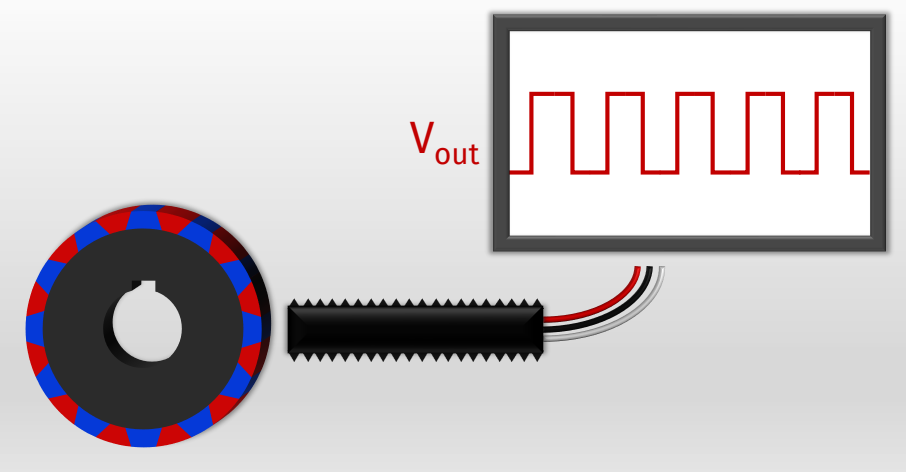


Figure 3.18: Schematic components of a magnetic incremental encoder based on inductive pickup.

If the difference between the two speed values exceeds 10% the system is declared faulty and the safe state is entered. The capability of fault detection in a two-channel configuration makes this a Category 3 subsystem.

Subsystems 2 and 3 are the logic. In this case the safe input module is not used since the information is already available in the PLC for the calculations to be made. Lastly, **subsystem 4** is the Sick S300 laser scanner, which is the output of the safety function. Here, 4 digital inputs allow $2^4 = 16$ combinations and thus 16 safety fields can be switched accordingly. On the actual system however, only 4 safety fields are used, for which 2 digital inputs are sufficient. These 4 fields (one of which is fundamentally a muting function) are associated to the speed according to table 3.1 and shown in figure 5.2.

Field	Speed (m/s)	Coverage in driving direction (cm)	Lateral coverage from scanner position on each side (cm)
1	$0 \leq v \leq 0.29$	0	0
2	$0.3 \leq v \leq 0.59$	63	50
3	$0.6 \leq v \leq 0.99$	90	50
4	$1 \leq v \leq 1.49$	120	50

Table 3.1: Safety field sizes according to the speed of the AGV

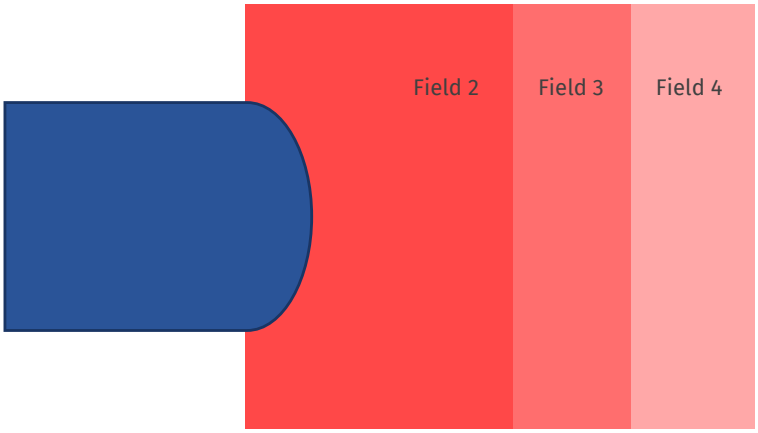


Figure 3.19: Schematic representation of the sizes of safety fields.

3.1.1 Cost of the system

This section will be dedicated to the cost analysis of the components involved in the safety system. From now on, with the term "safety system" it will be indicated the system that allows the execution of all 3 safety functions. Subsequently, since more safety functions have in common one same component, that exact component will (reasonably) not be present in greater quantity than strictly necessary. The following pie chart highlights the prices and relative weight of the cost of each component.

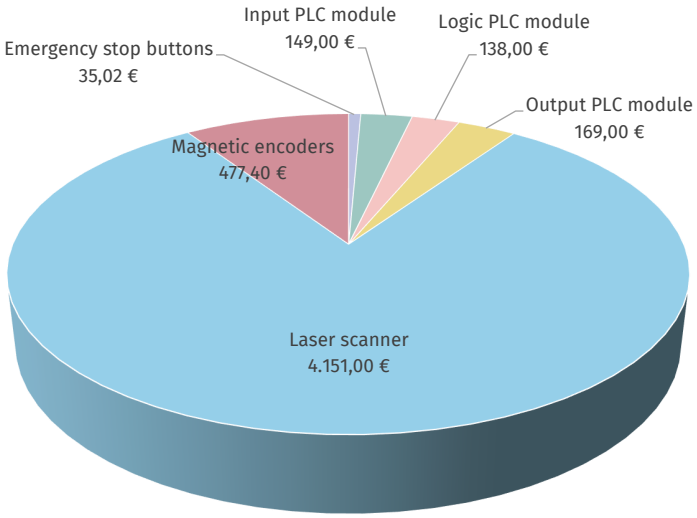


Figure 3.20: Cost of the safety components and relative impact on the cost of the whole safety system. The cost of the whole system, or the sum of each slice of the pie, is 5119,42€.

It is immediately visible that the biggest slice of the pie is taken by the laser scanner. This shouldn't surprise much, since the technology and precision of this instrument have been already discussed in the previous chapters. Despite being the most expensive, this is not an easily replaceable component of the safety system. Moreover, the same piece of instrument is used to perform SLAM (Simultaneous Localization And Mapping) for natural navigation, which is one of the strengths of the company's AGVs.

The other important part of the cost is due to the safety PLC. This comprises two input modules, the logic module and two output modules, with similar price ranges per item. Due to their construction and certifications, these components have prices at least 200% higher than the non-safety equivalents, so they make about one fourth of the overall safety system cost. The safety PLC could theoretically be eliminated, with savings around 700€ per AGV, employing other methods for the safety functions that it currently covers:

- SF1 can be easily performed without a PLC utilizing a hardwired relay system. As a matter of fact, the PLC evolved from the relay circuits improving the flexibility and the logic possibilities. However, the safe stop of a machine by emergency stop button is a rather easy task to accomplish for a wired relay system, as there's no need for elaborate software.
- SF2 requires bypassing the PLC and interfacing the OSSDs of the laser scanner directly with the STO digital inputs of the servo drive, which need to be connected to the emergency stop buttons relay system as well. This is a tricky task and would require some research and experimentation.
- SF3 could be potentially easier since some of the latest laser scanners include an encoder evaluation module built in their system. This will however need more research: one of the problems is that when an AGV is performing a rotation around its axis, the speed detected from the encoders is not zero, so the safety fields will be erroneously activated, bringing the vehicle to an emergency stop if it's inside a tight area.

Next, the magnetic encoders appear to be rather expensive as well. Their working principle is fairly simple and has been discussed above, however the main advantage compared to optical encoders is the greater robustness to wear, dust and interference. The necessity of having a pair of redundant encoders lies in the fact that the feedback system of the motors is not safety-rated, so it can't provide an input signal which is reliable enough for the speed evaluation (and thus the safety field switch). For this reason, a two-channels architecture shall be used.

It is theoretically possible to use a single safe encoder per motor, so that the speed signal is already compliant with ISO 13849. This is the case with the encoder shown in figure 3.21. It is an optical encoder made by SICK and complying with PL d, which is the

minimum acceptable for the safety system in which it's used. Its IP65 level of protection ensures resistance to dust and water splashes, which is necessary when used on an AGV. However, these encoders are available at a list price around 400€ per item, more than double the price of both currently employed magnetic encoders.

Figure 3.21: Sick safety encoders DFS60S Pro, Cat. 3 PL d.

The benefits of using a pair of safety encoders are however limited by the fact that the servomotors themselves have already a feedback system. The three-phase AC synchronous servomotors come with a built-in feedback that plugs into the servo driver card and is used for the motor control. This is called OCT (One Cable Technology) and features an incremental encoder integrated in the servomotor housing. For this reason, one channel of the speed detection subsystem is already built in the servomotors, so the second channel doesn't need to be safety-certified. It then seems that the usage of non-safety rated encoders is sufficient for the application, however one last consideration can be made. As seen before, if function SF 3 has to be performed without a safety PLC, two encoders can be connected directly to the laser scanner. For this reason, having safety encoders is necessary to maintain a high performance level.

Lastly, the emergency stop buttons complete the pie chart. These components are a fundamental part of the safety system and cannot be substituted under any circumstance.

3.2 proANT 490 safety system

The three safety functions that the basic version of proANT 490 carries out, similarly to what seen before with proANT 436, are:

- SF1 - Safe stop initiated by emergency button $\mathrm{PL}_r = d$
- SF2 - Safe stop initiated by laser scanner $\mathrm{PL}_r = d$
- SF3 - Dynamic safety field switch according to speed $\mathrm{PL}_r = d$

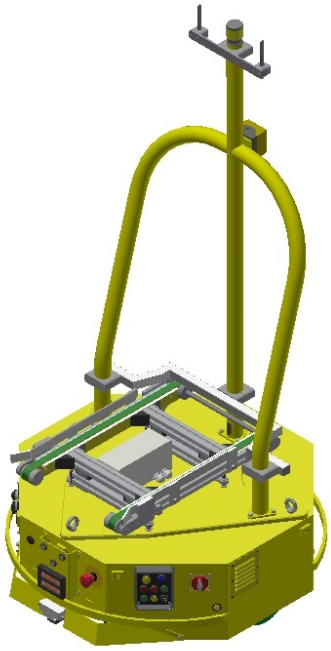


Figure 3.22: Isometric view of the proANT 490. The emergency stop button is visible on the front of the vehicle.

Every safety function has its own safety system that will be discussed below. However, some features are common to more than one function:

- On power failure, the engines stop and the AGV is halted
- Both SF1 and SF2 bring the system into a safe state
- The safe state corresponds to the activation of the Sick FlexiSoft Safety Relays, that interrupt the current to the motors servo drive and activate the brakes.

SF1 - Safe stop initiated by emergency button

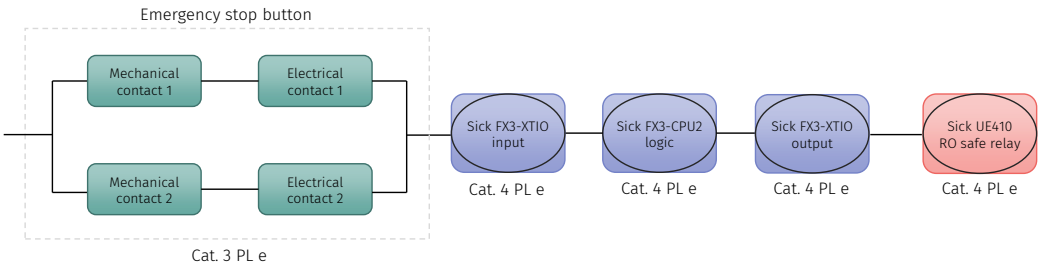


Figure 3.23: Safety system that performs the safety function 1

This safety function has a $PL_r = d$. The event that triggers the safe state is the actuation of the emergency stop button present in front of the AGV, as visible in figure 3.22.

Subsystem 1 consists of one emergency stop button, made of two elements: the emergency stop head and the contact unit (figure 3.24). The two electric contacts are mechanically linked to the button, so both the electrical and mechanical parts of each button can be seen as a two-channel configuration according to ISO 13849-1 2015 table C.1, note 3 "Each contact element (including the mechanical actuation) can be considered as one channel with a respective $B10_D$ value". This architecture is congruent with Category 3 (when a single fault occurs, the safety function is always performed; some, but not all, faults will be detected; accumulation of undetected faults can lead to the loss of the safety function).

The calculation of the PFH_D follows the same steps that have been discussed for the proANT 436 system, and will not be here repeated. The rest of the chain is made of enclosed subsystems of which the manufacturer states the safety performance levels and further details.

Subsystem 2 and **Subsystem 4** differ only by their function, while the module is just one, the Sick FX3-XTIO input/output module. The two separate blocks in the block diagram serve the only purpose to clarify the logical chain. This module presents 8 safety

Figure 3.24: Emergency-stop mushroom pushbutton (Siemens 3SU1000-1HB20-0AA0) and Contact units (Siemens 3SU1400-1AA10-1HA0).

inputs, 4 safe outputs and 2 test outputs. The module meets the requirements of Cat. 4, PL e. The two different contacts of the emergency stop button are connected to this module, so that the built-in test functions can be used to detect random wiring faults. Figure 3.25 shows this module.

Figure 3.25: Sick FX3-XTIO input/output module.

Subsystem 3 is the main module of the PLC, which contains the logic and general function blocks. It's the model FX3-CPU2 shown in figure 3.26 (left) and complying with Cat. 4 PL e. Application-specific function blocks are also available, simplifying the programming work and reducing the time and cost of certification.

Subsystem 5 is connected to the outputs of the I/O module and consists of a safe relay module, the Sick UE410-4RO4 shown in figure 3.26. It features 4 outputs (enable current contacts) as well as 2 control inputs and 2 contactor monitoring contacts. This module contains the relays that cut off the current to the servo drives, allowing a safe stop of the vehicle subsequent to the engaging of the brakes. This way of stopping the vehicle is compatible with the STO (Safe Torque Off) stop.

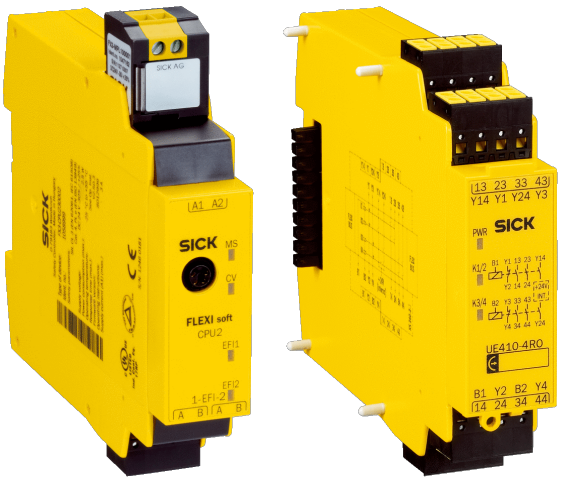


Figure 3.26: Sick FX3-CPU2 logic module (left) and Sick UE410-4RO4 safe relay module (right).

After describing all the subsystems and calculating the PFH_D for each of them (or reading it from the manufacturer's datasheet) it is possible to calculate the PL reached by the overall system together with the overall PFH_D. This can be done simply by summation of the $PFH_{D,i}$ of every subsystem (formula in section 2.3.8), or with the simplified method based on the single PL of each subsystem, in case not all PFH_D values are available. In the end the system has a PL e and $PFH_D = 2.9 \cdot 10^{-8}\ 1/h$.

SF2 - Safe stop initiated by laser scanner

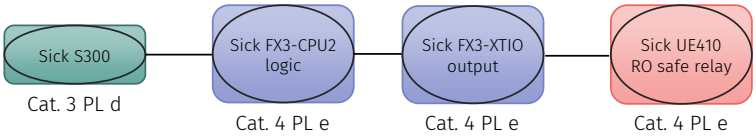


Figure 3.27: Safety system that performs the safety function 2

This safety function halts the AGV when an obstacle is detected from the laser scanner, with a safety performance level of PL_r = d. The laser scanner and the safety PLC are produced by the same manufacturer, so they reach a good level of integration and they are particularly easy to fit together.

Subsystem 1 is again the Sick S300 laser scanner, the optical sensor that monitors the area surrounding the front part of the AGV. It has been extensively discussed within the proANT 436 system, on page 35. **Subsystems 2, 3 and 4** are the same as the previous safety function. The laser scanner activates the safe state when triggered, similarly to

how the emergency stop button triggers the safe state when pushed. In this case, every component is an encapsulated subsystem for which the manufacturer certifies all the required safety features, so that the overall performance level can be calculated according to section 2.3.8. In the end, a PL d ($\text{PFH}_D = 8.4 \cdot 10^{-8}\ 1/h$) has been reached.

Additionally, the laser scanner must send data to the IPC for navigation. This function requires an additional module, the FX0-GCAN CANopen Gateway. Data is transferred indeed via CANopen industrial network at speeds up to 1000 kbit/s. However this module isn't strictly related to the safety system, so it will not take part on the cost calculation.

SF3 - Dynamic safety field switch

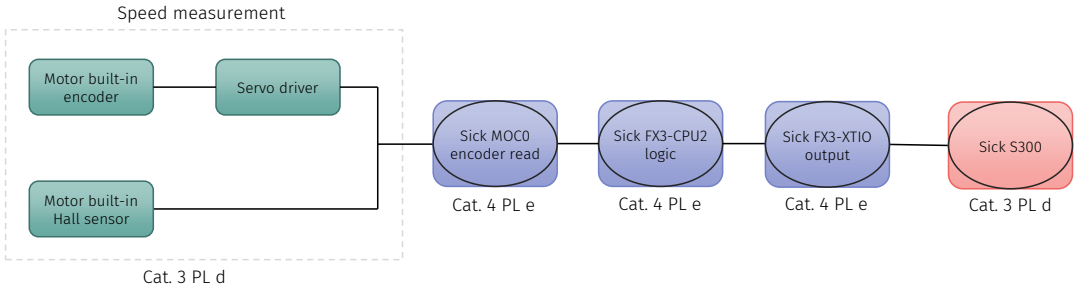


Figure 3.28: Safety system that performs the safety function 3

The safety field switch function is a very important part of the safe navigation of the AGVs. A fatal error, and the effects could be irreversible: if the safety field is too small for the speed of the vehicle, the emergency stop will not be triggered soon enough, and a crash will occur with the obstacle. On the other hand, a too big safety field compared to the speed of the robot restricts its freedom of movement, as seen on page 37.

Subsystem 1 is the speed measurement input. It consists of two channels arranged in a Category 3 subsystem, to calculate a safe speed measurement out of two unsafe signals. The pair of sensors are already pre-installed in the servomotors, and consist of an optical encoder and a Hall-effect speed sensor. The latter is a sensor made of two main components: a toothed gear connected to the rotating shaft of which the speed must be measured, and a Hall-effect probe that gives a digital output when the magnetic field in front of it is modified. Picture 3.29 should clarify this structure.
The sensor is fundamentally a proximity sensor, of which the working principle is schematized in figure 3.30. It contains a metal plate with excitation current passing through it and a magnet. When one of the ferromagnetic gear's teeth get close enough to the sensor, the magnetic field is modified and thus the electrons passing through the metal plate are deviated. This creates (or modifies) a potential difference between the two sides of the plate that are not connected to the excitation wires. The variation of this potential difference is in the realm of a few μV, thus operational amplifiers are used to

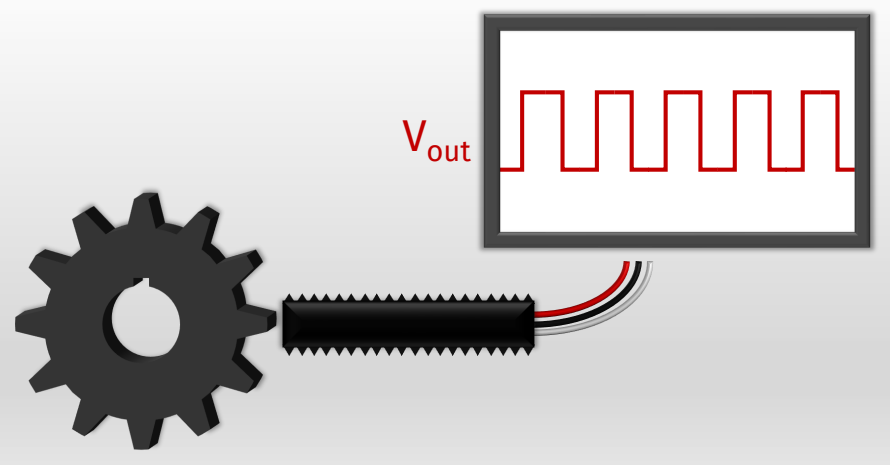


Figure 3.29: Hall sensor speed measurement setup.

increase this value. Additionally, a Smith trigger is used to further amplify and digitize the signal, so that a square wave like the one on the above figure is outputted. If p is the number of recorded peaks in one minute, and z is the number of teeth of the gear, the angular speed of the shaft is calculated with the formula:

$$n = p/z \ (rpm)$$

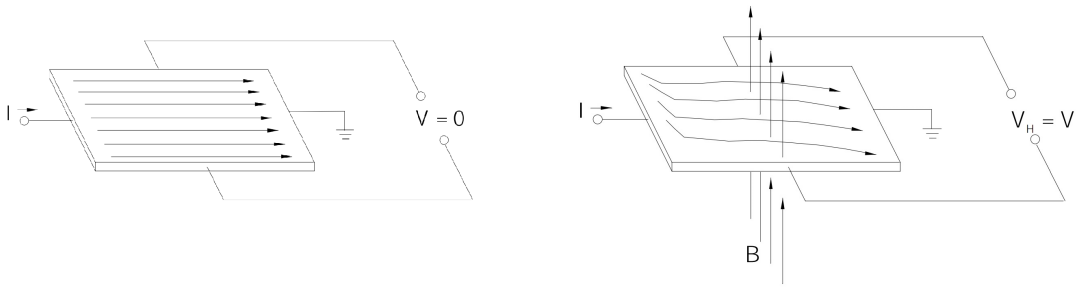


Figure 3.30: Hall effect principle. With no magnetic field, the measured voltage is zero and the current I passes through the plate. Applying a magnetic field B, part of the electrons are deviated and generate a non-zero voltage at the opposite ends of the plate.

The two signals from the encoder and the hall sensor are then elaborated by the servo driver and sent to the next subsystem.

Subsystem 2 is the encoder/speed evaluation unit MOC0 by Sick. It gets the input from the sensors and sends the data to **Subsystem 3**, namely the logic of the safe PLC, to calculate the congruence between the speed measured by the two different sensors. The treshold of allowance of the speed difference can be set by the user; a typical value is 10% difference between the two speeds. A higher difference triggers the safe state.

Subsystem 4 is the output module and **Subsystem 5** is the laser scanner. Two digital outputs exit the PLC and are connected to the laser scanner. The $2^2 = 4$ combinations allow 4 fields to be switched according to the speed, as seen in table 3.1.

3.2.1 Cost of the system

As previously done with the proANT 436, it will be here highlighted the cost aspect of the system. Figure 3.31 contains a pie chart representative of the prices and relative weights of each component. At a first glance, the prices of the two described safety systems are very similar. This calculation, however, doesn't take into account the encoders and gear tooth sensors that provide the two channels for the safety calculation of the speed. In fact, these are integrated inside the servomotors and only a summary speculation can be made about their cost.

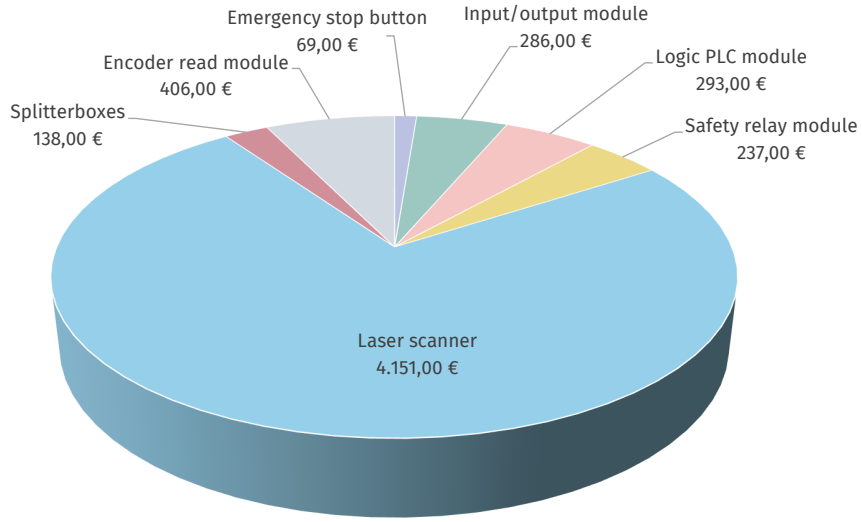


Figure 3.31: Cost of the safety components and relative impact on the cost of the whole safety system. The cost of the whole system, or the sum of each slice of the pie, is 2.695,00€.

The biggest slice of the pie is taken here again by the laser scanner, which is probably the least replaceable component of the system, considering also its navigation function. The model is the same used on the other vehicle discussed in this work, therefore it will not be further described.

The remaining quarter of the pie is taken almost entirely by the safe PLC that comprises

an input/output module, a logic module, two safety relay modules, one encoder read module and an interface between the servo drive and the encoder read module itself. Compared to the safe PLC components needed for the proANT 436, that score a total price of 703 €, the safety PLC system of the proANT 490 has a total price of 1167 €, 66 % more expensive than the Beckhoff modules. The higher expense is partially justified by the fact that the Sick safety PLC is a system on its own, so the PLC that controls the AGV can be completely separated and doesn't need to be manufactured by a specific brand. Moreover, Sick components' integration in safety applications is a leverage point of their ecosystem, so the PLC is easy to program and connect to other components.

3.3 Additional safety components of the ProAnt AGVs

Apart from the basic needs of a safety system in an Automated Guided Vehicle, more safety functions and components can be used to further improve the level of protection against hazards coming from the normal procedures that these vehicles go through. Here, some of these additional components will be briefly presented.

Couple of side scanners

Two additional side scanners can be mounted on the robots, so that they can detect objects which are placed above or below the recognized level of the safety laser scanner. Moreover, they secure the mechanisms area when the AGV is performing an automatic load/unload procedure. If objects are detected within these vertical safety fields, the respective scanner reports it to the PLC, which stops the AGV immediately.

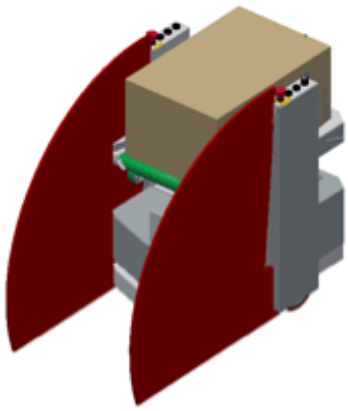


Figure 3.32: Detection of obstacles with side scanners. The area in red is the field of detection of the laser scanner.

Additional 3D Camera

An optional 3D camera can be mounted in the front part of the vehicle to detect a broader variety of obstacles in its path. This allows to eliminate the restriction of detecting obstacles just at a height of 12cm. The camera used is the Asus Xtion, a stereo camera with a resolution of 1280x1024 pixel and a distance of usage between 0.8 m and 3.5 m. The field of view of 58°horizontal and 45°vertical is visible in figure 3.33 (left). A truthful representation of the field of view from above is shown in figure 3.33 (right); it's immediately visible that the blind zone of the camera is too large to guarantee a safe protection of the vehicle. Moreover, the chain of components that constitute the system does not comply with a sufficient performance level for the application. This will be the main topic of section 5.3.

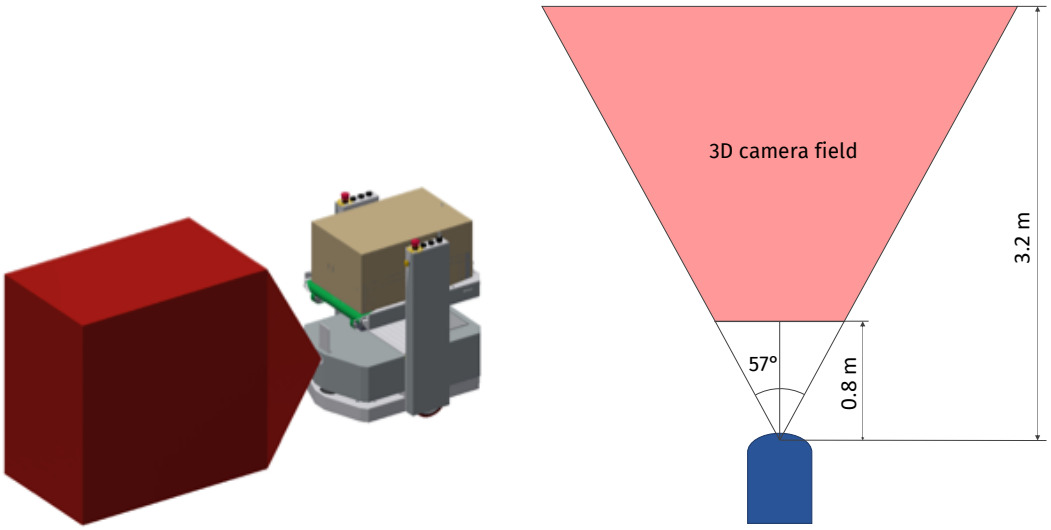


Figure 3.33: Field of view of the 3D camera from an isometric view (left) and a geometric representation as seen from the top (right).

Reverse laser scanner

For a total coverage of the area surrounding the AGV, a reverse scanner can be implemented. The reverse scanner supervises the area behind the vehicle and stops it whenever an obstacle is detected while driving reverse.
The proANT vehicles drive reverse only while undocking from a charging station. In this case the vehicle with no reverse scanner drives "blind" without detecting humans or obstacles. According to EN1525 Chapter 5.9.5.6 this is allowed, since the vehicle doesn't drive faster than 0.3 m/s.

Other sensors

In more demanding applications, when customers require particular needs, additional safety sensors are placed to monitor the position of the conveyor. These are non-contact inductive safety switches (figure 3.34) that enable or disable the side scanners when the conveyor is extended. Moreover, they safely prevent the movement of the AGV when the conveyor is lifted and/or extended, since this would dangerously modify the center of gravity of the vehicle and make it hazardously unstable.

Figure 3.34: Sick IN3000 inductive sensor.

Chapter 4

State of the art for AGV safety systems

Below will be discussed the main safety functions an AGV must fulfill and the technologies used to match the requirements. Particular interest will be given to the functionalities provided by the vehicles and the different types of AGVs. By analyzing how other manufacturers ensure personal safety in their mobile platforms, it will be interesting to notice a common pattern in every single robot.

4.1 Functionalities an AGV safety system must fulfill

During operation of the robots, a series of hazards arises from the mere fact that the machines themselves are moving in an area that is usually shared with humans and other obstacles:

- The main hazard is due to the robot moving forward at a certain speed and potentially crashing into people and other obstacles. To make this movement safe, a sensor is positioned in the frontal part of the robot with the aim of detecting obstructions of the path.
- When performing a turn around a corner it's convenient that the area detected by the sensor follows the curved shape of the robot's path, since in this case the movement is not in a straight line.
- Automatic loading and unloading procedures could need to be secured, for example when a conveyor belt is used by the AGV to perform the load/unload.
- The procedure of docking to a charging station could need to be protected if there is the possibility of a human to get trapped during the docking process.

Other fundamental safety functions include:

- Emergency stop initiated by push buttons, needed to safely stop the machine in case of danger or necessity.
- Safety field switch function, used to adjust the depth of the safety field according to the current speed of the vehicle.

4.2 Competitor's technology

To analyze the technology used by other manufacturers, it is useful to classify the different types of AGVs according to their structure and functionalities. A general classification of AGV types could be the following:

- Forklift
- Differential drive
- Omni-wheel platform
- Magnetic or wire guided

Examples of these structures and their safety systems are described in the following sections.

Forklift-type AGVs

This type of vehicle is the evolution of a human-guided forklift. It is able to carry heavy payloads, lift them from the ground and eventually stack them into shelves. The front of the AGV must be secured with a safety field to ensure safe navigation, as well as the back that carries the two forks. In fact, when loading and unloading it's important to make sure no obstacle can dangerously interfere with the procedure. A model from Jungheinrich is shown in figure 4.1.

Another model of this category is the Egemin ATL (figure 4.2), capable of heavy duty material handling. A rather big structure needs to be secured in many ways, so apart from the front and back laser scanners, another scanner is mounted on the top of the vehicle. This creates a virtual curtain that secures the access to the load/unload area in order to prevent the hazards arising from this operation.

Figure 4.1: Jungheinrich ERC 215a carries a maximum payload of 1500kg and it's equipped with two Sick S3000 laser scanners, in the front and back of the vehicle.

Figure 4.2: Egemin ATL, with additional scanner on top to secure the whole load/unload area.

Figure 4.3: JBT JayBoT, with two laser scanners in the front to secure the sides of the vehicle.

Much smaller is the robot from JBT, figure 4.3. It is capable of performing natural navigation and laser navigation. The difference between the two of them is that natural navigation is based upon a map created by the robot itself during its commissioning, whereas laser navigation utilizes reflective spots placed in the plant as references for the robot. The vehicle presents two laser scanners on the front to secure the sides of it.

Last, the Seegrid GT10 carries the usual back and front scanners, plus another scanner on the top, facing down (figure 4.4). This allows to secure the load/unload operations and also to detect whether or not there is a driver in the vehicle, since this model features manual as well as automated drive.

Figure 4.4: Seegrid GT10, manual and automated guided vehicle allows great flexibility in warehouse facilities.

Differential drive AGVs

These vehicles are characterized by two central wheels driven by two independent motors, allowing the robot to revolve around its axis and thus eliminating the problem of the minimum steering radius. The weight is then distributed among different roller wheels positioned in the base of the robot. An example of this structure is the Comau Agile 1500 shown in figure 4.5. This vehicle is equipped with two Sick S300 laser scanners facing forward and backwards and a FlexiSoft safety PLC still from Sick. Capable of natural, laser and magnetic stripe navigation, the maximum positioning repeatability is $\pm 10mm$. The design of this model allows it to cruise under the load, lift it slightly from the ground and transport it to the goal.

Different design but same type of drive is visible in the AGVE A2 in figure 1.1. The two safety laser scanners in front allow it to have its sides secured, whereas the lidar on the top allows laser navigation. Multiple structures are possible for the vehicle, including tugger, forklift and slide telescopic forks.

Next, the Kivnon K32 is a towing AGV that can move payloads of up to 2000kg and it's equipped with one laser scanner on the front, figure 4.7. It is not uncommon to see this type of AGVs tow multiple carts inside automotive factories.

A really interesting vehicle is the LD Platform by Omron, shown in figure 4.8. For its

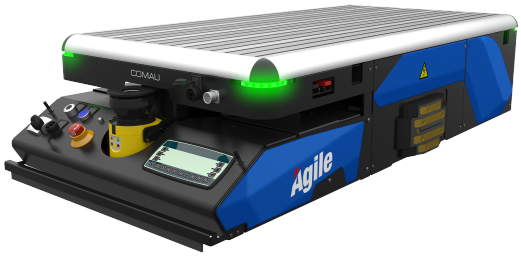


Figure 4.5: Comau Agile 1500, equipped with two Sick S300 laser scanners.

Figure 4.6: AGVE A2 with two laser scanners to secure the front and the sides of the vehicle.

Figure 4.7: Kivnon K32 with one laser scanner in front.

Figure 4.8: Omron LD Platform, a very flexible vehicle featuring different interesting sensor solutions.

primary safety function it utilizes a classic Sick S300 safety laser scanner placed at a height of 200mm, and the sensing is enhanced by additional solutions:

- A front bumper that stops the vehicle when tripped
- A low front laser scanner that ensures the detection of low-profile obstacles
- Side laser scanners (Sick TiM series) mounted with a vertical field to secure the sides of the additional structure
- Rear sonar sensors for obstacle detection when moving backwards

The latter feature is very interesting to analyze. As visible in figure 4.9, four ultrasonic modules (2 senders and 2 receivers) allow the back of the vehicle to be monitored within

Figure 4.9: Close-up picture of Omron LD's back sonars.

a 2 m range. Despite this feature not being safety-related, and no performance level being calculated upon it, it's an additional feature that could be studied and developed for the proANT fleet.

Omni-wheel platforms

This vehicles are equipped with special wheels that allow them to drive in any direction (backwards, forwards and sideways), that are shown in figure 4.10. They are conventional wheels with rollers attached to their circumference at a 45° angle. Thanks to this feature, when two wheels on the same side are counter-rotating, the vehicle strafes sideways. Due to the omni-directional drive behavior, each side of the AGV could be the forward driving side, so it's necessary to secure all around the robot with two laser scanners having a field of 270° and positioned on two opposite corners of the vehicle. This type of movement is particularly efficient with tight spaces and the need of high degrees of mobility.

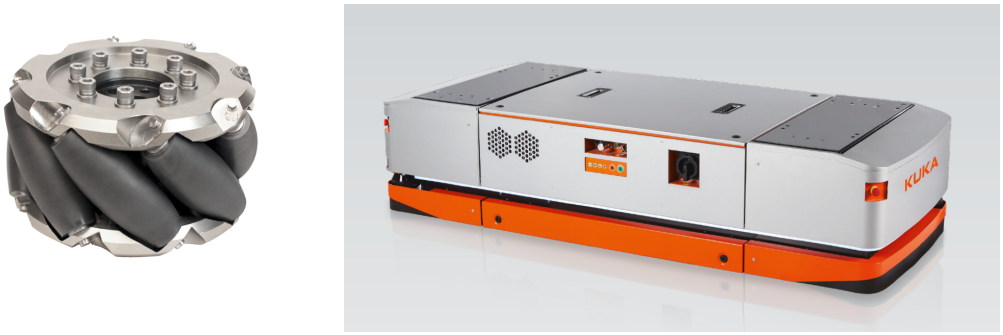


Figure 4.10: Mecanum wheel and a Kuka Mobility platform 1500.

Magnetic or wire guided AGVs

Analyzing the safety systems of this category of vehicles is really interesting. In fact, a

Figure 4.11: On the left a SmartCart 100 ST-R and on the right a Toyota TAE050, both magnetic guided AGVs that use a laser scanner for personal safety.

magnetic or wire guided AGV doesn't need information about its surroundings, but still the personal safety is ensured by a safety laser scanner. This means not only that the current detection system employed in the proANT fleet is probably the most efficient and optimized, but also that it has the fundamental benefit of allowing the robots to navigate naturally, without incorporating additional sensing equipment. Some examples are given in figure 4.11.

Conclusion

In this section, an overlook of the current technology used by AGV manufacturers has been given. The safety functions that an AGV must have are at least two: emergency stop with a push button and automated personnel detection. Looking into the documentation provided by manufacturers, it is possible to only assess which are the sensors used for safety purposes, but not the whole system. In general however, the laser scanners must be controlled by a safety PLC (most of them comply with ISO 13849 Cat. 4 PL e), that will send an output to the motor's drivers, allowing to enter the safe state. Entering the safe state can be done either with a safety relay cutting the power supply to the servo drive card, or via the STO (Safe Torque Off) function present in more recent drivers. This function can be triggered by the safety PLC via a dedicated input, it ensures that no torque-generating energy can continue to act upon a motor and prevents unintentional starting. However, cutting the torque of the motors is not sufficient to stop the vehicle safely, so it is combined with the built-in braking mechanism of the motors, to ensure a short braking time. A more detailed explanation of STO is depicted on page 31.

Chapter 5

Alternative safety systems

This chapter presents a review of some other possible sensors and structures of the safety system to ensure personal safety and a reliable detection of obstacles and personnel. First of all, it will be discussed the possibility of changing the current laser scanner, the Sick S300, with another safety laser scanner of comparable performance. Then it will be analyzed the possibility to use two redundant non-safe laser scanners, connected to two redundant IPCs, to perform the safety field evaluation as well as navigation data acquisition, with a focus on safe software. Next, the usage of cameras as an alternative sensing component will be discussed, with all the advantages and disadvantages as well as the current state of the art technology on functional safety cameras. Finally, a technological solution based on safety ultrasonic sensors will be taken into account, discussing pros and cons and the most suitable types of platforms for this technology.

5.1 Laser scanner market research

The safety laser scanner is without any doubt the most expensive piece of equipment of all the safety system. For this reason, a good improvement would consist in finding a different sensor with comparable features but at lower prices, or a more performing sensor with a comparable price. The main features that have been taken into account when comparing different sensors are scanning angle, number of safety fields, safety field range and angular resolution, maximum reach, power consumption, navigation data acquisition, dimensions and price.

Scanning angle

It's the angle of the circular sector, with the center on the laser beam source, that surrounds the sensor. As seen in chapter 3.1 (laser scanner stop function) the laser beam source is mounted on a rotating head that scans all the environment several times per second. This makes it possible to have a very broad scanning angle, ideally up to 360°, as in several non-safety Lidars. In AGVs applications however, a scanning angle of 270° is found to be sufficient, thus the Sick S300 employed in the proANT platforms has exactly

this aperture. In some mobile platforms applications it can be found a different type of laser scanner, with an angle of only 190°, but these platforms are often bigger and mount other safety laser scanners around their perimeter.

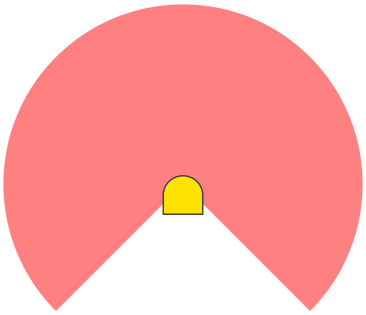


Figure 5.1: Scanning angle of 270°.

Number of safety fields

As seen in chapter 3.1 (safety field switch function), having different safety field plays an important role in the flexibility and capabilities of an AGV. In fact, changing the safety field size and shape according to the speed of the vehicle improves safety and, in some cases, it's fundamental for driving through narrow paths. In the proANT AGVs 4 safety fields are currently used, so this is the minimum requirement for a possible alternative sensor.

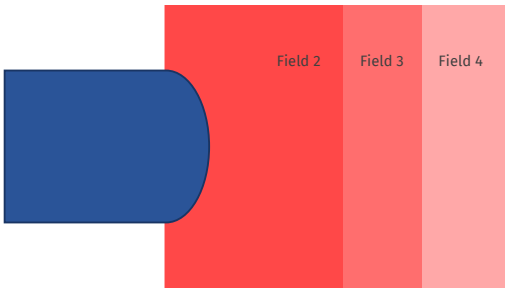


Figure 5.2: Schematic representation of the safety fields (the 1st safety field corresponds to a speed lower than 0.3 m/s and it is essentially a muting function, with no safety field at all).

Safety field range

This feature reflects the capability of the laser scanner to reliably detect small objects. Since the sensor has a fixed angular resolution, it is easy to realize that the smaller the object that has to be reliably detected, the smaller the safety field can be. Figure 5.3 well explains this concept: on the right, a small object with a diameter of 30 mm can

be reliably detected up to a radius of, let's say, 2 m, whereas moving it farther will result in a lack of detection. The bigger object on the right instead can be detected from farther away. In other terms, the angular resolution of the scanner must be fine enough to guarantee a safety field radius of at least 2 m with reliable detection of an object with a 30 mm radius.

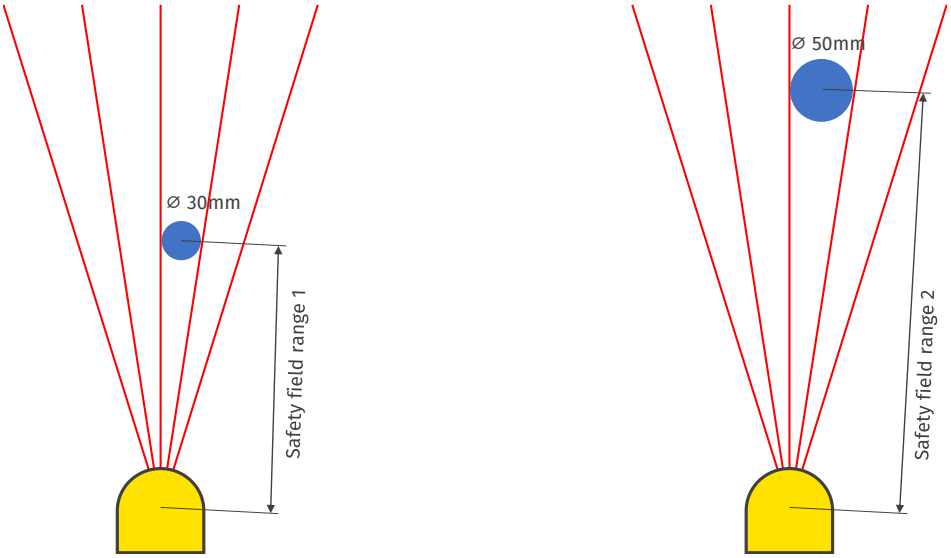


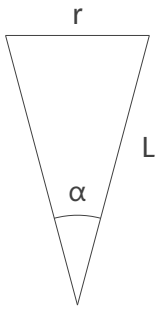
Figure 5.3: Schematic representation of the safety field range limits.

Maximum reach

To efficiently map the environment and subsequently compare the map with the scanned point cloud, the AGV must detect its surroundings with a good reach of detection. Too small of a detected surrounding area would make it difficult for the navigation system to see far in front or to navigate in really large spaces. For this reason, a minimum required reach of the navigation range would be around 15 m. It's interesting to notice, however, that with an angular resolution of 0.5° at a distance of 15 m, the linear resolution would be around 13 cm, so the precision of these points is rather poor (figure 5.4).

Navigation data

In most common applications, safety laser scanners are used to monitor dangerous areas around a machine. For this purpose the sensor must be positioned on the machine and the safety fields must be set connecting a computer and using usually some proprietary software to define the areas. Once all the areas are set, the laser scanner works on its own and it just needs to detect obstacles in its field and switch the OSSD outputs accordingly. In a mobile platform application however, the laser scanner is the sensing device that allows the detection of the surroundings, so there must be a stream of data continuously flowing to the IPC and specifically to the navigation software. The best, fastest way to



$$r = 2L \cdot \sin\left(\frac{\alpha}{2}\right) = 2 \cdot 1500 \cdot \sin\left(\frac{5°}{2}\right) = 13 \text{ cm}$$

Figure 5.4: Calculation of the linear resolution from the angular resolution. The small angle allows to approximate the arc r with a segment.

stream this data is via Ethernet. Not all the laser scanners, though, allow the stream of data that is fundamental for the double purpose of the laser scanner: navigation and functional safety.

Power consumption

In a mobile platform the power consumption is critical because it influences how long it can work with a single charge. It is thus fundamental to choose an energy efficient laser scanner. Moreover, when comparing the consumption of this sensor, the parameter used is the power consumption without an output load.

Having presented all the features needed in a safety laser scanner mounted on an AGV and used for localization other than functional safety, the actual market research on figure 5.5 can be considered. The first sensor is the Sick S300, currently used in the proANT 436 and proANT 490 safety systems. Starting the comparison with the scanning angle, it's clear that the Allen Bradley Multizone and the Panasonic SD3 can be eliminated. The Allen Bradley Mini has just one safety field that can be set, so it is not suitable. The the safety field range must be bigger than 2 m, and this brings to the elimination of the IDEC SE2L. The navigation range instead is too small in the LeiShen W300G. Looking at the power consumption, it's possible to discard the PILZ PSENscan and the Leuze RSL420P.

In the end, just 6 laser scanners remain. Out of these ones, the Sick S300 is the cheapest and better solution, followed by the Hokuyo, the Keyence SZ, the Omron OS32C and the other laser scanners from Sick. Moreover, it must be stated that the prices shown are the list prices, whereas the price of the Sick S300 has a discount on large quantities. This means that with large quantities it could be possible to have cheaper prices on the other plausible sensors. However it must also be taken into account the programming effort that is needed for switching to a different sensor, not only for the setting of the safety fields and other safety parameters, but also for the data used for navigation, since a different manufacturer would mean different communication protocols. Finally, the best option here seems to keep using the safety laser scanner that is currently employed

in the vehicles.

Figure 5.5: Research and comparison of the main features for different laser scanners and manufacturers.

5.2 Non-safety, redundant Lidars configuration

As an extension to the concept of redundancy that has been seen in the previous chapters (for example on the emergency stop button redundant contacts) one could think about using two redundant, non-safety laser scanners to monitor the safety field in front of the AGV. Figure 5.6 shows this disposition. In the eventuality of a failure of one channel, the other channel would still pick up the obstacle and, comparing the data with the other laser scanner, detect the failure.

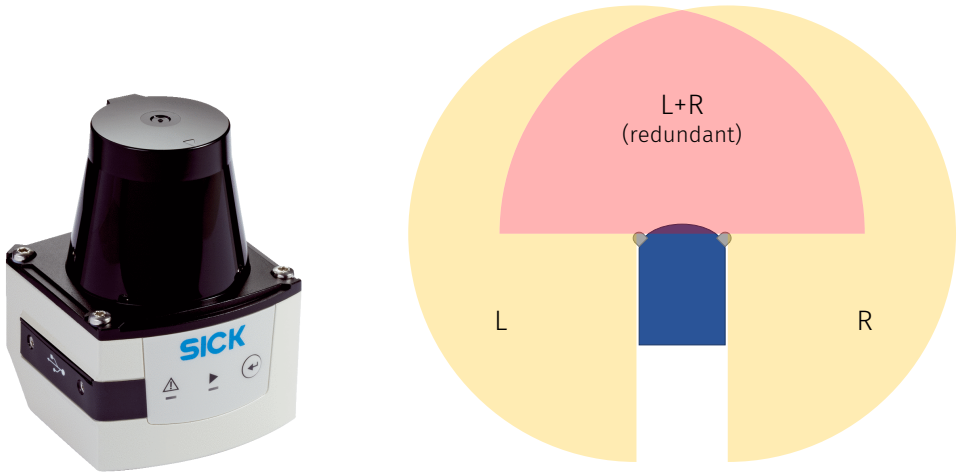


Figure 5.6: Sick TIM 561 LiDAR sensor and physical disposition of two redundant, non-safety laser scanners with a field of view of 270°.

In a safety laser scanner, raw data is elaborated in an embedded system to monitor the safety field. Only after this process, the scanned data set is sent to the IPC in the form of vectors and other values. In particular, the vector `ranges` contains the distance value of all the scanned points, so when a distance value is smaller than the threshold (set in the embedded system through the setup software from Sick) the laser scanner itself triggers the safe outputs.

The two non-safety laser scanners, on the contrary, send the scanned data set directly via Ethernet to a logic element to elaborate them. This logic element could be either one safety PLC or two IPCs in a redundant architecture. The safety PLC however, as seen on page 29, can be programmed only using the function blocks developed, tested and certified by the manufacturer. This makes it impossible to program the software for elaborating the scanned data inside a safety PLC.

The other option would then be to use two Industrial PCs in a two-channel redundant architecture as shown on figure 5.7. Enclosed in the dashed box is the two-channel subsystem with Lidars and IPCs. Looking into the IPCs however it's immediately clear that

these safety computations will have to run together with all the other software that allows the AGV to navigate. Obviously, from a safety point of view, running multiple tasks in a complex operating system like Ubuntu is subject to a great probability of software failure.

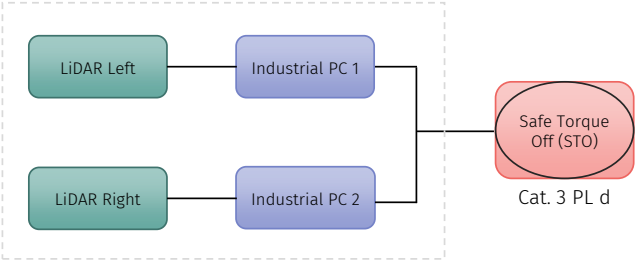


Figure 5.7: Block diagram of the theoretical safety system made of two redundant Lidars and IPCs.

From a cost point of view this configuration may appear convenient since the expensive safety laser scanner and safety PLC are not present anymore, however the reality is more complex. With a price tag of approximately 1500€ per unit, two Lidars do cost less than a safety laser scanner, and the cost of the safety PLC is omitted, which for a Beckhoff system means a saving of around 600€. On the other hand, the price of a single IPC revolves around 600€ per unit, making this system more expensive.

In conclusion, a solution like this would over-complicate the system, whereas in functional safety one of the most important features is simplicity, which reflects the need for fool-proof systems. Ideally, the best safety system would be a hard-wired, enclosed system capable of detecting errors through redundancy and self test. In AGVs, however, the technology used to detect obstacles and to ensure safety is clearly complex, thus the use of a safety PLC is a huge advantage.

5.3 Camera vision

Cameras are currently used in functional safety, when the monitored area is fixed. The norm PD IEC/TS 61496-4-3 [10] gives guidance on this particular topic, which is partly still in a concept phase. In the field of industrial mobile vehicle safety however, there are some challenges that need to be addressed. This will be done in the following pages.

Figure 5.8: Rockwell Automations' Guardmaster SC300 Safety Camera and a plausible machine application.

Rockwell Automation safety camera system

Safety certified cameras are currently available on the market as an established technology. An example is the Guardmaster SC300 Safety Camera made by Rockwell Automation, shown in figure 5.8. This camera can act as a virtual barrier and trigger a safety related stop of the machinery to which it is connected. The report document "Safety Function: Safety Camera" [13], provided by Rockwell itself, will be here discussed.

The first step for the design of all safety systems is the risk assessment, where the simplified model presented in chapter 2.3.2 can be used. According to the report, a Cat. 3 PL d system is required, leading to the scheme in figure 5.9. Hazardous motion is interrupted or prevented by triggering the safety camera. The safety camera is wired to a pair of safety inputs on a safety input module (SI1) which monitors output signal switching devices OSSD1 and OSSD2 from the camera. If the camera is blocked, OSSD1 and OSSD2 go low (0) and the controller drops out the safety contactors. The safety contactors (K1 and K2) are connected to a pair of safety outputs on a safety output module (SO1). The I/O module is connected via CIP Safety over an EtherNet/IP network to the safety controller (SC1). The safety code in SC1 monitors the status of the safety camera by using the pre-certified safety instruction Dual Channel Input Stop (DCS). When all safety input interlocks are satisfied, no faults are detected, and the Reset button is pressed and released, a second pre-certified function block called Configurable Redundant Output (CROUT) controls and monitors feedback for a pair of redundant contactors.

The safety camera has on board diagnostic to dynamically test the signal wiring for shorts: if a fault occurs, both OSSD are set low (0), and the controller drops the safety contactors. Shorts to 0 VDC and wire off are also seen as an open circuit by the input module and result in entering safe state. The final control device, in this case a pair of safety contactors K1 and K2 are controlled by a safety output module. They are wired

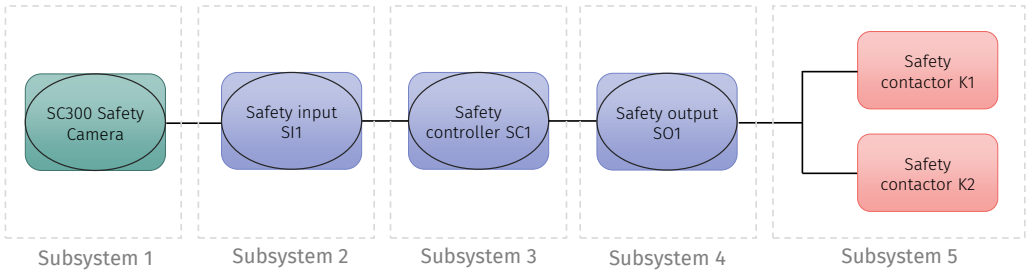


Figure 5.9: Block diagram of the Rockwell SC300 Camera safety system.

in a redundant series configuration and tested via a wired connection to the input module.

After the risk assessment, stating that a Cat. 3 PL d system is needed to perform the safe stop, the safe distance must be calculated. Determining the distance between the hazard and the sensing equipment is crucial when the delay time of the safety system is not negligible. The formula to calculate the safe distance is the following:

$$S = (K \cdot T) + C$$

Where K (mm/s) is the approaching speed of the body (or body part) subjected to eventual danger, T (s) is the maximum time between the tripping of the safety device and the machine stop, and C (mm) is the intrusion distance, a parameter involving the resolution of the camera. For example, if $K = 1600\ mm/s$, $T = 900\ ms$, $C = 100\ mm$ the distance between the sensing device and the actual hazard must be at least $S = 1540\ mm$.

The main drawback of this system is that the camera is fixed in a certain position. In fact, after mounting the camera in a corner as shown in figure 5.9, the inner frame must be marked with a special reflective tape. Then, the user needs to push the "Teach" button present on the camera to acquire the current image. If the image detected by the camera differs from the image taken during the "Teach" procedure, the two OSSD1 and OSSD2 of the camera go low (0) and the safe state is triggered by dropping the safety contactors. Other safety applications are being currently developed, making use of cameras without the reflective tape but with patterns and scene recognition. In particular, the norm PD IEC-TR 61496-4 parts 1, 2 and 3 [10] gives guidance on design and testing of such systems.

In any case, all applications currently available are fixed, thus this solution is completely unsuitable for the natural navigating AGVs that see a different frame every time a snapshot is taken, so for this reason the system will not be discussed further.

3D stereo camera

There is theoretically the possibility of connecting two 3D cameras, looking in the same direction, to create a category 3 system. Having then redundant sensors could be the solution to the poor reliability and precision of cameras compared to much more solid technologies like laser scanners.

Figure 5.10: Asus Xtion Pro used in proANT AGVs as an additional detecting measure.

The single camera needs to connect via ROS (Robot Operating System), an open source platform for Linux that has been developed with the purpose of creating an efficient operating system for controlling robots [27]. The camera currently used in proANT platforms is an additional safety measure, capable of detecting objects in a 3-dimensional space in front of the robot, as previously discussed on page 51. The camera triggers a Boolean variable sent to the PLC, which stops the vehicle when the field of view of the camera is invaded.

A stereo camera however presents a quite rough resolution, so the detection of obstacles would not be robust enough. Moreover, the algorithm for manipulation of data coming from a stereo camera is complex and fundamentally unsuitable for safety applications.

Time of Flight camera

Another option for safety cameras is a Time-of-Flight camera like the one shown in figure 5.11. ToF cameras are used as driver assistance and safety sensors in the automotive sector, in applications such as active pedestrian protection, emergency brake assist but also interior applications such as checking for correct driver position. A ToF camera has a much lower computational cost compared to 3D stereo cameras, and uses a principle similar to the Lidar laser scanner: a pulse is sent and received by the sensor and the elapsed time is proportional to the distance of the detected object. Such a sensor has no moving parts and can scan a whole 3D scene in a single snapshot. The main problems are however related to the small field of view, so at least 2 cameras are required to cover an area close to the laser scanner safety field.

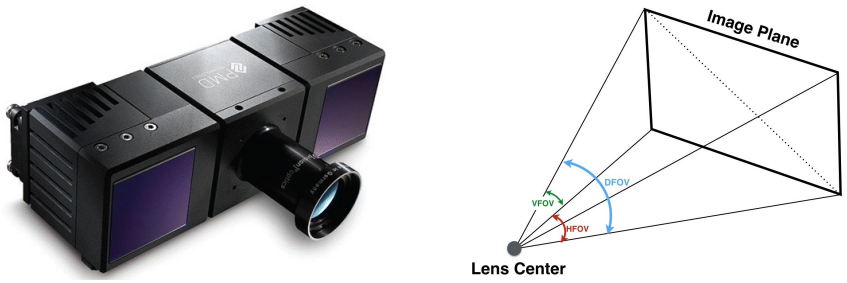


Figure 5.11: Left: classic example of Time of Flight camera, the PMD CamCube 3.0. Right: 3-dimensional field of view of a ToF camera.

A ToF camera consists of at least the following components:

- Lighting unit: it illuminates the scene. Either LEDs or laser diodes are used, which can be modulated sufficiently fast, so that the sensor can perfectly measure the running time. The pulse duration moves in the nanosecond range. The lighting is mostly in the near infrared, so the environment is not visually disturbed by the camera.

- Optics: an optic collects the reflected light from the environment and reflects the scene on the sensor. An optical bandpass filter only lets through the wavelength with which the lighting works. Thus, a large part of the disturbing background light is eliminated.

- Sensor: The heart of the TOF camera is the sensor, which measures the runtime separately for each pixel. The image sensor resembles other chips for digital cameras with the difference that a pixel is much more complicated: It does not have to simply collect the incident light, but measure the runtime. Due to the more complicated structure, the pixels are large in comparison to digital cameras, they reach side lengths up to 100 μm. The resolution of the PMD CamCube 3.0 for example is 204 $\times$ 204 pixels with an edge length of 45 μm.

- Control electronics: the lighting and the sensor must be controlled with sophisticated electronics to achieve the highest possible accuracy. If the control signals between lighting and sensor only move by 10 ps , the measured distance changes by 1.5 mm.

- Evaluation/interface: the calculation of the distance from the measured values is usually done directly in the camera system. For this purpose, calibration values are also stored in the system. The interface is used under either USB or Ethernet.

The data sensed by the camera is a point cloud similar to the one in figure 5.12. Since every point of the point cloud could potentially be treated independently, it is possible to create different zones inside the field of view of the cameras, for example to limit the

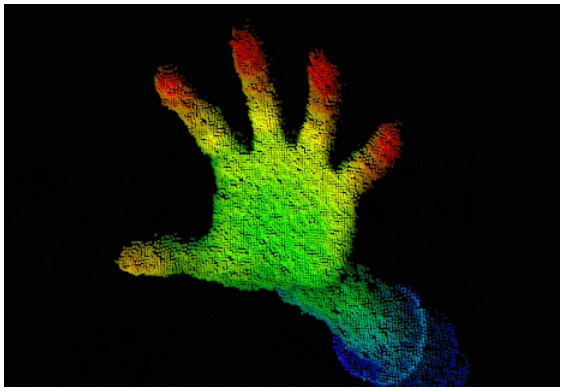


Figure 5.12: Representation of the point cloud sensed by a Time of Flight camera. Each pixel has a value of depth associated to it, which is then translated in a color scale.

width of the safety field to 1 m, which is the required dimension for this application.

Figure 5.13 shows a possible arrangement of two cameras on an AGV. This disposition of the cameras guarantees the protection of the whole front part of the vehicle and doesn't have any blind spots. However it could be very difficult to mount the cameras so far inside the body of the AGV, since usually that part is where the payload is positioned. Moreover, this disposition considers only the safety-related aspects of the application. It is fundamental to notice that navigation would not be possible with such a small field of view, so other sensors would need to be used for the purpose.

The main issue with ToF cameras lies in the integration with the safety system. In fact, conversely to safety laser scanners, there is currently no ToF camera that complies with ISO 13849 PL d or higher. Another big problem is that safety PLCs don't currently have a function block that allows to compute the data coming from a ToF camera in a safety certified way. Detecting the distance in fact can be done with simple algorithms, however (as seen on page 29) the safety PLC can be programmed only using the function blocks developed, tested and certified by the manufacturer.

Another disadvantage of ToF cameras includes mutual interference: if several systems are in operation, it may be that the different cameras interfere with each other and thus the distance value is falsified. Still, there are several ways to get around this, like time multiplex or the use of different frequencies of the light pulses. Multiple reflection is also a known issue: in contrast to the laser scanning systems, since an entire scene (not just a single point) is illuminated, it is possible for multiply reflected light to pass from an object back onto the sensor. The measured distance in this case can be greater than in reality.

Finally, power consumption could be an issue as well since a single ToF camera will consume around 20 W, but in a two-camera configuration a power consumption of 40 W

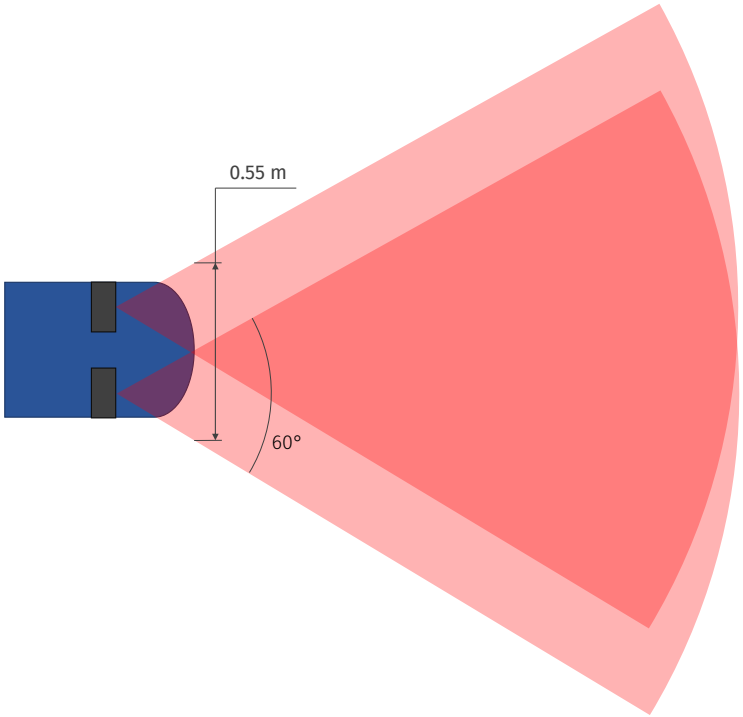


Figure 5.13: Arrangement of two cameras on an AGV in a realistic scale, highlighting the field of view in red.

is expected, namely 6.6 times the consumption of a safety laser scanner.

5.4 Ultrasonic sensors

Similarly to the principle of Time of Flight (ToF) described when introducing the laser scanners, sonars send a burst of sound waves in the range above 16 kHz and detect the reflected sound; measuring the time between these two events leads to calculation of the distance between sensor and object. These systems are not a human invention: a bat's natural sonar can detect a perfectly camouflaged moth, and dolphins use the same principle to find their prey in murky water. Both these animals obtain their basic means of subsistence by detecting and evaluating the echo of sonic waves.

In technical applications, sonars have been widely used in ships for detecting the depth and conformation of the seabed. More recently, ultrasonic sensors are mounted in cars for parking aid, to assist the driver with tight maneuvers (figure 5.14). Similar sensors are used in industrial applications to detect the level of liquids, solids, powders and granular materials. Their great reliability and robustness to dust and dirt is a really important

feature, and the sensor is also capable of cleaning itself through the ultrasonic vibration.

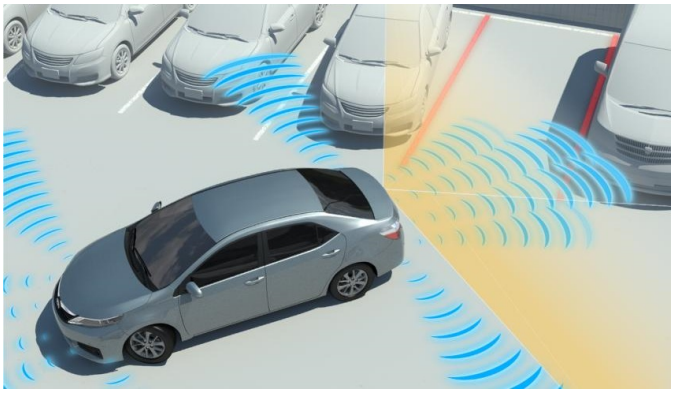


Figure 5.14: Common arrangement of parking sensors.

In safety applications these sensors are mostly unknown, however some options have been found and will be here discussed. It is the case of Mayser USI Safety ultrasonic industrial sensors [16], shown in figure 5.16. The system is comprised of the evaluation unit and up to 2 ultrasonic transducers, with two OSSD outputs (Output Signal Switching Device) as safe outputs that can be connected to the safe PLC inputs and trigger the safe state. The detection parameters can be set via USB using a proprietary software.

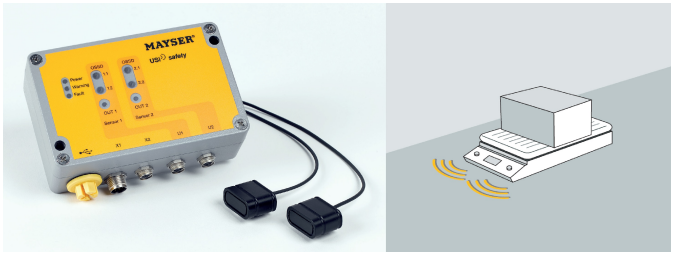


Figure 5.15: Mayser ultrasonic sensors and a possible AGV application.

One big advantage of these sensors compared to the laser scanner is the 3-dimensional sensed field. It has an aperture of $\pm 17^{\circ}$ on the broad side and $\pm 5^{\circ}$ on the narrow side. Moreover, the safety field can reach up to 2 m, which is ideal for the application, since the Sick S300 laser scanner currently used in the proANT vehicles has a safety field range of 2 meters. The resolution however is around 1 cm, so this system can't be used for high precision applications. Before getting deep into these sensors it's interesting to mention that the power consumption of this module is approximately 3.6 W, almost a half of the power consumption of the Sick S300 laser scanner, which is around 6 W.

For this type of sensors, the setup part is crucial and it will be here described by referring to the Mayser USi Safety operating instructions. Two operating modes are currently

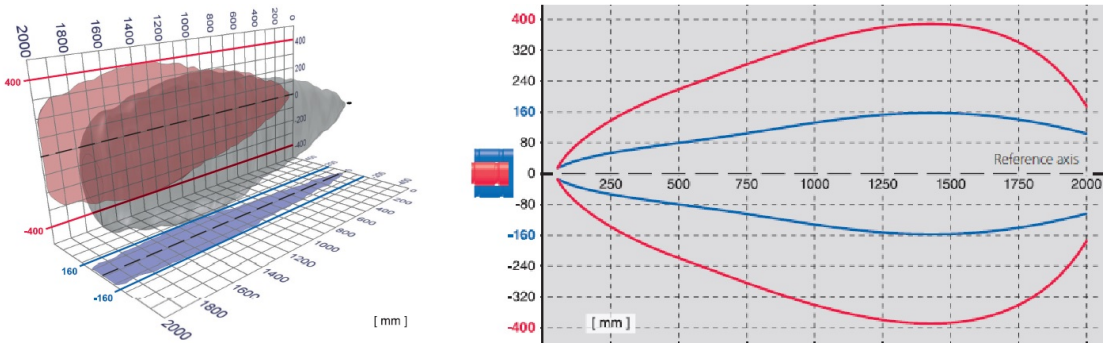


Figure 5.16: Shape of the sound field, with an aperture of approximately ±17° on the broad side and ±5° on the narrow side.

available: the first (standard) operating mode switches both OSSD outputs when the field is obstructed; the second operating mode has instead two field ranges, a warning field and a protection field, that activate respectively the unsafe output and the OSSDs. The sizes of both warning field and safety field are set via software, after a careful design process that considers many factors.

Temperature compensation

First of all, the temperature of the environment greatly influences the measurement of the distance. In fact, speed of sound is not constant, but greatly depends on the medium. In its most generic definition, the speed of sound is defined as the partial derivative of pressure over density, at constant entropy, all under square root:

$$c = \sqrt{\left(\frac{\partial p}{\partial \rho}\right)_s}$$

Approximating the pressure p with the ideal gas law, and considering the bulk modulus of ideal gases as well as substituting the density with mass over volume, the equation of the speed of sound takes the well-known form:

$$c = \sqrt{\gamma R_* T}$$

For more technical applications however, the speed of sound is linearized considering dry air (0% humidity) at temperatures near 0°C. Applicable with sufficient accuracy, the linearized formula is:

$$c(\theta) = 331 + (\theta \cdot 0.6) \quad (m/s)$$

As an *echo* recognition unit, the sound emitted by the ultrasonic sender is reflected by the obstacle and travels back to the sensor. If an object is detected at the distance $d = 2$ m, then the sound moves the distance $s = 2d = 4$ m until it is received again and evaluated

by the unit. The time required for this is:

$$t(\theta) = \frac{s}{c(\theta)}$$

Differences of tens of degrees Celsius can lead to errors of several centimeters in the evaluation of distance: For example, an object at 2 m distance is perceived 7.5 cm closer at a temperature of 40°C, if not compensated.

Field dimensions

After temperature compensation, the calculation of the safety field dimensions is fundamental and needs to be carried out with criterion. The general calculation formula for the minimum distance S is:

$$S = (K \cdot T) + C \quad (mm)$$

Where K (mm/s) is the relative approach speed between obstacle and sensors, T (s) is the stopping time required by the system to get to a safe state, and C (mm) is a safety constant that takes into account the montage, worst-case scenarios and temperature differences.

Considering an AGV the relative speed K is the summation of two speeds: in a worst-case scenario, a person walks towards the AGV with a speed $k_1 = 1600$ mm/s (according to ISO 13855 [5]), while the AGV itself moves at a maximum speed of $k_2 = 1500$ mm/s (the proANT AGVs top speed). This case however is not taken into account, since walking against a full speed running AGV is not a considerable human behavior. In fact, the AGV can be easily seen and avoided by a human walking towards it, so this brings the speed coefficient to $K = 1500$ mm/s.

The stopping time T comprises two elements as well: the response time of the protective device, $t_1 = MS \cdot 1/f$ where MS is the number of multiple scans (for default settings, MS=3) and f is the measuring frequency, f=33 Hz for this sensor unit. Subsequently, $t_1 = 0.091s$. The stopping time of the machine t_2 is instead the time between the receipt of the OFF signal in the safety PLC and the achievement of the safe state, and it is estimated around $t_2 = 1$ s.

The constant C will for simplicity only take into account the temperature. Figure 5.17 shows the average monthly temperatures in Berlin, that will be taken as a reference. This estimation brings however two main sources of error: first, the mean monthly temperature doesn't reflect the lowest and highest temperatures, which are the ones to take into account when calculating this coefficient. Secondly however, the temperatures inside an industrial facility are always milder than the temperatures outdoors, so the effect of highest and lowest temperatures is mitigated and thus on first approximation the above-

mentioned figure can be used. The minimum temperature is then $\theta_{min} = -2°C$ and the maximum temperature is $\theta_{MAX} = 25°C$, whereas an average annual temperature of around $\theta_{avg} = 10°C$ is calculated.

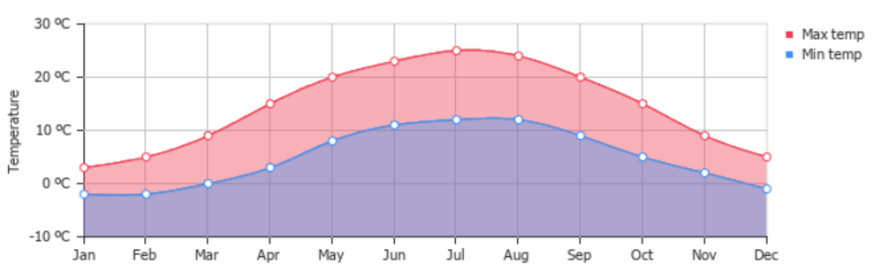


Figure 5.17: Average minimum and maximum temperatures in Berlin, Germany. Copyright 2019 www.weather-and-climate.com

On the practical side then, a temperature of $\theta_{avg} = 10°C$ will be indicated when setting up the module. The coefficient C is an addition to the safety field, and takes into account only the decrease of temperature from the average. The reason for this was well explained when presenting the topic of temperature compensation. When the temperature increases sound waves move faster, and thus the perceived objects appear closer since the travel time is shorter. When the temperature decreases from the average there is an opposite effect: perceived objects appear farther than they really are, and this is a dangerous condition. For this reason, when calculating the coefficient C, the temperature difference to consider is $\Delta\theta = \theta_{avg} - \theta_{min} = 12°C$. Coefficient C is then calculated using the formula:

$$C = \Delta\theta \cdot 0.0017 \cdot d \quad (mm)$$

Where d is the measuring distance that, erring on the safe side, will be considered $d = 2000$ mm, leading to a calculation of $C = 41$ mm.

It must be stated out, however, that AGVs often share their paths with humans, and thus it's very common to have temperatures around 18°C and up, but usually not lower. The temperature compensation is then highly influenced also by the facility itself, so this parameter can be calculated accurately only during commissioning.

Finally, having all the coefficients leads to the calculation of a safety field length $S = 1.7$ m. Using the two-fields operating mode, the safety field can be set to $S_s = 1.7$ m and the warning field to $S_w = 2$ m. When the warning field is harmed, the AGV starts to slow down without performing a full safe stop: this allows to mitigate brake wear and generally to reduce stress on components and mechanical structure.

Additional indications

Testing is a fundamental part of the design of a safety system, so this procedure must be carried out with high awareness. Norm EN 1525 [6] well explains how to carry out a proper test for driver-less vehicle safety applications. As an addition, due to the technology used in ultrasonic sensors, test specimens with a high sound absorption coefficient are to be preferred.

Basic settings like the warning field and safety field lengths are manageable in the dedicated software user interface after a secured log in. Activating the expert mode allows the user to change more parameters of the system, for example:

- Transmission intensity, or the volume of the sound burst sent by the emitter.
- Temperature compensation, as discussed earlier, relates to the mean temperature, which will be around 10°C. In highly fluctuating temperatures, connecting a temperature sensor is possible and will ensure improved detection robustness.
- Sensitivity of the sensor, useful to better detect highly absorbent materials.
- Multiple scans from 3 to 20 are available. Low parameter values make the unit more sensitive, whereas high values make it more tolerant to disturbance.

Another possibility of the USi safety sensors is that of creating dynamic oscillograms during functioning, like the one shown in figure 5.18. In this case a teach-in function has been used to make the system learn that an obstacle in point 3 corresponds to a safe state, and everything different from that spectrum triggers a safe output. This can be useful when the sensors in an AGV detect the ground or parts of the vehicle itself.

Safety field coverage

As mentioned earlier, the sensors have an angular aperture of 34° on the broad side and 10° on the narrow side. Figure 5.19 shows a possible disposition of the sensors, having the aim of creating a protected field around the robot that resembles the safety field currently set on the laser scanner. In the same figure there is a visual representation of the height of the safety field when mounted 12 cm from the floor. By using 2 ultrasonic sensors, and thus one evaluation unit, a field of approximately 1.9 m of length and 1.1 m of maximum width in front of the robot can be achieved. From the above mentioned figure is however clearly visible that the safety field is quite narrow in the initial part, almost half as wide as the current laser safety field.

Also, the overlapping of sound waves that could interfere with each other is an issue. Since the sensors are close to each others in fact, sound waves coming from a sensor could be reflected by the obstacle and be detected by the other sensor, thus increasing the uncertainty of the measurement. Moreover, the noise generated by one sensor could

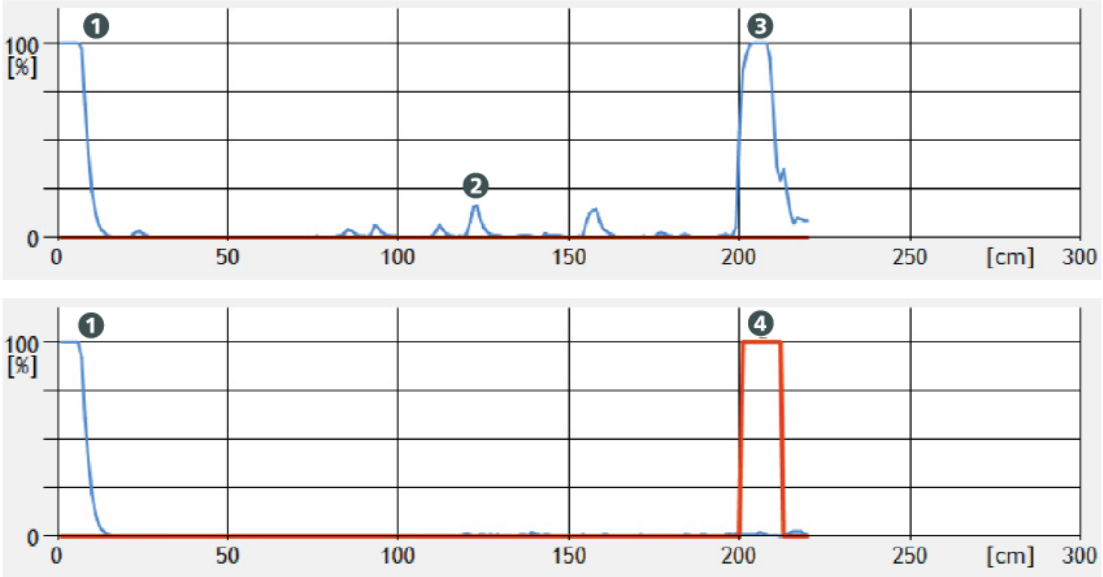


Figure 5.18: Example of oscillogram. On top, the plateau 1 on the left edge shows the normal oscillation of the sensor (ultrasonic transducer). The small peak at 2 is an insignificant reflection. The high peak 3 at about 210 cm distance shows a reference object that is accepted as given after the teach in. On the bottom figure, the empty red envelope curve at 4 indicates that the reference object is missing.

interfere with the functioning of the other.

A solution could consist in setting each sensor to send waves in a specific range of frequencies, however all the sensors do already emit sound in a range of frequencies for robustness purposes. In fact, certain surfaces absorb certain frequencies more than others, so the detection capabilities increase when broadening the spectrum. This leads to another huge problem that will lead to discard the safety ultrasonic sensors configuration.

By the nature of the sensors themselves, it is not possible to obtain navigation data. The spectrum analyzed before is in fact the most complex information that can be taken from the unit. This leads to the need of an additional sensor for detecting the position of the robot itself, for example a non safety laser scanner or camera. The problem doesn't exist if, for example, the AGVs are line guided, magnetic spot guided or laser-guided (these AGVs have a 360° laser scanner on top that calculates its position via triangulation of reflective spots mounted in the facility).

Lastly, the cost of this system plays a decisive role. At a price tag around 2000 €, the complete ultrasonic sensor system should be used in combination with a non-safety laser scanner for navigation, and this would discard all the convenience. For a line guided AGV however, solving the problem of overlapping and interference could lead to

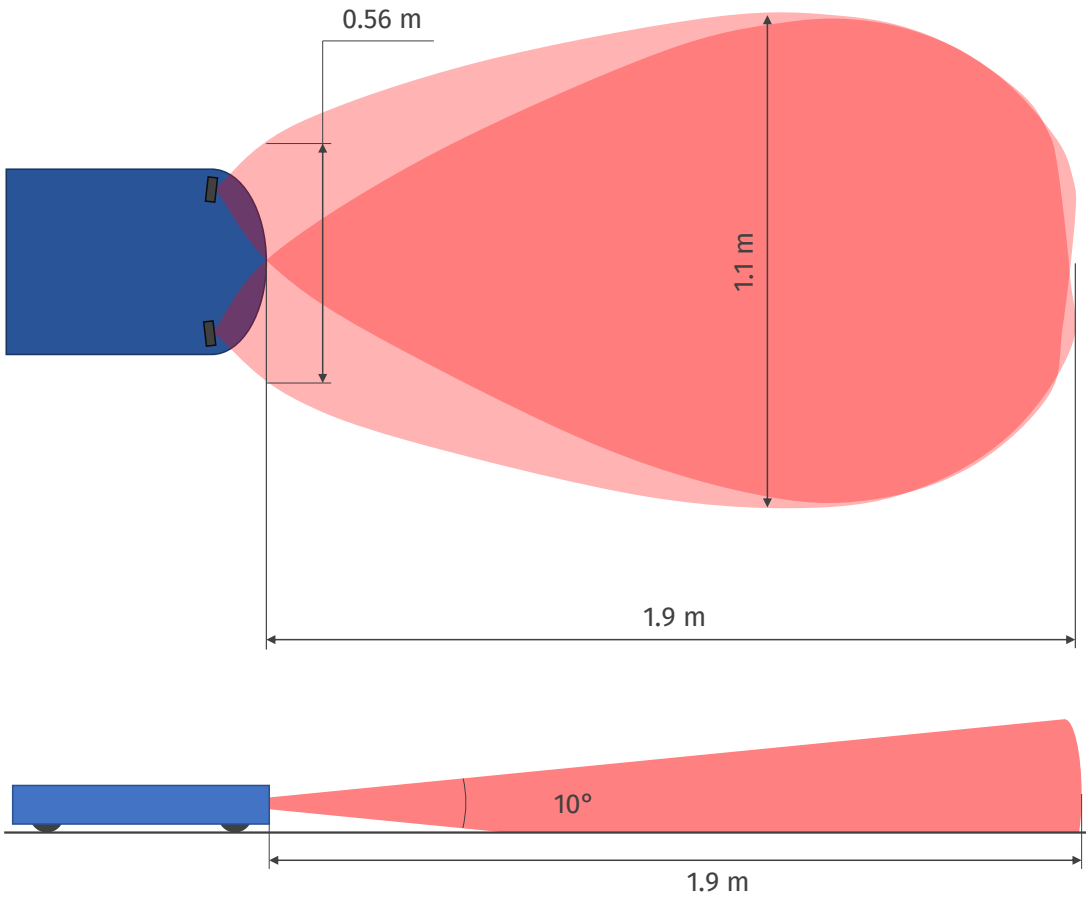


Figure 5.19: Possible disposition of the ultrasonic sensors.

a possible solution, since the lack of navigation data is not a major problem. This type of AGVs are beyond the scope of the present study, however this option could be worth some consideration and further testing.

Chapter 6

Future improvements

This chapter contains an introduction to arguments that go beyond the scope of the present document. At first, it will be briefly suggested how to move forward in the ultrasonic sensors implementation via testing. The mobile robots that would benefit from this solution are not present in the company's range of vehicles, so a precise and detailed testing phase is not required. After presenting the current solutions and the possible improvements that can take place right now, a different point of view is taken by improvements that rely on technological advancements. This is the case of 3D solid state Lidar, a cutting-edge technological solution for producing 3D images of a scene and use them for navigation.

6.1 Test campaign of ultrasonic sensors

Implementation of different technologies in a current system requires different phases of testing, trial and error. After mounting the ultrasonic sensors on the AGV, the detection tests must be carried out. EN 1525 [6] gives the minimum required tests that need to be carried out in order to confirm the expected safety performance.

Since sound waves react differently to different materials, the test specimens must be various. For example, cylinders with velvet cloth wrapped around are a good representation of human legs. Generally speaking, spongy materials diffuse sound waves better, and are the harder to detect.

Apart from clothes, also different shapes are detected differently. In fact, highly diffusing shapes like cones are found to be extremely hard to detect. Nevertheless, the main application of the safety system is to ensure personal safety, so these shapes are really far from the shape of the human body and should not be considered.

More information on the ultrasonic technology applications can be found on the "Technology Guide for Ultrasonics" by Pepperl+Fuchs [15].

6.2 Solid state lidar

The future of autonomous navigation in vehicles and robotics will likely depend on Light Detection and Ranging (LiDAR) technology. The latest innovation in this technology is solid-state LiDAR, which is gaining traction as a promising technology that is cheaper, faster, and provides higher resolution than traditional LiDAR. Interestingly, the manufacturers' predictions state that the price of these components could eventually fall below $100 per unit.

The traditional lidar systems discussed earlier in this paper are electromechanical: they rely on moving parts that have to be precise and accurate in order to obtain measurements suitable for autonomous navigation. These measurements come from photons from a laser, which then reflect back off surfaces and concentrate into a collector that can determine the distances of these objects. The laser and collector must rotate in order to scan the area around it. The moving parts involved put a restriction on the size of the system, since making them small and compact would increase the difficulties in the precise manufacturing required, which then drives up cost.

Solid-state LiDAR on the other hand is a system built entirely on a silicon chip. No moving parts are involved, which not only makes more resilient to vibrations, but can be made smaller much more easily. This lends to production being cheaper.

Many companies are moving towards this technology right now. Among them, Panasonic plans to develop a 3D Lidar with a field of view of 270° horizontal and 60° vertical. The sensor will be able to detect at a maximum of 50 m distance and connect via Ethernet.

Figure 6.1: Implementation example of a 3D Solid State Lidar on the front of a self driving car.

Chapter 7

Conclusions

This master thesis revolved around the topic of personal safety in an industrial environment. It is the result of a research carried out at InSystems Automation GmbH, a company that manufactures flexible and personalized AGV solutions.

In the first part of the document (chapter 2) various safety norms have been described. The starting point is that an Automated Guided Vehicle has to operate in an industrial environment without increasing the hazard levels of the plant. A safety system, in its most generic aspect, must then reduce the hazard coming from industrial machines and equipment. In its simplest form it consists of an input device, a logic device and an output device. The main characteristics of a safety system are the structure, the reliability of components, the self-diagnostic functions and the resistance to common cause failures. All these aspect need to be considered when going through the design workflow, which starts with the identification of the single safety function (for example the stop initiated by a safe guard). All the process can also be computer-aided using software like SISTEMA [25].

The theoretical description is followed in chapter 3 by a walk-though of the current safety systems that are used in the proANT robots. Each of them carries out the three basic safety functions: safe stop initiated by emergency stop button, safe stop initiated by laser scanner and dynamic safety field switch according to speed. Each safety function is then treated independently and the safety performance level is calculated step by step for the first safety function of the proANT 436. This process allows to better understand the function block diagrams, that are a fundamental part of the schematizing of safety systems, as well as the workflow that was previously described. After that, the components used in the system are described, with particular emphasis on complex components like laser scanners. Those are used not only for safety, but also for the navigation of the robots inside a plant. Apart from being the most complex component, the laser scanner is also the most expensive, taking three quarters of the overall cost of the safety system.

After describing the safety system used in the proANT vehicles, chapter 4 contains an

analysis of the competitors. Mobile robots from 13 different manufacturers are divided into four different types: forklift, differential drive, omni-wheel platform, magnetic or wire guided. Every type has similar aspects but also different functions that need to be carried out by different types of sensors. A common thread is however observed: all the AGVs use laser scanners to ensure personal safety. This is particularly interesting when dealing with line guided AGVs that don't need information about their position but still use laser scanners.

Since the main safety function of the laser scanner is to detect obstacles in front of the vehicle, and since this is the most expensive components, chapter 5 is focused on giving possible alternatives to this detecting technology. Studying the usage of different solutions brings more awareness to the actual problem: for example, it becomes clear how the usage of cameras instead of laser scanners adds more unnecessary complications, despite seeming a rather viable solution. Also the use of a different laser scanner from another manufacturer seems like a good way to reduce cost. However, when facing the programming effort needed to interface the new module with safety and navigation software, it is clear that for low production volumes this is not convenient.

Lastly, the possibility of using ultrasonic sensors to detect obstacles seems like the most suitable solution. In fact, the cost of the ultrasonic sensors is half the cost of a laser scanner. Ultrasonic sensors however cannot give any information about the position of the robot in the plant, so another lidar sensor would be needed for navigation. This is the case for natural navigation robots, however some types of AGVs (like magnetic or line guided platforms) could benefit from these sensors since they do not need any data about the surrounding environment. For this reason, chapter 6 gives some suggestions about the deployment of ultrasonic sensors in AGVs. The chapter then ends with some hints about the new developing technology of solid state 3D lidar.

Bibliography

[1] ISO 12100:2010. *Safety of machinery — General principles for design — Risk assessment and risk reduction*. Standard. International Organization for Standardization, 2010.

[2] BS EN ISO 13849-1:2015. *Safety of machinery. Safety-related parts of control systems. General principles for design*. Standard. British Standards Institution, 2015.

[3] BS EN ISO 13849-2:2012. *Safety of machinery — Safety related parts of control systems - Part 2: Validation*. Standard. British Standards Institution, 2012.

[4] BS EN ISO 13850:2015. *Safety of machinery — Emergency stop function — Principles for design*. Standard. British Standards Institution, 2015.

[5] BS EN ISO 13855:2010. *Safety of machinery — Positioning of safeguards with respect to the approach speeds of parts of the human body*. Standard. British Standards Institution, 2010.

[6] BS EN 1525:1998. *Safety of industrial trucks — Driverless trucks and their systems*. Standard. British Standards Institution, 1998.

[7] BS EN 954-1 : 1997. *Safety of machinery - Safety related parts of control systems - Part 1. General principles for design*. Standard. 1997.

[8] BGIA Report 2/2008e. *Functional safety of machine controls - Application of EN ISO 13849*. Report. German Social Accident Insurance (DGUV), 2009.

[9] BS EN 418:19928. *Safety of machinery — Emergency stop equipment, functional aspects — Principles for design*. Standard. British Standards Institution, 1992.

[10] PD IEC/TS 61496-4-3. *Safety of machinery — Electro-sensitive protective equipment*. Standard. British Standards Institution, 2015.

[11] BS EN IEC 61496-3:2019. *Safety of machinery - Electrosensitive protective equipment*. Standard. British Standards Institution, 2019.

[12] Henrik Andreasson et al. "Autonomous transport vehicles: Where we are and what is missing". In: *IEEE Robotics and Automation Magazine* 22.1 (2015), pp. 64–75.

[13] Rockwell Automation. *Safety Function: Safety Camera*. Dec. 1, 2013. URL: `http://literature.rockwellautomation.com/idc/groups/literature/documents/at/safety-at114_-en-p.pdf`.

[14] Sobers Lourdu Xavier Francis et al. "A ToF-Camera as a 3D Vision Sensor for Autonomous Mobile Robotics". In: *International Journal of Advanced Robotic Systems* 12.11 (2015), p. 156. DOI: 10.5772/61348. eprint: https://doi.org/10.5772/61348. URL: https://doi.org/10.5772/61348.

[15] Pepperl Fuchs. *Technology Guide for Ultrasonics*. URL: https://www.pepperl-fuchs.com/global/en/36955.htm.

[16] Mayser GmbH. *Ultrasonic industrial sensor USi Safety*. URL: https://www.mayser.com/media/895/download/BA-USi-safety_EN.pdf?v=1.

[17] Roni-Jussi Halme et al. "Review of vision-based safety systems for human-robot collaboration". In: *Procedia CIRP* 72 (2018), pp. 111–116.

[18] Georg Halmetschlager-Funek et al. "An empirical evaluation of ten depth cameras: Bias, precision, lateral noise, different lighting conditions and materials, and multiple sensor setups in indoor environments". In: *IEEE Robotics and Automation Magazine* 26.1 (2018), pp. 67–77.

[19] *Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA)*. URL: https://www.dguv.de/ifa/index-2.jsp.

[20] Seongsoo Lee and Sukhan Lee. "Embedded visual SLAM: Applications for low-cost consumer robots". In: *IEEE Robotics and Automation Magazine* 20.4 (2013), pp. 83–95.

[21] Jens Lienig and Hans Bruemmer. *Fundamentals of electronic systems design*. Springer, 2017.

[22] Stefan May et al. "3D time-of-flight cameras for mobile robotics". In: *2006 IEEE/RSJ International Conference on Intelligent Robots and Systems* (2006).

[23] Sick. *Guide for Safe Machinery*. July 7, 2015. URL: https://cdn.sick.com/media/docs/8/78/678/Special_information_Guide_for_Safe_Machinery_en_IM0014678.PDF.

[24] Sick. *Sick S300 Expert User Guide*. Apr. 17, 2019. URL: https://cdn.sick.com/media/docs/9/79/379/Product_overview_Opto_Electronic_Protective_Devices_en_IM0069379.PDF.

[25] *Software-Assistent SISTEMA: Safety Integrity Software Tool for the Evaluation of Machine Applications*. 2019. URL: https://www.dguv.de/ifa/praxishilfen/practical-solutions-machine-safety/software-sistema/index.jsp.

[26] *Web page Beckhoff EL6900 | TwinSAFE Logic*. URL: https://www.beckhoff.com/EL6900/.

[27] *Web page ROS*. URL: https://www.ros.org/.

[28] *Web page Tesla Autopilot*. URL: https://www.tesla.com/autopilot?redirect=no.