Autonomous Vehicles on the Factory Floor: An Approach to Safety

Ana Margarida Trigo
Centre Algoritmi, AE/LOG-Brg
University of Minho, Bosch
Guimarães, Portugal
trigo@ieee.org
0000-0003-1624-8732

Toni Machado
AE/LOG-Brg
Bosch
Braga, Portugal
toni.machado@pt.bosch.com
0000-0002-8286-3496

Tiago Malheiro
Department of Industrial Electronics,
Centre Algoritmi
University of Minho
Guimarães, Portugal
tmalheiro@dei.uminho.pt
0000-0001-7462-5765

Luís Louro
Centre Algoritmi
University of Minho
Guimarães, Portugal
llouro@dei.uminho.pt
0000-0003-1708-8881

Alberto Fonseca
Equipment Safety and Engineering Department
CATIM – Technological Centre for Metalworking Industry
alberto.fonseca@catim.pt

Sérgio Monteiro
Department of Industrial Electronics,
Centre Algoritmi
University of Minho
Guimarães, Portugal
sergio@dei.uminho.pt
0000-0002-5028-0974

Estela Bicho
Department of Industrial Electronics,
Centre Algoritmi
University of Minho
Guimarães, Portugal
estela.bicho@dei.uminho.pt
0000-0003-2715-4037

2021 IEEE 30th International Symposium on Industrial Electronics (ISIE) | 978-1-7281-9023-5/21/$31.00 ©2021 IEEE | DOI: 10.1109/ISIE45552.2021.9576211

***Abstract*— This paper provides insights into a safety assurance procedure and its application in an Autonomous Vehicle (AV) solution. The product, object of study, is composed of a kit that is integrated into a stacker forklift truck to add autonomous features to the exclusively manually driven vehicle. Integrating the kit in the conventional vehicle gives new applications to the machine, making the CE marking, previously affixed, no longer valid. The focus of this work is the safety assurance of the solution incorporated in the vehicle. After implementing the procedure, the AV solution is ready to start the last stage of the proof-of-concept phase: to operate in the factory environment. The factory environment will be shared with humans and other vehicles operated by humans, increasing the need for behavior reliability.**

***Keywords*— autonomous vehicles, driverless industrial trucks, safety management, Machinery Directive, industry 4.0**

I. Introduction

Organizations need to comply with legal requirements to be able to sell their products and services. Product designers and engineers should address occupational health and safety issues in all phases of the product's lifecycle. With the increasing complexity of systems and the introduction of smart systems on factory floors, new challenges arise.

The work here presented is part of a project being developed in the consortium between the University of Minho and Bosch Car Multimedia. It has the potential to habilitate industry 4.0 in the intralogistics field, allowing the reuse of conventional vehicles already in operation. This project - designated Smart Autonomous Mobile Units (SAMU) - intends to develop AV solutions for the autonomous transportation of materials and end products, in dynamic environments shared with human operators and other vehicles. Thus, safety and behavior reliability are of paramount importance. Three parts compose a SAMU: 1) a conventional intralogistics vehicle (e.g. stacker forklift truck); 2) a kit, henceforth cited as SAMU-kit, that has hardware control modules (including firmware), and several components that are available in the market, for instance, safety LIDAR's or safety relays; and 3) software, hereafter called by SAMU-sw. The goal is to use the developed SAMU-kit+SAMU-sw to convert conventional (human-operated) vehicles into autonomous vehicles. Previous SAMU project publications featuring motion control for autonomous tugger and stacker vehicles in dynamic factory floors shared with human operators are reported in [1], [2].

Automated systems are used to facilitate human work, but are limited in the decision-making ability, requiring human intervention. In contrast, autonomous systems are capable of deciding by themselves how to proceed, with little human intervention [3]. One challenge of autonomous solutions concerns safety in the operation of a system that makes decisions by itself. Safety is defined in ISO 26262-1:2018, "Functional Safety – Part 1: Vocabulary", as the absence of unreasonable risk [4]. An option to eliminate risk regards the definition of an operational safety concept, which will enable the implementation of measures to decrease risks and ideally, mitigate them [5]. Note that some researchers consider that the standard was not designed pondering autonomous vehicles solutions [6].

In the European single market, Machinery Directive 2006/42/EC is the main legislation regarding the free movement of machines within the single market. Moreover, the directive states mandatory Essential Health and Safety Requirements (EHSR) [7]. This means that the customer can rely on the equipment with CE marking affixed, since it complies with the demanding level of safety protection of employees and the users of the equipment, as well as other goods. European access law website, EUR-lex [8], should be

978-1-7281-9023-5/21/$31.00 ©2021 IEEE

checked periodically to assure the legal acts and the harmonized standards in force. ISO 12100 "Safety of Machinery - General principles for design - Risk assessment and risk reduction" [9] is one of the harmonized standards and should be followed to safety assurance. ISO 12100 standard defines a structure for a set of standards that are divided into three groups: type-A standards, which are basic safety standards; type-B1 for particular safety aspects and type-B2 for safeguards; and type-C, related with machine-specific technical standards. To notice that requirements established on type-C standards take precedent over the requirements included on type-B or type-A standards. European Directives were developed considering unconnected and static systems, where safety can be assessed with higher reliability [10]. With the industry 4.0 revolution, new challenges and standards for dynamic systems are required by manufacturers. Although recent standards are published, such as ISO 3691-4:2020 "Safety requirements and verification — Part 4: Driverless industrial trucks and their systems" [11], the variety of scenarios with autonomous vehicles demands a careful look for each application. Another key standard to the automotive industry, previously mentioned is ISO 26262. Nonetheless, AVs are out of the scope since this standard has the human driver accountable for safety [12] [13].

Safety assurance of autonomous systems cannot be done in a single step [3]. Instead, it should consider the product lifecycle. There is uncertainty regarding the aspects that will be subject to regulation. Original Equipment Manufacturers (OEMs) use miles of driving as a key performance indicator (KPI) for autonomous cars' safety. RAND published an article that demonstrates it would take hundreds of millions of miles to assure autonomous car reliability. It would take hundreds of years, with the existing fleets, to achieve the number of miles required [14]. Although intralogistics vehicles operate indoor, safety is likewise a challenge.

Companies providing intralogistics vehicles with autonomous functionalities comply with harmonized standards. For instance, MiR500 [15] comply with ISO 13849-1:2015 "Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design" [16], ISO 13849-2:2012 "Safety of machinery - Safety-related parts of control systems - Part 2: Validation" [17], OMRON LD series adds ISO 12100 [18] to the previous standards and KUKA also includes ISO 3691-4:2020 [19]. Nevertheless, companies do not share how they are implementing the safety requirements or safety approaches within the organizations. Hence, the literature reveals a gap in the safety topic for the application of AV technology on powered trucks that operate in environments shared with people and other goods. After the work to qualify SAMUv1 to operate on the factory floor, we decided to disseminate the knowledge obtained during this process, contributing to close this gap.

This paper researches the procedure developed to qualify SAMU vehicles as safe to operate in intralogistics facilities. The safety procedure is based on the Machinery Directive [7], mandatory for machines commercialized in the European single market. In this directive's scope, SAMU-kit's commercialization requires a notified body's participation, since it is classified as a 'safety component'. Results presented in this paper regards SAMU version 1 (SAMUv1), which corresponds to incorporating the SAMU-kit and SAMU-sw in conventional stacker forklift trucks (Fig. 1). The operation area of SAMUv1 is shared with people and goods, which requires the implementation of additional safety measures to guarantee the safety and integrity of people and property. We believe this is a valuable contribution since the literature reveals a gap on the safety topic for the application of AV technology on powered trucks that operate in environments shared with people and other goods (c.f. Section II). Companies providing intralogistics vehicles with autonomous functionalities do not share how they implement the safety requirements, maintaining the approaches within the organization.



Fig. 1. SAMUv1, Stacker forklift truck with SAMU-kit and SAMU-sw, a full service video is available in https://youtu.be/9J4aLRy2-Mc[2].

The remainder of the paper is structured as follows: section II constitutes a guideline to use for autonomous systems, and for each step of the safety assurance procedure, the work refined with SAMUv1 use case, is disclosed. The paper ends with conclusions and an outlook for future work in the section III.

II. Autonomous Vehicle Safety Approach to SAMUv1 Use Case

The safety assurance procedure can have modifications according to the nature of the product in construction. However, a typical structure can be applied in a machinery safety process, shown in Fig. 2.

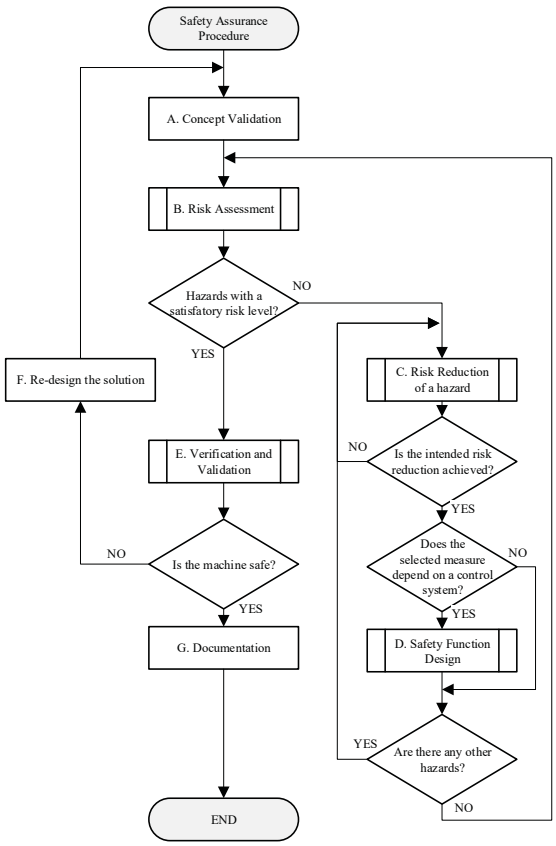


Fig. 2. Safety Assurance Procedure Overview, based on [9], [16] and [17].

Each task is briefly explained in the following subsections, and it is identified with the corresponding character of each step illustrated in Fig. 2.

A. Concept Validation

The concept validation concerns the identification of safety requirements. These should be searched within the regulations, standards, or norms applicable to the system in analysis. User and machine specifications should also be collected, including a description of the machine lifecycle phases, technical drawings and relevant technical documents. For the SAMUv1 application, TABLE I lists key requirements applicable to the SAMUv1 solution.

TABLE I. KEY SAFETY REQUIREMENTS APPLICABLE TO SAMUV1 SOLUTION, BASED ON [11].

Safety Requirement Description	ID
Electrical requirements shall comply with EN 1175 series [20].	SR1
The driverless truck must have a system to detect persons in the truck's path, also referred to as personnel detection means.	SR2
Safety distances shall comply with ISO 13857 [21], which covers distances to prevent reach or access by upper and lower limbs.	SR3
The braking system should be designed to stop the truck within the operating range of the personnel detection means for the worst-case scenario conditions.	SR4
After a detected person moves out of the protective field, the truck may restart automatically only after 2 seconds and following appropriate visual and/or acoustic warnings.	SR5
If it is impossible to guarantee the stop before contact, the AV speed shall not exceed 0.3 m/s.	SR6
Maximum speed must be defined as 0.3 m/s if the personnel detection means is muted.	SR7
A stopping device, for instance, a manual emergency stop button, shall be within 600 mm from the hazardous point. Automatic restart shall not be permitted after the emergency stop button has been activated.	SR8
A mode selector shall be placed in the machine to operate in manual and autonomous mode. Unauthorized and/or incorrect mode selection shall be prevented by suitable means. Only authorized and trained personnel may select the operational mode or operate the truck.	SR9
The presence of the operator shall deactivate all automated functions.	SR10
When in manual control, the truck should stop all movements in case of loss of control and the personnel detection means may be deactivated.	SR11
Deactivation of a manual control shall not cause activation of the automatic mode.	SR12
When in autonomous mode of operation, the truck should not transport persons.	SR13
The zones classified as "Operating Hazards", such as the load transfer area, must be identified as such, once these areas correspond to operation modes where the personnel detection means are muted [11].	SR14
Performance Level required (PLr) of safety-related parts of control systems: • Braking system-control, PLr d; • Personnel detection system, PLr d; • Automatic battery charging, PLr b; • Emergency stop, PLr c; • Automatic Manual and Maintenance modes, PLr c.	SR15

The standard ISO 5053-1:2015 defines a driverless truck as a "powered truck including any trailers, designed to travel automatically in which the safety of operation does not depend on an operator" [22]. SAMU solution is a driverless truck, and it has to comply with type-C standard ISO 3691-4:2020 [11]. For type-B standards, ISO 13849-1:2015 [16] and ISO 13849-2:2012 [17] were adopted. As a type-A standard, ISO 12100:2010 is followed. Acquiring standards and identifying the applicable requirements is crucial to develop a successful safety procedure.

In future versions of the SAMU project, the concept validation will be reapplied, and unless standards suffer revisions or a new applicable standard is published, this will be a short step to revisit.

B. Risk Assessment

According to clause 5 of ISO 12100, the risk assessment is composed of the Risk Analysis and the Risk Evaluation [9], as Fig. 3 exhibits. The risk assessment is revisited along with the procedure whenever needed and especially after implementing risk reduction measures, to confirm if there are no new hazards to be considered.

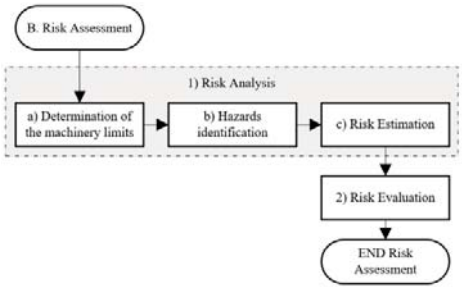


Fig. 3. Schematic representation of risk assessment process based on [9].

1) Risk Analysis

The risk analysis is composed of the following steps: a) determination of the machinery limits; b) hazards identification; and c) risk estimation.

a) Determination of the limits of the machine

The constraints of the machine through all the machine lifecycle phases should be analyzed. Machine lifecycle includes: transport assembly and installation; commissioning; operation; cleaning; maintenance; fault-finding or troubleshooting; dismantling or disabling [9]. The outcome should be a machine specification comprising the machine properties description, functional capabilities and conditions expected of the operational environment.

Initial tests were made to confirm the specifications of the stacker forklift truck used for SAMUv1. For instance, the braking system was tested using a sample of measures performed for several speeds and for the conditions with load and no load. These tests are helpful to find how well the vehicle operates in limited conditions such as speed or steering. Moreover, these tests allow the analysis of conditions to implement the safety requirement SR4.

The specification of the machine limits was established, and the machine's available information, such as electrical schematics, SAMU kit components information and vehicle dimensions, were collected. The analysis of the electrical schematics allows the verification of compliance with the safety requirement SR1.

b) Hazards Identification

The approach adopted to identify hazards was the brainstorming method. Initially, the hazards identification

from other stackers and Automated Guided Vehicles (AGVs) were searched to find common hazards. Several sessions took place with the development team, including a machinery safety expert. ISO/TR 14121-2:2012 "Safety of machinery — Risk assessment — Part 2: Practical guidance and examples of methods" [23] can be consulted. A list of the initial hazards covers the lifetime of the machine, including maintenance and staff training. Table II shows an example of SAMUv1 hazard description and the hazards identification list structure. Note that the initial risk assessment does not include the safety systems installed, such as the detection of obstacles.

TABLE II. STRUCTURE OF THE HAZARD IDENTIFICATION LIST.

List Structure	Example of a hazard of SAMUv1
1. Task or Operation	Autonomous navigation from a point to another
2. Hazard Zone	Machine surroundings
3. Origin related to…	Autonomous vehicle movement
4. Potential Consequences	Collision or impact with people or goods
5. Hazardous Situation	Operation is done close to people or goods
6. Hazardous Event	Goods or people are not detected
7. Possible Solution	Incorporate safety sensors to detect obstacles in the path of the truck to give the command to stop the AV if people or goods are detected

c) Risk Estimation

The risk estimation can be done by scoring the severity of harm and the probability of its occurrence. The severity of harm is attributed using two considerations: if it is classified as slight, severe, or death; and if it affects only one person or several individuals. The probability of occurrence of harm is recognized considering: (i) the exposure of people to the harm, (ii) the occurrence of a hazardous event, and (iii) the possibility of avoiding or limiting the harm. Several risk estimation tools can be applied, for instance, risk matrix, risk graph, or numerical scoring are referred on ISO/TR 14121-2:2012 [23]. Each team can choose the tool that better fits the defined purpose and safety strategy.

For SAMUv1, we used the risk estimation matrix. Each team member does an individual estimation of the severity of the risks (S) and the likelihood for the risks to occur (L). The *severity* of the risk is classified in 4 levels: 1 – acceptable, 2 – tolerable, 3 – undesirable and 4 – intolerable. The *likelihood* for the risks to occur is classified among 4 levels: 1 – remote, 2 – improbable, 3 – possible and 4 – probable. After the individual estimation is completed, in a team session, the estimation attributed for a risk is discussed, and the worst estimation is always considered, unless a good argument is conceived and accepted by all the team members.

2) Risk Evaluation

After the risk analysis is settled, it is necessary to determine if a risk reduction is needed. The risk evaluation defines which hazards will be considered to perform a risk reduction and mitigation. If the identified risks have a satisfactory risk level, the manufacturer can begin the verification and validation phase. From the evaluation of the risks identified for SAMUv1, the risks classified as extreme and high (see "Initial Risk Level", TABLE III) are the priority to work on. The remaining risks are likely to be mitigated with the measures implemented for the higher level risks.

C. Risk Reduction and Risk Mitigation of a Hazard

Risk reduction and risk mitigation can be done following the three steps method illustrated in Fig. 4.

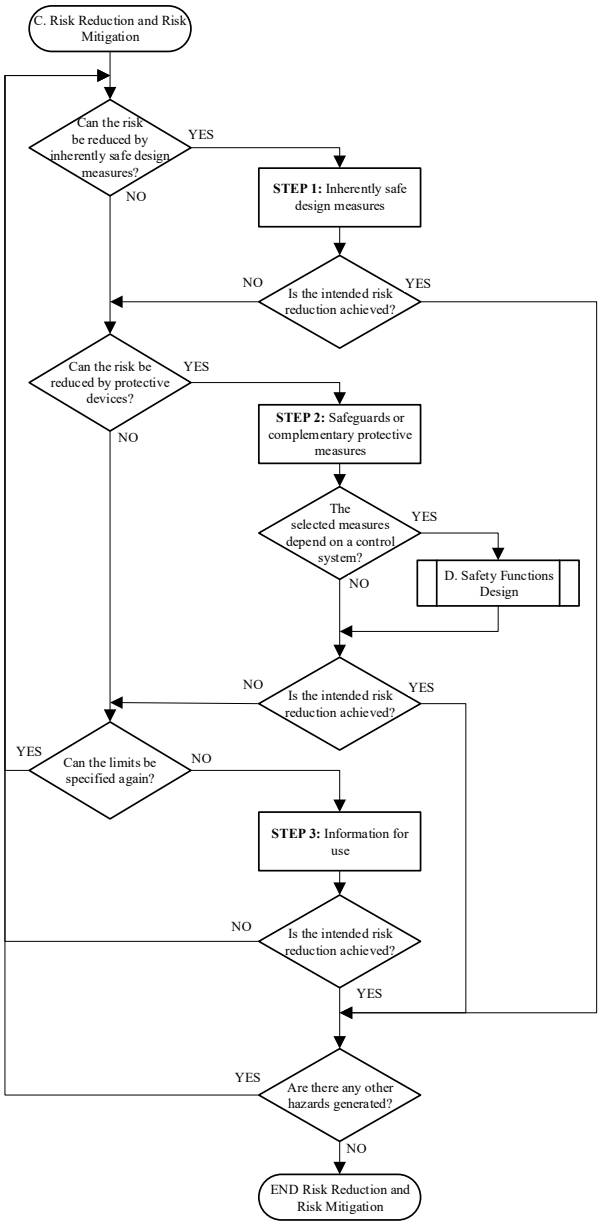


Fig. 4. Risk Reduction and Risk Mitigation of a Hazard based on ISO 12100 [9].

The first step is the elimination of hazards by design. For SAMUv1, step 1 does not apply in any of the hazards identified. The next step is reduction through safeguarding or using complementary measures. In the following subsection, safety functions are presented as part of step 2. To comply with SR13 additional components were added, namely a sensor to stop the vehicle if an operator tries to be transported when in autonomous mode. This last measure, plus the manual interference with the tiller-arm or pushing any of its buttons, leads to the deactivation of all automated functions, conforming with SR10. These extra inputs to stop the machine were added in the same branch of the emergency stop button already part of the vehicle. If one of the inputs is activated, the vehicle stops. Step 3 corresponds to complement the safety with information of use. For SAMUv1, this information integrates the training requirements to operate the machine. To

comply with SR14, the information identifying the "operating hazards" corresponds to the load and unload zones, where the system to detect persons in the forks zone has to be muted to be possible to perform the load and unload task.

TABLE III. INITIAL RISKS EVALUATION AND RISKS RE-EVALUATION.

Task or Operation / Potential Consequences	S	L	Initial Risk Level	S	L	Re-evaluation Risk Level
Navigation / Collision or impact with people or goods	3	3	Extreme	3	1	Medium
Navigation / People Trapped	3	2	High	2	1	Low
Navigation / People Crushed	4	2	High	2	1	Low
Move to… / Collision or impact with people or goods	2	2	Medium	2	1	Low
Move to… / People Trapped	3	2	High	3	1	Medium
Move to / People Crushed	4	2	High	4	1	Medium
Pick load with forks/ People Trapped	3	1	Medium	1	1	Low
Pick load with forks / Goods or people crushed between forks-pallet and upper shelf	3	1	Medium	1	1	Low
Drop load with forks / Collision or impact of the forks with people or goods	4	1	Medium	2	1	Low
Drop load with forks / Load Falls	4	1	Medium	2	1	Low
Drop load with forks / People Trapped	4	1	Medium	2	1	Low
Switch between modes of operation / The operational mode changes without the desire of the operator	4	3	Extreme	4	1	Medium

D. Safety Functions Design

When the risk reduction of a hazard is composed by a control system, a Safety Function (SF) needs to be defined and the performance of the safety related parts of the control system (SRP/CS) needs to be evaluated.

One guide to design a safety function is shown in Fig. 5. The performance level required (PLr) should be determined. PLr can be defined from **a** (lower risk) to **e** (higher risk), as represented in Fig. 6, using the following three risks parameters:

Parameter 1 – The severity of injury to be classified in slight (S1) or severe (S2);

Parameter 2 – The frequency and/or exposure times to hazard to be defined between short frequency/exposure (F1) or long frequency/exposure (F2);

Parameter 3 – The possibility of avoiding the hazard, in the possibility of avoiding or limiting harm (P1), or scarcely possible (P2).

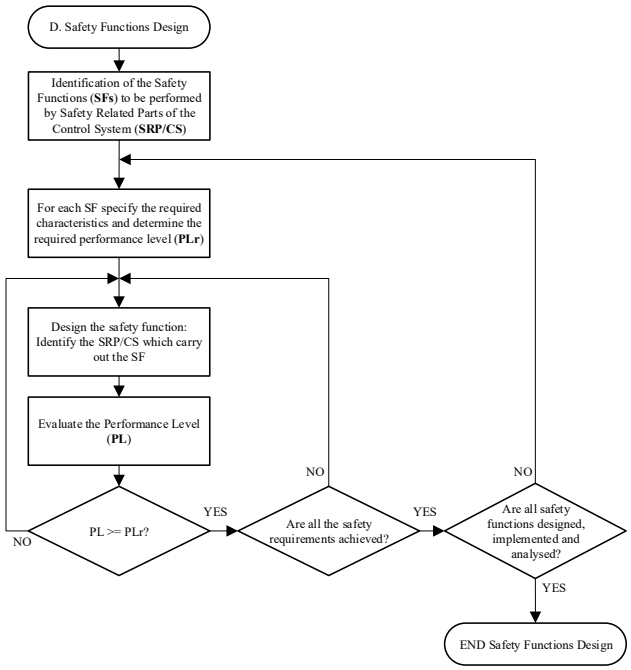


Fig. 5. Safety Functions Design based on ISO 13849-1:2015 [16].

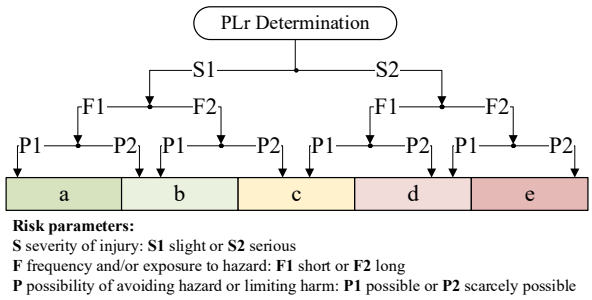


Fig. 6. Determination of PLr, based on ISO 13849-1:2015 [16].

With the PLr determined, the safety function should be designed with the SRP/CS to carry out the safety well defined. Following, the safety function should be represented in block diagrams to determine the performance level of the input, logic and output, respectively, PL_I, PL_L and PL_O and the interconnecting means, i_{ab}, i_{bc} (see Fig. 7).

Each safety function will have an evaluation of the performance level, considering the performance level of the input, logic and output elements. When PL ≥ PLr, the safety function is satisfactory and complies with safety requirements. In the next subsection, the five safety functions implemented on SAMUv1 are presented. Two aspects not implemented as SFs are part of the documentation. The first is related to the operation of SAMUv1 in two distinct operational modes: manual mode or autonomous mode. To comply with SR9 (see Table I), in the operational manual is the warning that only operators with additional training for this specific vehicle can be allowed to drive the machine. The other aspect regards SR12. The vehicle was designed to operate in autonomous mode by default, since future versions of the product, will exclusively operate in autonomous mode. This requirement is reported in the information of use.

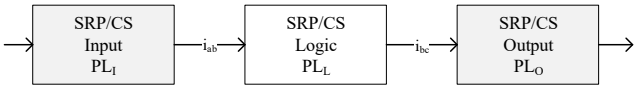


Fig. 7. Block Diagram representation of the SF components, based on [16].

1) *Safety Functions Design and Implementation*

a) *Safety Function SF1*

To comply with the safety requirement SR8 described in Table I, manual stop emergency pushbuttons were installed in the vehicle, one button on both lateral sides of the SAMUv1. These buttons can be activated in both operational modes (autonomous and manual), fulfilling the SR11. The block diagram of SF1 is represented in Fig. 8. The manual emergency-stop buttons have a turn to release the system, satisfying the SR5 since it does not allow an automatic restart.

It is important to note that the conventional vehicle drive (output) in both safety function SF1 and SF2 has PL c, meaning that, unfortunately, the SF PL will be level c in the best-case scenario, not fulfilling all the PL required by the safety requirement SR15. This has an impact on the overall system PL. Nevertheless, in this work's scope, the SAMU-kit as a safety component has the desirable PL.

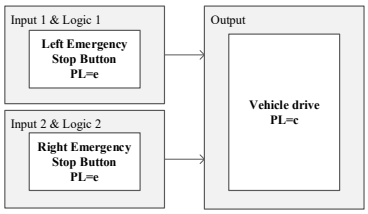


Fig. 8. Block diagram of Safety Function SF1 – Emergency Stop Buttons.

b) *Safety Function SF2*

The second safety function concerns the emergency stopping of the vehicle due to obstacles in the path. In other words, SF2 implements personnel detection means and satisfies the SR2 and the SR4 (Table I). The SF2 was designed using safety laser scanners and safety relays. This circuit is activated on the autonomous operation mode. The block diagram of SF2 is in Fig. 9.

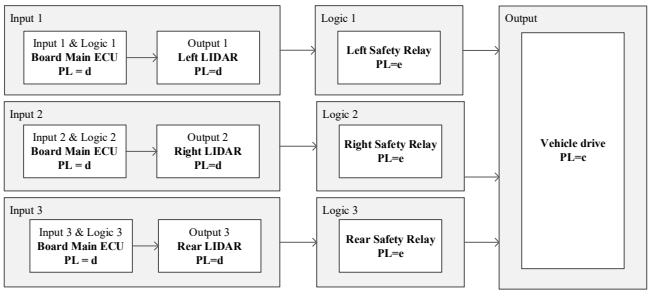


Fig. 9. Block diagram of Safety Function SF2.

c) *Safety Function SF3*

The third safety function resulted from the concerns of muting the detection means systems of personnel, having the same block diagram as SF2. To solve this issue, several measures were implemented in the system, low level, firmware. The concept of navigation state is defined considering the movement the vehicle has to execute. States defined are "move forward", “turn right”, “turn left” or “manoeuvre”. Each navigation state’s definition represents different movements that the vehicle has to be able to execute, and different speeds and steering angles ranges are established considering each different movement. In other words, each navigation state has a predefined protective field, a range of speed and a range steering angle. As an example, when the vehicle is in navigation state “turn right” it will operate with two conditions: 1) the vehicle is limited to operate with the steering angle between -5º and -50º; 2) the speed is limited to 0.5 m/s. Moreover, conditions are also implemented to guarantee safety when changing between different navigations states, such as verifying if the forks are in the right level to change to a certain navigation state.

The strategy of reduction by steps of the scanners protective fields (PFs) is applied for the load and unload tasks with a maximum speed of 0.25 m/s. Fig. 10 represents the protective fields defined for the tasks done in the operating hazards zones. This measure reduces the risk, since the protective field is reduced progressively when executing the load and unloading tasks. The vehicle behavior can cope with conflicting situations, for example, when a pallet is removed, or when the PFs are obstructed, the vehicle waits until the pallet is in place or the path is clear to continue the task. The SF3 satisfies safety requirement SR3 with the protective fields’ definition to each navigation state and SR6 and SR7 by limiting the speed to 0.25 m/s when the personnel detection means is muted.

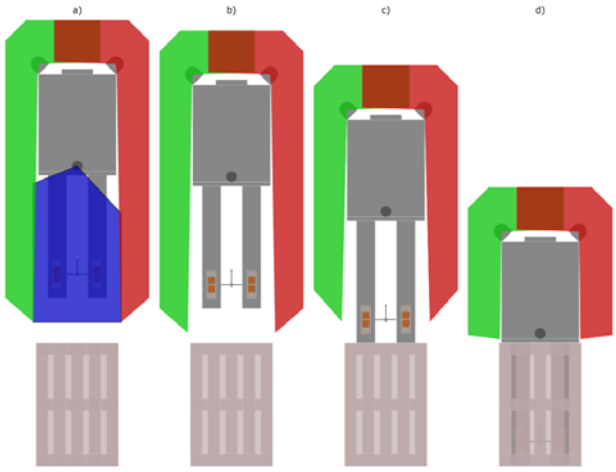


Fig. 10. Progressive decreasing in 3 steps of the protective fields when in picking operation.

d) *Safety Function SF4*

The fourth safety function respects the exchange between operations modes. The safety focus resides in the commutation from manual operation mode to autonomous operation mode to guarantee the activation of the system detection means for personnel. To guarantee the activation, two possible implementations are considered as possible solutions to be implemented in the future. The first one could be through the monitorization of the solid-state relays during the commutation. The second possible implementation could be done through the implementation of a checking routine. To allow the activation of the autonomous operation mode, the human driver must check the scanners. Only after the scanners’ protective fields are clear again (meaning the system detection means for personnel is activated) the vehicle is allowed to start the autonomous operations. The second implementation is considered to be more viable to include in the SAMUv1 and will be implemented in the future.

e) *Safety Function SF5*

The last designed and implemented safety function regards the fulfillment of SR13. To guarantee that the truck does not transport persons when in autonomous operation mode, a sensor was incorporated in the pedestrian platform to assure the platform is closed. If the platform goes down, meaning the

platform is in transport position, the vehicle will stop. The block diagram is shown in Fig. 11.

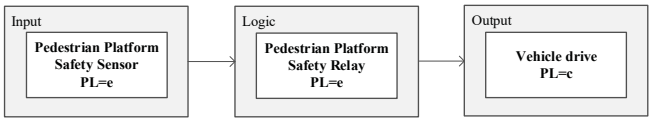


Fig. 11. Block diagram of Safety Function SF5.

2) Risk Assessment Re-evaluation

After implementing the designed safety functions, the re-evaluation of the risks concludes that all the risks initially classified as extreme and high are now classified as medium or low level of risk, Table III. This means SAMUv1 solution is ready to be verified and validated.

E. Verification and Validation

The verification and validation phase shall provide evidence that the implemented safety functions cover the safety requirements. A verification and validation plan is defined. The plan should include a fault list and verification tests for each component of the system, focusing on the safety functions parts. The validation of the system comprises the performance and the satisfaction of the requirements. One method used for software validation is the V&V (Verification and Validation) model. ISO 13849-2:2012 focuses on system validation and can be consulted for deeper knowledge [17].

For SAMUv1, this phase starts with the definition of a tests plan based on Rexroth "10 steps to Performance Level" manual [24]. The verification and validation phase was done in two parts. The first one comprised the verification and validation by analyzing the documentation of the solution. The second part fulfilled the tests plan. Table IV aggregates the performed tests and the obtained results. The group of tests includes the functional testing of all SFs, tests of the emergency stop buttons and the deactivation of autonomous operation mode. Furthermore, for each navigation state's worst-case scenarios, was tested if the implemented PFs allow the system to detect an obstacle and perform the emergency stop in the defined time and distance to an obstacle. The measurement of distances was done by measuring the distance between the front scanners and the obstacle, or between the closest front scanner to the obstacle and the distance between the obstacle and the center of the forks, Fig. 12. The time SAMUv1 takes to stop was calculated using the timestamp when one of the PFs is obstructed and the timestamp when the system stops. In Fig. 13 are some examples of the behavior testing when facing obstructions in the path [2]. Another group of tests concerns the analysis of the behavior when sending commands that firmware should not accept, such as sending speed parameters outside the predefined range of values for a certain navigation state.

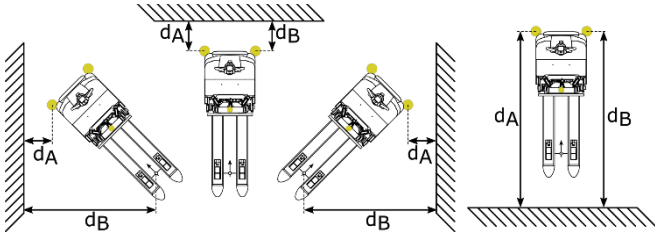


Fig. 12. Measurements of distances in the tests to calculate the stop distance of the vehicle to an obstacle.

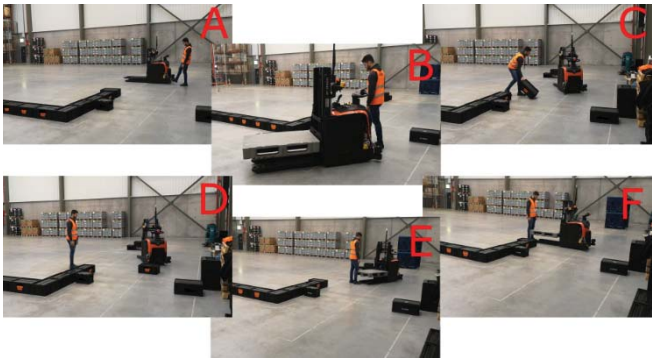


Fig. 13. Examples of performed tests: A and B, a person obstructs vehicle path; C and D, an obstacle is thrown to the vehicle path; E and F, Progressive decreasing of PFs on load and unload tasks.

TABLE IV. TESTS RESULTS.

Group of Tests Description	Overall Results
ID 1 – Safety Function 1, Emergency stop buttons.	All actions performed to test emergency safety buttons, with the machine stopped or moving, were successful.
ID 2 – Safety Function 2, Navigation states worst case scenario stopping distance.	It was confirmed that defined PFs to the navigation's states allow SAMUv1 to stop within a safety distance to the obstacle, never less than 250mm. It was used the approach shown in Fig. 12. Moreover, the vehicle was disturbed by human operators to verify its behavior (see Fig. 13 from A to D). PFs were also tested when powering on SAMUv1.
ID3 – Safety Function 3, Reduction by steps of the scanners PFs strategy, when performing the load and unload tasks.	The load and unload tasks were tested, with obstructions to the vehicle path (Fig. 13 E and F). The vehicle behaved as expected. Speeds above 0.25 m/s are not accepted by the system.
ID 4 – Safety Function 4, Commutation between manual and autonomous mode of operation.	The modes of operation were commuted several times, with the correct activation and deactivation of the system detection means for personnel.
ID 5 – Safety Function 5, Pedestrian platform sensor correct functioning.	After a person tries to get on the vehicle platform, the PFs are interrupted, which stops the vehicle. The platform sensor activates the manual operation mode, not allowing the movement of people while in autonomous mode.
ID 6 – Communication Protocol, Simultaneous commands.	When a person tries to activate the tiller arm, simultaneously with other commands from the hardware control module, it is verified that the system commutes to manual mode of operation, requiring human intervention to proceed in manual mode or to reactivate the autonomous mode of operation.
ID 7 – Firmware, Send parameters outside the predefined range of values to a certain navigation state.	For each navigation state, parameters outside the predefined range were sent and the system did not accept the commands, as expected.
ID 8 – Manually driven emergency stop button, Emergency stop button part of the vehicle manually driven.	The emergency stop button, already present in the powered truck, was tested and it is working as expected.
ID 9 – Complete service, Run complete services to verify SAMUv1 operation.	Starting from the parking zone, loading and unloading a pallet and returning to park, two different services were executed with success several times. These services had different load and unload zones.

All the tests performed have shown a robust system, fulfilling the safety requirements, TABLE I.

F. Redesign of the solution

Following the verification and validation results, if the solution does not show a high level of safety reliability or satisfactory functional performance, the system should be redesigned, considering the safety requirements collected.

SAMUv1 solution does not need to be redesigned, once the desired safety level was reached. Therefore, there are lessons learned to consider to the next version of the product development. A relevant fact to be mentioned concerns the modifications performed along with this safety procedure to the SAMUv1. For instance, as already referred, a sensor was introduced in the pedestrian platform to have the platform's position input, an encoder was placed to know the forks' position, and two manual stop emergency pushbuttons were incorporated in the solution. Initially, SAMUv1 had two scanners, and a third one was later integrated into the forks zone to reinforce the vehicle rear. Moreover, software routines were implemented to add progressive muting, through steps of the protective fields, when performing a task on the operating hazards zones, with the speed is limited to a maximum of 0.25 m/s by firmware.

G. Documentation of the process

The last step concerns the documentation of the safety process, to be used as evidence. The compilation of all the technical documents (schematics, components information, block diagrams, or process flow diagrams), the operational manual, the information of use, the information about the maintenance and the correct use of the machine, among other information are gathered.

III. Conclusions and Future Work

In future research with a focus on CE marking for SAMU-kit, a notified body will be required; hence the product to sell constitutes a safety component mentioned in point 21 of Annex IV of the European directive 2006/42/CE - Machinery Directive [7] with the intention to be incorporated in an indoor powered truck. From the work developed for SAMUv1, the safety procedure guarantees that measures were taken to avoid incidents while executing vehicles' ultimate tests (proof of concept). The result obtained for SAMU-kit is PL d. Unfortunately, the vehicle drive's performance level corresponds to PL c, meaning that the SAMUv1 safety functions' performance level will be in the best scenario level c. The drive of the powered truck must be analyzed before incorporating SAMU-kit to achieve a better PL. Another lesson learned corresponds to the test environment's corridor width in the industrial facility for SAMUv1 to operate. The corridor is narrower than the theoretical value. The reduction of PFs is performed carefully since the vehicle operates at lower speeds, and the reduction is meticulously tested in the verification and validation phase, and conditions are imposed at low level, firmware. With the required corridor width, the speed could be higher.

As a result of this research, new knowledge was assimilated, and it will be advantageous for future developments in the SAMU project. The introduction of autonomous systems should mitigate existing risks without introducing new ones. As previously mentioned, the complexity of systems is increasing. Legislation is needed, as well as metrics to compare different solutions. Researchers and developers should share safety approaches when developing autonomous systems and demonstrate that their solutions are safe by design and by default.

Acknowledgments

This work has been supported by FCT – Fundação para a Ciência e Tecnologia within the R&D Units Project Scope: UIDB/00319/2020 and by the scholarship PB/BDE/135106/2017 by FCT.

References

[1] L. Louro *et al.*, "Motion Control for Autonomous Tugger Vehicles in Dynamic Factory Floors Shared with Human Operators," *IECON Proc.*, vol. 2019-Octob, pp. 5255–5262, 2019.

[2] L. Louro *et al.*, "A safe autonomous stacker in human shared workspaces ∗," *IECON Proc.*, vol. 2020-Octob, pp. 4389–4396, 2020.

[3] S. Baruah, P. Lee, P. Sarathy, and M. Wolf, "Achieving Resiliency and Behavior Assurance in Autonomous Navigation: An Industry Perspective," *Proc. IEEE*, vol. 108, no. 7, pp. 1196–1207, 2020.

[4] ISO, "ISO 26262-1 Road vehicles - Functional Safety - Part 1: Vocabulary," 2018.

[5] M. Maurer, J. C. Gerdes, B. Lenz, and H. Winner, *Autonomous driving: Technical, legal and social aspects*. 2016.

[6] C. B. S. T. Molina, J. R. De Almeida, L. F. Vismari, R. I. R. Gonzalez, J. K. Naufal, and J. B. Camargo, "Assuring Fully Autonomous Vehicles Safety by Design: The Autonomous Vehicle Control (AVC) Module Strategy," *Proc. - 47th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Networks Work. DSN-W 2017*, pp. 16–21, 2017.

[7] European Commission, "Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC," *Off. J. Eur. Union*, 2006.

[8] European Commission, "EUR-lex, Access to European Union law." [Online]. Available: https://eur-lex.europa.eu/homepage.html.

[9] ISO, "ISO 12100:2010 Safety of Machinery - General principles for design - Risk assessment and risk reduction," 2010.

[10] S. Anastasi and L. Monica, "Evolution of European product directives in perspective of industry 4.0," *WIT Trans. Built Environ.*, vol. 174, pp. 163–168, 2018.

[11] ISO, "ISO 3691-4:2020 Industrial trucks — Safety requirements and verification — Part 4: Driverless industrial trucks and their systems," 2020.

[12] P. Koopman and M. Wagner, "Challenges in Autonomous Vehicle Testing and Validation," *SAE Int. J. Transp. Saf.*, vol. 4, no. 1, pp. 15–24, 2016.

[13] P. Koopman and M. Wagner, "Autonomous Vehicle Safety: An Interdisciplinary Challenge," *IEEE Intell. Transp. Syst. Mag.*, vol. 9, no. 1, pp. 90–96, 2017.

[14] N. Kalra and S. M. Paddock, "Driving to Safety - How Many Miles of Driving Would It Take to Demonstrate Autonomous Vehicle Reliability?," 2016.

[15] MiR, "MiR500 and MiR1000: Risk Analysis Guide v1 3," 2019.

[16] ISO, "ISO 13849-1:2015 Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design," 2015.

[17] ISO, "ISO 13849-2:2015 Safety of machinery — Safety-related parts of control systems — Part 2: Validation," 2015.

[18] OMRON, "Mobile Robots LD Series."

[19] KUKA, "Mobile Robots KMP1500." [Online]. Available: https://agv-distribution.com/wp-content/uploads/2020/05/KMP1500-agv-distribution.pdf.

[20] CEN, "DIN EN 1175 Safety of Industrial Trucks - Electrical/electronic requirements," 2018.

[21] ISO, "ISO 13857:2018-01 Safety of machinery – Safety distances to prevent hazard zones being reached by upper and lower limbs," 2018.

[22] ISO, "ISO 5053-1:2015 Industrial trucks — Terminology and Classification - Part 1: Types of industrial trucks," vol. 2015, 2015.

[23] ISO, "ISO/TR 14121-2:2012 Safety of machinery — Risk assessment — Part 2: Practical guidance and examples of methods," 2012.

[24] Rexroth Bosch Group, *Handbook for the Implementation of Functional Safety according to ISO 13849*. 2012.