A Risk-Informed Design Framework for Functional Safety System Design of Human–Robot Collaboration Applications

Wu, Jing; Ren, Junru; Ravn, Ole; Nalpantidis, Lazaros

Published in:
Safety

Link to article, DOI:
10.3390/safety11010024

Publication date:
2025

Document Version
Publisher's PDF, also known as Version of record

safety

MDPI

Article

A Risk-Informed Design Framework for Functional Safety System Design of Human–Robot Collaboration Applications

Jing Wu *, Junru Ren, Ole Ravn and Lazaros Nalpantidis

Department of Electrical and Photonics Engineering, Technical University of Denmark, 2800 Kongens Lyngby, Denmark; junre@dtu.dk (J.R.); oravn@dtu.dk (O.R.); lanalpa@dtu.dk (L.N.)
* Correspondence: jinwu@dtu.dk

Abstract: The safety of robotics and automation technologies is a significant concern for stakeholders in Industry 5.0. Ensuring cost-effectiveness and inherent safety requires applying the defense-in-depth principle. This paper introduces a novel risk-informed design framework for functional safety, integrating function-centered hazard identification and risk assessment via fault tree analysis (FTA). Demonstrated in the design of a semi-automated agricultural vehicle, the framework begins with a function-centered hazard identification approach (F-CHIA) based on ISO 12100. It examined design intents, identified hazard zones, and conducted task and function identification. Foreseeable functional hazardous situations are analyzed, leading to functional requirements and the identification of relevant directives, regulations, and standards. The F-CHIA outputs inform the functional safety analysis, assessing the required performance level and deriving specific requirements for software, hardware, and human operators using FTA. The functional requirements derived from F-CHIA are more systematic than traditional methods and serve as effective inputs for functional safety analysis in human–robot collaboration applications. The proposed framework enables design teams to focus on enhancing factors that improve functional safety performance levels, resulting in a more thorough and effective safety design process.

Keywords: risk-informed design; hazard identification; risk assessment; functional safety; robotics and automation systems

Academic Editor: Raphael Grzebieta

Received: 13 September 2024
Revised: 21 January 2025
Accepted: 25 January 2025
Published: 2 March 2025

Citation: Wu, J.; Ren, J.; Ravn, O.; Nalpantidis, L. A Risk-Informed Design Framework for Functional Safety System Design of Human–Robot Collaboration Applications. *Safety* **2025**, *11*, 24. https://doi.org/10.3390/safety11010024

1. Introduction

Safety in robotics and automation technologies [1] has become a major concern for stakeholders across various industries, including agriculture, manufacturing, and healthcare. As automation systems are increasingly deployed in diverse sectors, the importance of ensuring the health, safety, and environmental (HSE) protection of both operators and the relevant users cannot be overstated [2]. In the agricultural industry, for example, robots and automated systems are used to assist in tasks such as crop management, soil maintenance, and pesticide application. While these technologies can improve efficiency, they may also introduce new safety risks for workers, farmers, and bystanders [3]. The importance of managing occupational safety and health (OSH) is paramount, as these systems including digital components may introduce hazards that are not present in traditional machinery [4].

Risk assessment [5] has long been recognized as the cornerstone of HSE management, providing a structured process for identifying potential hazards and mitigating risks. However, despite its critical role, the robotics industry has no well-accepted risk assessment frameworks and mature methods [6,7]. Several studies suggest that existing safety standards for automated machines fail to address the unique challenges posed by complex

robotic systems, especially in human–robot collaboration (HRC) applications. Reference [8] pointed out that despite the available standards recognizing the paramount role of hazard analysis and risk assessment to appropriately implement safeguards in collaborative environments, the provision and/or revision of more specific guidelines seems to be desirable to best suit the collaborative context. Reference [9] investigated system-wide risk factor identification with the introduction of new technologies, highlighting that regulations often struggle to keep pace with technological advancements and remain more reactive than proactive. As stated in [10], going forward, as collaborative robot systems enable partial automation of tasks, HRC will continue to spread into workplaces and industries that might not have considered automation in the past. Rather than always being "caged" away from workers, more and more robot systems will be accessible to workers, yet human safety must still be protected. However, some advancements have been made. For instance, ref. [11] proposed a system-wide risk-awareness tool that adapts to evolving contexts where collaborative robots operate.

In addition, for automation technologies to meet high HSE protection standards, they must conform to regulatory requirements, such as the CE marking within the European Economic Area (EEA). The CE marking is a certification indicating that a product complies with HSE protection standards. However, achieving CE marking conformity is often hindered by the challenge of performing risk assessments early in the design phase. As ISO 12100 [12] recommends, risk assessments should ideally be conducted from the early design stages to identify hazards and assess risks before the product reaches the market. However, it is often unclear how designers, integrators, or users can orient design safeguards to outcomes of hazard analysis and risk assessment. Often, it is unclear which steps designers need to follow or which methods they can use to analyze hazards and assess risks, which may occur when robot systems and human co-workers perform collaborative/cooperative manufacturing tasks. Although a trend toward aligning requirements specified in the ISO/TS 15066 [13], ISO 10218-1 [14], and ISO 10218-2 [15] normative standards is discussed in several studies in the literature [16], a structured framework for orienting design safeguards in the normative standards to outcomes of hazard analysis and risk assessment is lacking. Furthermore, implementing an HRC application is difficult, mainly due to safety concerns and additional costs for safety measures. There are even indications that strict safety requirements are hampering the spread of HRC applications.

To address these challenges, a risk-based approach [17] initiated at the early stages of product design is essential. This approach emphasizes the need for comprehensive, adaptable, and proactive risk assessment frameworks tailored to the complexities of collaborative and autonomous systems. To tackle this challenge, a risk assessment framework during the early-phase design of an HRC application is proposed in this paper. Central to this framework is a function-centered hazard identification approach (F-CHIA). The F-CHIA identifies functional hazards and generates functional requirements specific to each identified hazard. These outputs are then used to inform the functional safety analysis, which assesses the required performance levels and derives specific requirements for software, hardware, and human operators through fault tree analysis (FTA). The framework was applied to a semi-automated agriculture tractor to design its functional safety system. It demonstrates the framework is feasible. The originality and advantageous features of this study are specifically summarized below:

I. The paper introduces a novel approach through F-CHIA to systematically link functional requirements with standards, addressing a critical gap in existing research. While reference [18] proposed combining robot type and application domain to identify relevant standards, this method is insufficient for systematically identifying standards that can prevent or mitigate function-centric hazards during the design phase. Our study focuses

on ensuring inherent safety from the start of the design process, a unique contribution that extends the scope of previous research.

II. The principles and procedures for using F-CHIA in the early design phase of a collaborative application are detailed through its application to a semi-automated agriculture tractor. The results not only inform the design of the functional safety system but also provide direct inputs for risk assessment, demonstrating how F-CHIA contributes to more efficient and safer robotic vehicle designs. This application highlights the practical utility of F-CHIA in enhancing design, analysis, and performance in ways that standard datasheets cannot achieve.

III. While the FTA in this study may present familiar information, its value lies in its systematic use of FTA to assess failure scenarios based on functional requirements identified through F-CHIA. This approach is not intended to showcase the capabilities of FTA but to demonstrate how it can be integrated into a broader risk assessment process to systematically define failure scenarios and assess required performance levels. The novelty lies in the integration of F-CHIA with FTA, which provides a more targeted, efficient, and function-specific risk analysis compared to traditional methods.

This paper is organized into Section 1, which introduced the research background and discussed requirements for robot and automation safety. The novelty and contribution of the paper were highlighted. A risk-informed design framework for the functional safety system design of HRC applications was proposed. In Section 3, a case study applying the proposed methods and framework was presented for the early-phase design of a semi-automated agriculture tractor. Sections 4 and 5 presented the discussions and conclusions, respectively.

2. Materials and Methods

In this paper, the requirements elicitation techniques, risk-informed regulatory framework, and risk-based approaches, i.e., F-CHIA and FTA, were utilized to establish the risk-informed design framework for the functional safety system design of HRC applications. In the following sub-sections, the concepts and methods are explained in detail.

2.1. Requirements Elicitation Techniques

Design can be viewed as a constraint satisfaction problem. Some of the constraints refer to the functions or goals of the artifact [19,20]. All the requirements have to be recorded in system requirements documents (SRDs) [21]. However, such knowledge used by design teams is not implicitly encoded. Experience and (prior) knowledge play a significant role. The acquisition of knowledge and expertise is through learning so that in the later design stage, the designers can produce a description of an artifact that will exhibit the necessary attributes to carry out the given functions. In this paper, the design problem is considered a class 2 design [22], which is an extension or modification of solutions and new implementations in the application field. One of the features of class 2 design is that the failure of design solutions is not explicitly known.

There are four dimensions to requirements elicitation [22]: application domain understanding, problem understanding, business understanding, and understanding of the needs and constraints of system stakeholders. Application domain knowledge is knowledge of the general area where the system is applied. For example, to understand the requirements for an HRC application, you must have background knowledge about the control algorithm of the robotics systems and the physical characteristics of the robotics systems. The problem understanding is the details of the specific customer problem where the system will be applied must be understood. For example, a robot arm is used to replace the work of picking up the tubes in the pharmaceutical industry. During problem understanding, you specialize

and extend general domain knowledge. Systems are generally intended to contribute in some way to the development of a business or organization. Requirements elicitation techniques commonly used are interviews, use-case analysis, observations, surveys and questionnaires, and brainstorming. In this study, brainstorming is adopted in a structured way through F-CHIA because these mentioned techniques are not able to systematically identify the functional requirements, and there is a missing link between the standards identification in relation to each functional requirement. It is essential because the identified latest relevant standards and regulations can ensure safety compliance throughout the design and development process. It is directly related to the regulatory framework currently implemented for ensuring machinery safety.

2.2. Risk-Informed Regulatory Framework

Developing suitable regulatory frameworks is essential to ensure safety. A promising approach to address this challenge is the risk-informed regulation (RiR) framework, which integrates risk insights with engineering practices and was first clearly stated in the Government Performance and Results Act (GPRA) established by the U.S. Congress in 1993 [23]. RiR framework is fully embraced by the nuclear industry [24]. It is essential to establish safety goals, which address the fundamental policy of acceptable safety levels and the question of "how safe is safe enough". RiR aims to motivate licensees to proactively improve safety and operational performance and minimize potential risks [24]. Compared to prescriptive, deterministic regulation, it pushes technology forward, as it will not be too conservative to be consistent with compliance [25]. In the EEA, regulations are well-adopted. One of the reasons is the market demand. The free movement of goods and labor within the EEA necessitates the establishment of common minimum standards to protect workers and consumers. As a result, the EEA has implemented a series of directives and regulations that primarily focus on occupational health and safety and product safety. Among these, there are product directives known as total harmonization directives, which must be fully implemented by all Member States, ensuring that the same rules apply across Europe. When it comes to the use of robot applications, several key products:

- Machinery Regulation 2023/1230/EU (that replaced Machinery Directive 2006/42/EC)
- Directive 2014/35/EU, also known as the "Low Voltage Directive"
- Directive 2014/30/EU, which addresses "Electromagnetic Compatibility"
- Directive 2017/745/EU, referred to as the "Medical Devices Regulation"

EEA directives and regulations adopt a precautious approach to ensure high-level safety and customer protection, leading to eliminating potential risks in advanced technologies. For example, Machinery Regulation 2023/1230/EU refines the definition of machinery by adding requirements on digital components, software capabilities, and cyber security, which supports machines' autonomous actions. Additionally, other regions and countries in the world have different approaches to regulation, shaped by their regional priorities, such as consumer protection, innovation, or economic development. While the EEA emphasizes uniformity and precaution, other regions, like the U.S., prioritize flexibility and innovation. The identification of directives and regulations should comply with specific regional principles.

To assist manufacturers in demonstrating compliance with the essential health and safety requirements outlined in these directives, corresponding standards have been introduced. If a standard is harmonized with the machinery regulation or other applicable regulations and directives, adherence to that standard implies conformity with the essential health and safety requirements of the respective regulation and directive.

In the current risk-informed regulatory framework, incorporating standards identification into safety evaluation workflows is essential despite the challenges it poses. This

study serves as the foundation for the functional evaluation of automation in this paper, as it provides a consistent context for regulators, industry, and standardization. In addition, standards alone are not enough for collaborative systems to ensure safety [10]. A dedicated risk-based approach is important for those automation systems that are specifically designed for HRC.

2.3. Risk-Based Approaches

Risk-based approaches utilize advanced tools and methods that are developed in the quantitative risk assessment and deterministic safety assessment based on the understanding of the concept of risks to assess risk associated with technologies [26]. As mentioned previously, the risk-informed regulatory framework is a legalization framework that integrates risk insights with engineering practices to ensure meeting safety goals. The risk-based approach is the risk assessment technique that can be utilized to assess safety to meet those safety goals.

It is generally not feasible to establish uniform risk management guidelines that apply across all application areas. Each application area presents its unique set of risks and challenges, making it difficult to devise a one-size-fits-all approach. However, knowledge transfer between different application areas is possible and valuable [27]. This transfer involves sharing insights, experiences, and best practices from one area to another.

These application areas can be broadly categorized as risk management in various industrial applications and risk management specific to robot and automation system application areas. Each of these areas requires tailored risk management strategies that address their specific contexts, hazards, and safety requirements.

To enhance risk-based approaches for less-intelligent systems, such as vehicles and cars, there is a need to establish a widely shared knowledge base. This knowledge base can serve as a foundation for adapting and applying safety methods to emerging fields like service robotics and autonomous robotics, which are expected to exhibit higher levels of intelligence and autonomy in the future.

By leveraging existing risk-based approaches and lessons learned from less-intelligent systems, it is possible to develop and refine risk-based approaches that align with the unique characteristics and challenges of more advanced robotics systems. This knowledge-sharing and adaptation process will help in building a comprehensive and robust framework for ensuring safety in future robotics applications. In this study, the F-CHIA and FTA for hazard identification and standardized performance level assessment for risk assessments are used.

2.4. Proposed Risk-Informed Design Framework for the Functional Safety System Design of HRC Applications

2.4.1. Functional Requirements and Hazard Identification

In the concept design stage, the function-centered design approach is dominant [28]. The functional requirements, including safety functions, are abstract. Correspondingly, function-centered hazard identification is naturally aligning the design intention for eliminating hazards that hinder its function realization. The other traditional hazard identification methods, such as FTA, failure mode and effect analysis (FMEA), and Hazard and Operability Studies (HAZOP), are not suitable for functional hazard identification. The detailed research on this argument can be found in the literature [29]. Based on the risk assessment framework in ISO 12100 and the principles in HAZOP [30,31], F-CHIA is proposed. The features of F-CHIA are: (i) It can be applied at all stages of the life cycle, (ii) It can be applied for complex systems, (iii) It can analyze functional requirements for each foreseeable hazard in terms of functions, (iv) It can provide systematic hazard identification on the functional level, and avoid repetitions of works (v) It integrates the

risk assessment elements in the ISO 12100 standard, which means it follows the recommendations by standards.

The F-CHIA starts by examining and agreeing on the design intent. Next, hazard zones are identified: the areas where users are exposed to any hazards. Because the HRC is not physically available in the early-phase design, the hazard zones are determined based on the design intents. The hazard zones pave the foundation of the initial layout of the HRC.

In each hazard zone, task identification is carried out. These tasks are the actions that people will perform while interacting with the machine or the operations the machine will carry out during its life cycle. Functions are identified in a selected task. Realizations represent how these functions are implemented and supported by certain properties [32]. The properties of the realizations can be static (e.g., shape and size) or dynamic (e.g., pose, velocity, and acceleration) and are crucial for perception [33].

Functional hazards are identified by analyzing potential deviations in function. These deviations are described using guide words such as "no," "part of," and "other than." Functional hazards can occur in three ways: (i) using a wrong function ("other than" + "function"), (ii) using a correct but degraded function ("part of" + "function"), or (iii) complete loss of function ("no" + "function") [34]. The analyzer applies the guide word to each selected function to clarify the hazard.

If all reasonably foreseeable functional hazards are identified, the next step is to investigate their causes, consequences, and properties. The outcome of this investigation is a set of functional requirements and relevant directives or standards. If any functional hazards are missed, feedback loops ensure the process is completed.

The hazard identification is recorded on a blank form (shown in Table 1). The flowchart of the function-centric hazard identification procedure for the early design phase of a collaborative application is depicted in Figure 1. The final outputs, including general functional requirements and functional safety inputs, are shown in Figure 2.

Table 1. Example of a blank form for the function-centric hazard identification.

Function-Centric Hazard Identification								
HRC:					Hazard zone:			
The phase of the life cycle:					Analyst:			
Task	**Function**	**Realization**	**Properties**	**Guide word**	**Deviation**	**Causes**	**Consequences**	**Functional requirement**

2.4.2. Functional Safety

The standardized three-step risk control approach for robotics includes:

- Step 1-Inherently safe design measures: This step focuses on designing robots with built-in safety features and risk-reduction mechanisms from the initial stages. It involves incorporating safety considerations into the design to minimize hazards and risks.
- Step 2-Safeguarding implementation of complementary protective measures: In this step, additional protective measures are implemented alongside the robot to mitigate risks. These measures can include physical barriers, safety sensors, emergency stop buttons, or other safety devices that work in conjunction with the robot.
- Step 3-Information for use: This step involves providing clear and comprehensive instructions, warnings, and guidelines to users about the safe operation and maintenance of the robot. It ensures that users have the necessary information to understand the risks associated with the robot and how to use it safely.

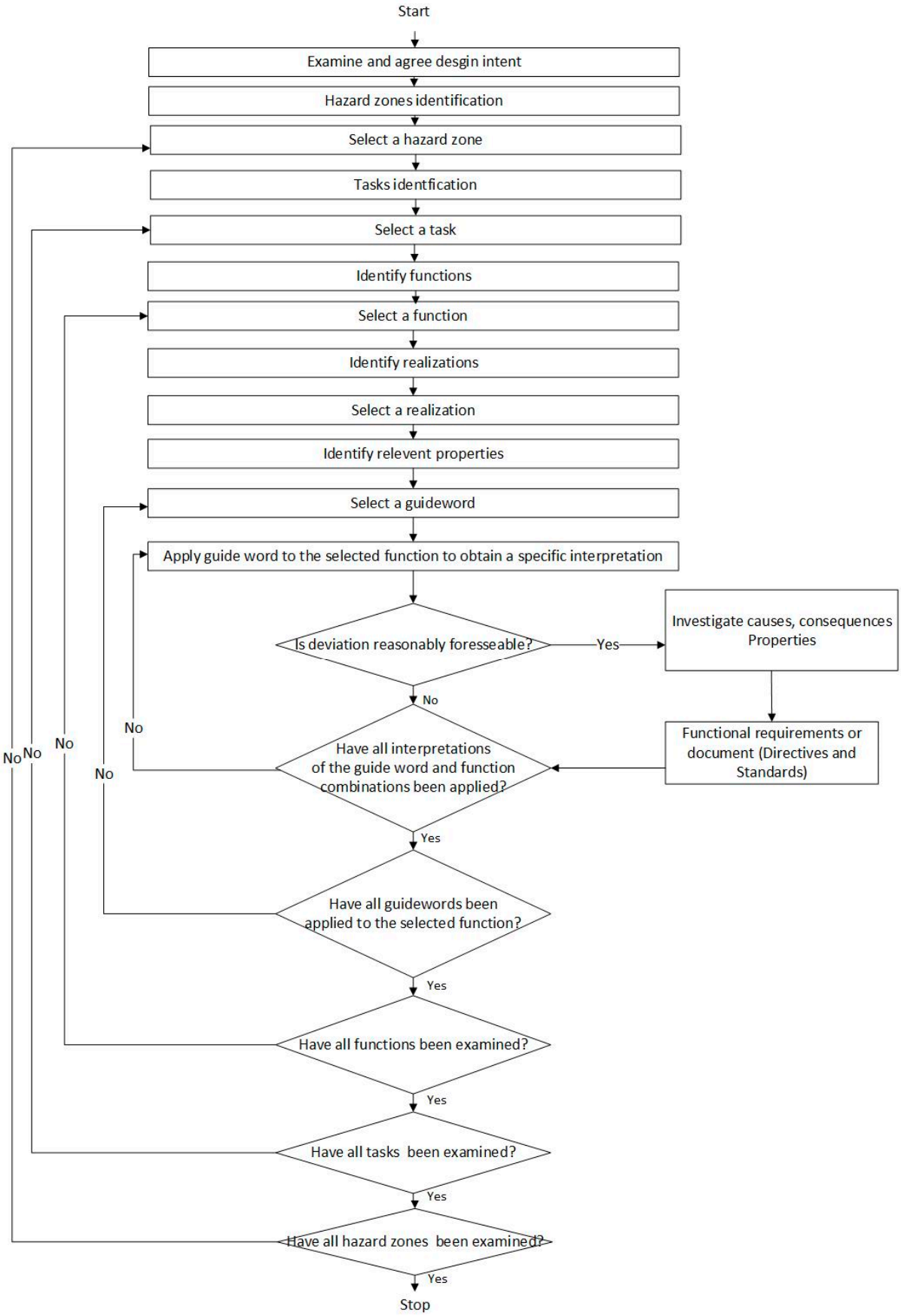

Figure 1. Flow chart of the function-centric hazard identification procedure in the early design phase of the collaborative application.

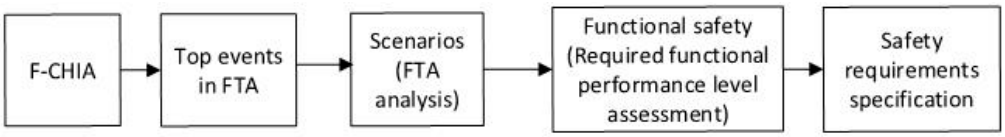

Figure 2. The procedure, from general functional requirements to safety requirements specification adopted in this study.

Functional safety concepts are widely accepted and form an integral part of the three-step risk-reduction measures. Functional safety aims to reduce risks by implementing safety functions and mechanisms within the robot system. Safety requirements (SRS) specification contains the requirements for the safety functions that have to be met by the safety-related control system in terms of characteristics of the safety functions (functional requirements) and required performance levels (PL_r). In the case study, the determination of PL_r follows the method in ISO 25119-2: 2023.

3. Results

As an illustration of the methods suggested in Section 2, the functional safety system design of a semi-automated agriculture tractor is performed in this section. The designed agriculture tractor is made in Denmark and will be traded in the European market. Therefore, the tractor needs to be CE-marked and is required to meet the safety, health, and environmental protection requirements.

3.1. Design Example-Design Intent

The machine is designed as an agricultural tractor, specifically for use in vineyards and similar agricultural fields. It operates in two modes: manual mode, where a human operator controls the tractor using the control panel, and autonomous mode, where the tractor leverages perception systems (such as cameras, LiDAR, and GPS) for navigation, obstacle avoidance, and task execution. The tractor can switch seamlessly between these modes depending on the task or environmental conditions. Operating in relatively flat terrain, the machine encounters obstacles like rows of grapevines, which must be navigated with high precision to avoid damage. The tractor can be equipped with various implements for soil maintenance, pesticide application, pruning, and other tasks, adapting to the farmer's needs. It operates mainly during the daytime but may face challenges in poor weather conditions, such as rain or fog, which can degrade sensor performance and affect navigation. Both manual and autonomous operation modes must account for these factors to ensure safe, efficient, and precise operation across varying environmental conditions. The main body of the machine is constructed by integrating the electrical system, agricultural facility attachment ports, and a mobile base. For our investigation, only the tractor's main body is taken into consideration. The safety analysis process does not encompass the design of agricultural attachments and accessories, such as the sprayer, which falls under the scope of the Machinery Regulation 2023/1230/EU.

3.2. Hazard Zones

Users may be exposed to any hazards in hazard zones. According to the approach procedure, the hazard zones have to be identified. As agricultural machinery with bi-operation modes, the tractor has opportunities to interact with both operators and nearby workers. In the early stages of design, hazard zone identification plays a crucial role in ensuring the safety of both humans and machines. The purpose of hazard zone identification is to identify and assess potential hazards that may arise from the interaction between humans and machines within a given environment. During the hazard identification process, tasks

are specified within each hazard zone to determine potential hazards associated with those tasks.

In the design case involving a combination of conventional tractors and technologically autonomous technologies, hazard zones are defined based on the specific interactions and risks associated with this combination. The presence of autonomous technologies introduces new considerations and potential hazards that may not exist with conventional tractors alone.

As a result, the hazard zones are identified as shown in Figure 3, and the explanations are:

Base zone: The mobile base serves as the module responsible for driving the tractor to its target working position.

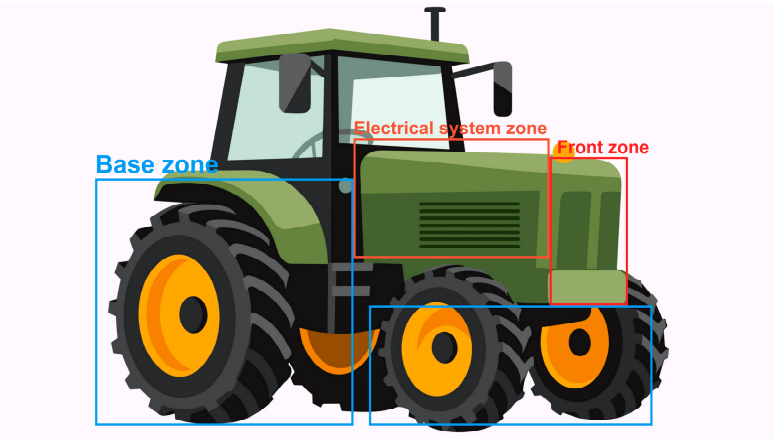

Figure 3. Illustration of the hazard zones on a schematic diagram of an agriculture tractor. The schematic diagram of the tractor is taken from vecteezy.com (accessed on 5 December 2024). Three hazard zones directly connected to the tractor are shown in the figure: Base, Electrical system, and Front zones. The surrounding zone, which is not connected to the tractor's physical components, refers to the space around the tractor and is not shown in the figure.

This area necessitates the consideration of mechanical structures for essential driving tasks, along with the hardware and software implementations required for autonomous navigation. During manual operation mode, a single operator is expected to be seated in the driver's seat, operating the tractor via the control panel or a joystick. In this instance, direct contact exists between the operator and the machine. However, as soon as the tractor enters autonomous mode, it utilizes sensor systems to detect its surroundings, determine its location, and plan its subsequent course of action. Unfortunately, due to potential issues arising from unreliable hardware and software implementation, individuals in close proximity to the tractor are exposed to hazards. These hazards could include risks associated with faulty sensing or processing, potentially resulting in collisions, unpredictable movements, or other unforeseen dangers.

Front zone: The front zone of the machine is designated for the installation of versatile end effectors, such as lifters and other agricultural facilities.

Depending on the specific usage requirements, various attachments may be necessary. However, irrespective of the chosen equipment, the component independent from the mobile base presents a risk when it comes into contact with the human body. Furthermore, in the event of a technical error, it can pose hazards to the surrounding environment. Therefore, careful consideration and appropriate safety measures are vital to mitigate potential risks associated with this front zone.

Electrical system zone: The electrical system zone serves the purpose of electrical power supply and core driving operations, encompassing batteries, circuits, displays, and other electronic components.

In addition to the traditional electrical elements, onboard sensors, and processors are installed to facilitate autonomous mode detection and computation. However, it is important to note that electrical system failure can be triggered by factors such as radiation, electromagnetic interference, and power exchange between equipment. Such failures pose significant risks to drivers and compromise human safety. Therefore, ensuring the reliability and robustness of the electrical system is crucial to prevent potential hazards.

Surrounding zone: The surrounding zone is designated for maintenance personnel and technicians who work in the immediate vicinity of the machine.

Erroneous actions from the machine in this zone can directly place individuals in hazardous situations. As this is an outdoor, high-power machine, noise pollution becomes a concern, potentially exposing those nearby to hearing-related illnesses. Additionally, the intense vibrations generated by the machine can cause discomfort for the operator and have adverse effects on both the environment and the operator's well-being. Therefore, in this hazard zone, non-physical variables such as noise, emissions, and vibrations are of primary consideration to ensure the safety and well-being of individuals in the surrounding area.

It is important to conduct a thorough analysis of each hazard zone to identify potential risks and hazards specific to the combination of conventional tractors and autonomous technologies. In the next section, the hazards associated with tasks in hazard zones are identified and recorded in the function-centric hazard identification tables.

3.3. Hazard Identification

The process of function-centric hazard identification starts with the identification of the tasks in the selected hazard zone, followed by the necessary functions that support each mission. Guide words are selected and applied to each function, generating deviation in hazardous situations. Potential realizations of the function aid the analyst in observing essential system properties and marking them for future risk analysis. The illustrated identification process here concentrates on the machine's design stage, where the tasks and relevant functions generally fulfill the requirements of human-machine interaction and its agricultural characteristics. However, the method can be used in other phases as well, including the implementation phase, to analyze the arrangement between specific components.

Our aim is not to identify every single hazard but rather to provide examples of a few typical tasks within each hazard zone as a means of illustrating the application of the method in real-life situations. To ensure a comprehensive identification of hazards, it is crucial to follow the steps outlined in Figure 1. The principle of the designing of the flowchart structure in Figure 1 is based on the HAZOP standard [35]. The analysis does not take into account failures of individual components since these can be prevented through regular inspections and maintenance. Instead, we will focus on discussing the foreseeable hazards in the use and time limits of the machine. The pesticides or other chemical solutions are not considered.

The hazard identification procedure in the early design phase of the collaborative application proposed in Figure 1 begins with identifying all the tasks that the collaborative application is expected to perform. This step ensures that the full scope of potential hazards across various use cases is considered. Once the tasks are identified, a specific task is selected for detailed evaluation. Following task selection, the design intent for the chosen task is carefully examined and agreed upon among all stakeholders. This ensures clarity and alignment on its intended purpose and functionality. Subsequently, the

specific functions required to execute the selected task are identified. Each function is then analyzed individually to understand the operational characteristics and their associated risks. Critical properties for each function, such as speed, force, or range of motion, are also identified. These properties play a key role in assessing deviations and potential hazards.

To systematically evaluate each function, guidewords are applied. These guidewords act as triggers to explore potential deviations from the intended design. Each application of a guideword generates specific scenarios, which are then assessed to determine whether the deviation is reasonably foreseeable. If a deviation is deemed foreseeable, its causes and consequences are investigated in detail. This step ensures that all relevant risks are thoroughly documented. The process continues by iterating through all interpretations of the guidewords for the selected function, ensuring comprehensive analysis.

Once all guidewords have been applied to the chosen function, the process moves to the next function within the task. This iterative approach ensures that every function is rigorously evaluated. Once all functions associated with the task have been examined, the focus shifts to identifying hazard zones within the collaborative application's operational environment. Each hazard zone is selected and assessed individually to ensure detailed evaluation. As with functions, hazard zones are examined one at a time until all zones have been evaluated. At this stage, the process progresses to identify realizations. This involves proposing practical measures, controls, or design features to address the hazards identified during the analysis. These realizations are crucial for mitigating risks and ensuring the safety of the collaborative application's operation.

The procedure then circles back to the list of tasks, selecting the next task for analysis if there are any remaining. The process repeats until all tasks, functions, and hazard zones have been thoroughly examined. By following this structured framework, hazards can be identified early in the design phase, allowing for the implementation of effective risk mitigation strategies. This not only improves the safety of collaborative robots but also facilitates compliance with relevant safety standards and regulations. This comprehensive and iterative approach ensures that all aspects of collaborative application operation and interaction are systematically evaluated, contributing to a safer and more reliable deployment of these advanced robotic systems.

Table 2 shows the results of function-centric hazard identification in the base zone for the selected typical tasks of the agriculture tractor in the early design phase. The tractor is considered a semi-automated machine that can be operated manually and autonomously. The tasks selected to illustrate the base zone hazard identification process are: Task 1—switch between the autonomous mode and the manual mode; Task 2—autonomous navigate on the field, avoiding humans, machines, and obstacles from the environment such as stones and vines; and Task 3—control the tractor mobile base in the manual mode. The last column in Table 2 is the assigned number for each identified functional hazardous situation. These numbers will be referred to when the relevant directives and hazards are identified to meet their corresponding functional requirements for each functional hazardous situation in Section 3.4.

Table 2. Function-centric hazard identification for the base zone for typical tasks in the design phase.

Function-Centric Hazard Identification									
HRCA: autonomous agricultural tractor					Hazard zone: Base zone				
The phase of the life cycle: design phase					Analyst:				
Task	**Function**	**Realization**	**Properties**	**Guide word**	**Deviation**	**Causes**	**Consequences**	**Functional requirements**	**No.**
1	Switch between the autonomous mode and the manual mode	Manually select the option	Machine status	Other than	Autonomous mode fails to start	Software error	The tractor cannot move. Time loss.	1. Set up at least two distinct accesses (for redundancy and safety, e.g., a mechanical button reachable when the operator is outside the tractor and an access on the control panel) to the mode switch while also minimizing the effect of complexity from multiple systemic accesses. 2. Provide 100% knowable instructions on how to switch the mode (for good decision support in the situation of autonomous mode failing to start to reduce possible human errors) in the user manual, considering the diverse educational level of the intended users. Two necessary formats of instructions can be diagram instructions showing appearances and positions of accesses and language instructions to describe operations in detail. Note that multiple languages and definitions of terminologies are expected to be provided to meet the needs of people from different educational backgrounds.	1.1.1
				Other than	The autonomous mode starts before the operator leaves the tractor.	As above	Extra injury to the operator when the collision happens.	1. As above. 2. Set up an independent emergency stop function that shall stop all hazardous motions and should be clearly marked and easily accessible. It shall only be reset by a deliberate manual action that does not cause a restart after resetting but shall only permit a restart to occur. The following information shall be provided: (a) stop category according to IEC 60204-1:2016 + AMD1: 2021. (b) span-of-control of the emergency stop; (c) maximum response time for the emergency stop, as measured from input state change until the termination of the hazardous function of the tractor. (d) maximum stopping time for the emergency stop, as measured from input state change until the termination of hazard function(s) of the tractor.	1.1.2

Table 2. *Cont.*

			Function-Centric Hazard Identification						
2	Perceive surroundings among dynamic objects, static obstacles, and drivable paths.	Camera detection with image processing algorithms and learning approach	1. Object type 2. Distance	No	The tractor fails to detect its surroundings, especially the road.	1. Blurry image due to the instability of the tractor 2. Weak brightness 3. Severe weather conditions	1. There is no valid input to the localization and navigation module. 2. The tractor fails to start the autonomous mode or moves improperly.	1. Set up specific limitations on maximum driving and turning speeds given different types of risky weather in autonomous mode in the user manual, providing 100% fully clear instructions to manually select operation conditions or set speed limitations (for good decision support to reduce human errors) considering a diverse educational level of the intended users. 2. Set up two image quality assessment modules: a subjective test module where humans can access captured images and provide evaluations and an objective test module where the computational software enables the comparison between references and targets. Use images with rain droplets, snow particles, and dust to simulate extreme conditions. Compare the module's output with known benchmarks for images in similar conditions. The verification and validation methods are a review of the documentation and information for use, practical tests, and simulation tests. Record the test conditions. Quality assessment is expected to start once the autonomous mode starts. The captured images are tested on several factors: brightness, resolution, contrast, noise, and blur. The system should have instant feedback on whether the series of input images is valid for autonomous navigation. If not, disable the autonomous mode. 3. Set up an emergency stop function as explained in 1.1.2. 4. Test the lighting system. The verification and validation methods are visual inspection, observation during operation, review of specifications and information for use, and practical tests.	1.2.1

Table 2. *Cont.*

			Function-Centric Hazard Identification						
				Part of	1. Not all obstacles in the scene are detected. 2. Distance between the tractor and the object is not available.	1. low-quality image 2. unreliable detection algorithm 3. limited detecting range of the camera	The tractor is not aware of changes in surroundings, which may cause collisions.	1. Set limitations on sensing and automation-related zones in the user manual, providing 100% fully clear instructions (for good decision support to reduce human errors) considering the diverse educational level of the intended users. Provide speed monitoring safety functions. 2. Analyze sensor performance classes and test detection capabilities of the sensors and software before implementation in the real-case application. Set specific, measurable criteria to assess the performance of sensors and software. Record the test conditions. 3. Set up an emergency stop function, see 1.1.2.	1.2.2
		Lidar detection	1. Distance 2. Reflective data	Part of	Not all obstacles are detected by Lidar.	1. The resolution of the Lidar is too low. 2. The vertical detecting range is limited.	As above	As above	1.2.3
Task	**Function**	**Realization**	**Properties**	**Guide word**	**Deviation**	**Causes**	**Consequences**	**Functional requirements**	**No.**
		combination of sensors	1. Object type 2. Distance 3. Reflective data	Part of	The detection is not as accurate as expected.	Calibration and data alignment between sensors are not conducted properly.	As above	1. As above 2. Provide 100% knowable instructions on how to perform the calibration of onboard sensors, e.g., camera, depth camera, and LiDAR in this case study (for good decision support to reduce possible human errors) in the user manual, considering the diverse educational levels of the intended users.	1.2.4
	Planning collision-free trajectory based on perception result.	The route is generated according to certain rules or traditional collision avoidance algorithms such as potential field methods	1. Knowledge of the environment (perception results) 2. Trajectory generation algorithm(s)	No/Part of	No trajectory is generated, or the provided trajectory cannot meet the collision-free requirement.	An improper route planning algorithm is used.	1. The tractor cannot avoid obstacles duly. 2. The tractor cannot drive on the expected path, i.e., The middle of the field trial.	1. Test the trajectory planning algorithm before implementation on the machine. Set specific, measurable criteria to assess the performance of the trajectory planning algorithm in both simulation and real implementation. Record the test conditions. 2. Calibrate the path at first use. Provide 100% knowable instructions on how to perform the calibration (for good decision support to reduce possible human errors) in the user manual, considering the diverse educational levels of the intended users.	1.2.5

Table 2. *Cont.*

Function-Centric Hazard Identification								
	Control the tractor driving on the expected trajectory.	The motor is controlled through specific control theories	1. Trajectory 2. The difference between the expected route and the driving on route 3. Constraints 4. Machine states	Part of	The control result is not as expected.	1. The parameter from the control system is not set properly. 2. The electrical module and the mechanical module are not well-compatible.	1. Component damage because the tractor cannot drive smoothly. 2. The tractor cannot follow the expected path. 3. Collision due to the tractor cannot react to the environment on time.	1. Provide suggested control parameters according to the ground condition. Test the control system before implementation. Record the test conditions. 2. Set up an emergency stop function, see 1.1.2.	1.2.6
3	The operator gives direct command to the tractor.	The operator sits in the driver's seat and controls the tractor through the control panel	Machine states	Part of	The human operator can control the tractor but fails to do it safely.	1. Operator's clothing, hair, or body parts get caught or entangled in mechanical parts and cause injury or entrapment. 2. Operator's inadequate awareness and understanding of the control system. 3. Human is injured due to bad ergonomics.	1. Collision, turnover, and other accidents due to human failure. 2. Human injury due to long-term work.	1. Set limits on operators. 2. Design the seat and the panel to follow the relevant standards to fully fulfill the requirements of human factor engineering. 3. Provide 100% knowable instructions on control systems (for good decision support to reduce possible human errors) in the user manual, considering the diverse educational levels of the intended users. 4. Provide protective measures in the cab.	1.3.1
	The control system conducts command from the operator.	The coordination between the electrical system with the engine and actuator	Machine states	Part of	The control system cannot react to the command on time.	Malfunctions in the electrical control system and the mechanical control system.	Collision, turnover, and other accidents due to malfunctions.	Test the control system in the manual mode before implementation. Record the test.	1.3.2

We use Task 2, autonomous navigation in the field, as an example to illustrate the process of hazard and functional requirement identification. To achieve autonomous navigation, three key functions must be realized: surroundings perception, path planning, and motor control. Each of these functions can be implemented through different realizations. For instance, in the perception function, realizations may include vision-based methods, LiDAR-based methods, or a combination of multiple sensor modalities. The properties of these realizations vary significantly; for example, vision-based perception is typically suited for detecting object types and short-range distances, while LiDAR-based perception is good at capturing point cloud reflections for detailed spatial awareness.

Based on the specific realization and its associated properties, guidewords are systematically applied to identify potential hazards, their causes, and their consequences. For example, in the case of vision-based perception, a failure scenario might arise under severe weather conditions, such as heavy rain or fog, leading to a complete loss of visual input. To address such hazards, functional requirements are generated to mitigate the associated risks. For this particular hazard, implementing an image quality assessment function can help monitor the reliability of the visual input, while a speed control function can adjust the vehicle's navigation speed to maintain safety under compromised conditions (Function 1.2.1). This example highlights the critical role of tailoring functional requirements to the specific realizations and properties of each task component, ensuring safety in the early design phase. The other results of function-centric hazard identification in the other hazard zones for the selected typical tasks are summarized in Appendix A.

3.4. Functional Requirements

The functional requirements in each functional hazardous situation are derived from the proposed causes and consequences. To illustrate this, let's consider the hazardous situations presented in Table 2. When the tractor operates autonomously, it is expected to detect its surroundings and gather valuable data. However, factors such as blurry image input, lousy weather, and poor lighting may cause the camera, the sole sensor, to fail in environment detection. This failure could have severe consequences, including irregular driving without necessary perception results. To address this issue, restrictions on maximal speeds and weather conditions should be implemented. Additionally, functions to assess the quality of the image series need to be established before activating the autonomous mode. An emergency stop function is also necessary to prevent accidents, such as collisions and turnovers.

When the tractor is operated manually, additional protective measures must be implemented to safeguard the operator from long-term harm, such as noise-induced sickness. Furthermore, detailed instructions on operating the control interface should be provided to minimize the likelihood of human error.

In summary, the functional requirements can be categorized into three main classes: inherent safer design, protective measures, and information for use. This classification aligns with the general requirements outlined in the ISO 12100 standard. It is worth highlighting that some key findings arise from these three classes of functional requirements.

3.4.1. Inherent Safer Design

Depending on the specifications, additional system functions are required for risk inspection and elimination. To ensure system reliability, tests should be conducted on algorithms, component performance, and mechanical systems. These tests are crucial in verifying the robustness of the system.

Moreover, limits need to be defined regarding the use of the system, as well as aspects such as space and time. Our findings indicate that it is important to limit the value of operation variables, personnel experience, and working space. By setting appropriate limits, potential risks associated with these factors can be mitigated.

In addition, relevant maintenance requirements should be specified to ensure the system's continued performance and reliability. Furthermore, the prevention of single-component failures can be addressed through the implementation of time limits, which establish intervals for maintenance and inspections.

3.4.2. Protective Measures

Physical protective measures should be provided to nearby humans to prevent the inevitable hazards from noise and emission. These protective measures play a critical role in creating a safe environment for both operators and individuals close to the system.

3.4.3. Information for Use

To mitigate hazards resulting from unintentional human faults, it is crucial to provide detailed instructions on the operation of the system, the proper use of components, and the appropriate selection of attachments. These instructions serve as important guidance for operators and users, helping them understand how to interact with the system safely and correctly.

3.5. Standards Identification

Directives, regulations, and standards serve as important references when implementing risk-reduction strategies. In our approach, we select directives and standards based on the functional requirements associated with each functional hazardous situation. This selection process is facilitated by the structured nature of our function-centric hazard identification approach, which guides analysts in searching for relevant documentation.

During the early design phase, our approach establishes a general connection between standards and functional requirements. However, as the design process progresses to later stages, such as detailed design and implementation, it becomes possible to identify the specific items within each standard that directly contribute to the implementation of safety functions. This ensures a more targeted and precise application of standards.

To illustrate the practical application of our approach, Table 3 provides the selected standards for the functional hazardous situations presented in Table 2. Furthermore, in Appendix B, we present a comprehensive list of all standards applicable to the identified hazards in the selected tasks and hazard zones.

Table 3. Identified directives, regulations, and standards for the functional hazardous situations associated with functional requirements, which are presented in Table 2.

Related Functional Requirements	Legislation Reference	Reference Number	Standard Title
All	Machinery Regulation 2023/1230/EU	ISO 12100:2011 [12]	Safety of machinery—General principles for design—Risk assessment and risk reduction
1.1.1, 1.1.2	Machinery Regulation 2023/1230/EU	EN ISO 14118: 2018 [36]	Safety of machinery—Prevention of unexpected start-up

Table 3. *Cont.*

Related Functional Requirements	Legislation Reference	Reference Number	Standard Title
1.1.2	Machinery Regulation 2023/1230/EU	EN ISO 13850:2015 [37]	Safety of machinery—Emergency stop function
1.2.1	Machinery Regulation 2023/1230/EU	EN 1837:2020 [38]	Safety of machinery—Integral lighting of machines
1.2.6, 1.3.2	Machinery Regulation 2023/1230/EU	EN ISO 13849-1:2023 [39] EN ISO 13849-2:2012 [40]	Safety of machinery—Safety-related parts of control system
1.2.6, 1.3.2	Machinery Regulation 2023/1230/EU	EN ISO 25119-1: 2023 [41] EN ISO 25119-1: 2023/A1: 2023 [42] EN ISO 25119-2: 2023 [43] EN ISO 25119-3: 2023 [44] EN ISO 25119-3: 2023/A1: 2023 [45] EN ISO 25119-4: 2023 [46] EN ISO 25119-4: 2023/A1: 2023 [47]	Tractors and machinery for agriculture and forestry—Safety-related parts of control systems
1.1.1, 1.1.2, 1.2.1, 1.2.2, 1.2.3, 1.2.4, 1.2.5, 1.2.6	Machinery Regulation 2023/1230/EU	EN ISO 18497:2018 [48]	Agricultural machinery and tractors–Safety of highly automated agricultural machines—Principles for design
1.2.3, 1.2.4	The low voltage directive (LVD) 2014/35/EU	EN ISO 11252:2013 [49]	Lasers and laser-related equipment—Laser device—Minimum requirements for documentation
1.2.3, 1.2.4	The low voltage directive (LVD) 2014/35/EU	DS/EN 60825-1:2014 [50]	Safety of laser products
1.1.1, 1.1.2	The low voltage directive (LVD) 2014/35/EU	EN IEC 60947-1: 2021 [51]	Low-voltage switchgear and control gear
1.1.1, 1.1.2, 1.2.1, 1.2.2, 1.2.3, 1.2.4, 1.2.5, 1.2.6	The low voltage directive (LVD) 2014/35/EU	EN IEC 62368-1:2024 [52] IEC TR 62368-2: 2019 [53] EN IEC 62368:3-2020 [54]	Audio/video, information and communication technology equipment

By incorporating relevant directives, regulations, and standards, our approach ensures that the necessary safety measures are implemented throughout the system's development. This systematic approach enhances safety outcomes and promotes compliance with established industry standards.

3.6. Functional Safety Based on the FTA Method

According to the function-centric hazard identification for the base zone for typical tasks in the design phase in Table 2. The navigation system is one of the designed safety-related systems in the case study. The navigation system perceives surroundings and plans paths. In the case study, the detection system is designed by a combination of lidar detection and vision-based detection. The system fault is that the navigation system fails.

The assumption is that the tractor is set in autonomous mode. The possible injured person could be a bystander. The assumption for the scenarios assessment is that the bystander is the farmer who works in the field. FTA is used to analyze the failure scenarios. The FTA analysis is shown in Figure 4.

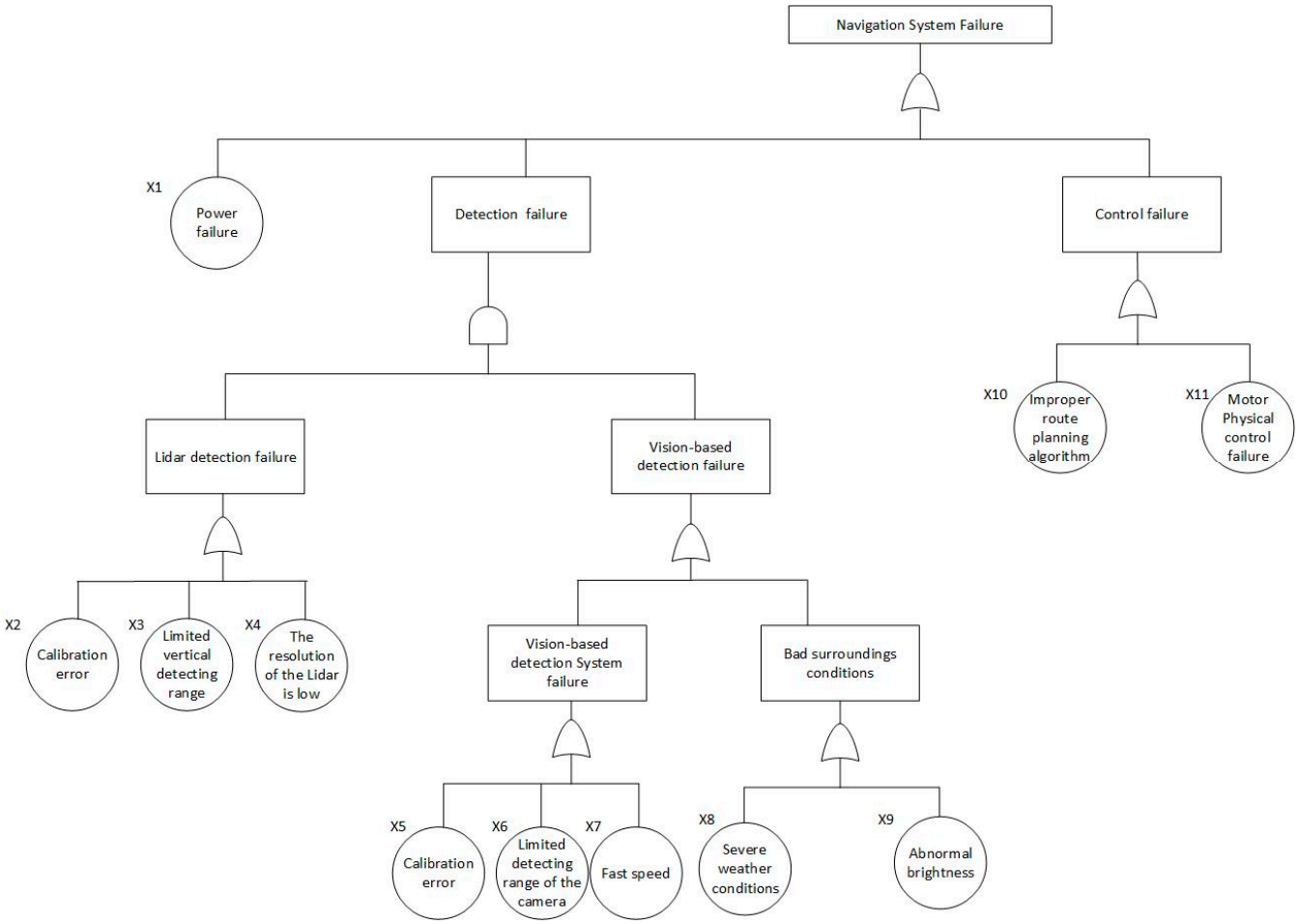

Figure 4. The fault tree of the navigation system failure.

The failure scenarios are represented by the minimal cut sets of the fault tree. A minimal cut set in fault tree analysis represents a combination of basic events (failures) that lead to the top event (system failure). The minimal cut sets are {X1}, {X10}, {X11}, {X2X5}, {X2X6}, {X2X7}, {X2X8}, {X2X9}, {X3X5}, {X3X6}, {X3X7}, {X3X8}, {X3X9}, {X4X5}, {X4X6}, {X4X7}, {X4X8}, {X4X9}. The determination of PLr for the identified scenarios by FTA is shown in Table 4. The determination of PLr is based on the combination of severity (S), exposure (E), and controllability (C) values for each identified hazardous situation according to ISO 25119-2:2023. The resulting PLr=c (the highest identified value). The result indicates that the required performance level for the navigation system is c. In the detailed design stage, the performance level (PL) of the navigation system must be equal to or higher than the PLr. The countermeasures for improving the PL of the navigation system should focus on the factors that reduce the number of minimal cut sets analyzed in the FTA or eliminate the basic event in a minimal cut set.

Table 4. Determination of PLr for the identified scenarios by FTA.

Scenario	Classification of Injuries (S)	Classification of Exposure to the Hazardous Situation (E)	Classification of Avoidance of Harm (C)	PL_r
X1	S0	N.A.	C2	QM
X10	S2	E2	C3	b
X11	S0	N.A.	C2	QM
X2, X5	S2	E2	C3	b
X2, X6	S2	E2	C3	b
X2, X7	S3	E2	C3	c
X2, X8	S2	E2	C3	b
X2, X9	S2	E2	C3	b
X3, X5	S2	E2	C3	b
X3, X6	S2	E2	C3	b
X3, X7	S3	E2	C3	c
X3, X8	S2	E2	C3	b
X3, X9	S2	E2	C3	b
X4, X5	S2	E2	C3	b
X4, X6	S2	E2	C3	b
X4, X7	S3	E2	C3	c
X4, X8	S2	E2	C3	b
X4, X9	S2	E2	C3	b

The same method can be applied to other safety-related functions identified in the functional requirements.

4. Discussion

The proposed F-CHIA approach offers several advantages and usefulness in the lifecycle of human–robot collaborative applications. Firstly, it provides a structured approach to function-centric hazard identification, specifically tailored for the early-phase design. This approach offers a systematic framework for identifying functional hazards, their causes, consequences, and properties, ensuring a comprehensive analysis. Additionally, the approach integrates with the recommendations of ISO 12100, ensuring compliance with safety standards. By utilizing F-CHIA in the early design phase, functional requirements and associated documents, including identified directives and standards, can be identified for all foreseeable functional hazardous situations. This enables the development of safety-critical features and risk-reduction strategies right from the outset of the design process. Moreover, by establishing a broad relationship between standards and functional requirements in the early design phase, F-CHIA sets the groundwork for later stages to identify specific elements within each standard that directly contribute to the implementation of safety functions. Furthermore, F-CHIA helps to avoid redundant work by systematically identifying hazards at the functional level. Focusing on functional deviations allows for a more targeted analysis of potential hazards, thereby reducing the chances of overlooking critical safety aspects.

The CE marking procedure for collaborative robots presents unique challenges due to their dynamic interactive nature and the need to integrate standards and regulations with advanced technologies. The introduction of F-CHIA enables functional design and risk assessment in the early phases of product development. By identifying key functions at the outset, F-CHIA provides a foundational knowledge base that facilitates the search for relevant standards and regulations governing the implementation of these functions. This framework considers the specific use-case scenarios during the design phase, allowing for a tailored approach to analyzing the dynamic interactions inherent to cobot operation. It establishes a logical pathway for aligning new technologies with appropriate regulatory requirements, ensuring compliance with CE marking procedures. F-CHIA offers a structured solution to overcoming the complexities associated with certifying collaborative robots under CE marking. FTA facilitates the process of risk assessment. It examines the possible causal paths for the designed safety-related systems failures as well as enables the design team to focus on factors that improve functional safety performance levels.

From the HSE management point of view, the proposed framework promotes collaboration between designers, engineers, and safety experts. By involving different stakeholders in the examination of design intent, identification of hazard zones, and analysis of tasks and functions, the framework facilitates a shared understanding of safety requirements and fosters effective communication.

In addition, the paper illustrates the application of the framework using the example of a semi-automated agricultural tractor, which aligns closely with the principles of Industry 5.0. Industry 5.0 emphasizes collaboration between humans and advanced technologies, underscoring a human-centric approach for a safer, more sustainable, and resilient world. The tractor demonstrates this by enabling human operators to interact seamlessly with automation, reducing physical strain and enhancing decision-making through supportive functions. With its perception and monitoring systems, the tractor can operate effectively in varying environments. Furthermore, the safety-related functions assessment in the paper enhances its productivity and reliability, aligning with Industry 5.0's emphasis on resilience and sustainability. Importantly, the semi-automated tractor augments human capabilities rather than replacing operators, reinforcing Industry 5.0's goal of empowering workers while integrating advanced technologies into human-centric solutions.

While the methodology proposed in this work addresses systematic function identification in autonomous system functional safety analysis, a limitation arises regarding the quantification process for functional requirements. In standard safety analysis procedures, quantification is typically performed following a comprehensive risk assessment, during which specific implementations are selected, and the corresponding functional requirements are quantified based on standards and the prerequisites of software algorithms. It is, therefore, important to emphasize that the focus of this research is on decomposing the robot's tasks into functions, linking potential functional requirements to relevant standards, and providing a reference framework to support subsequent risk assessment steps. Quantification should be regarded as a subsequent step conducted after the risk assessment of specific scenarios.

5. Conclusions

This paper introduces a novel risk-informed design framework for functional safety, integrating F-CHIA and risk assessment via FTA. As demonstrated in the design of a semi-automated agricultural vehicle, the framework begins with hazard identification by using F-CHIA. It examines design intents, identifies hazard zones, and conducts task and function identification. Foreseeable functional hazardous situations are analyzed, leading to functional requirements and the identification of relevant directives, regulations, and standards. Its key features include applicability throughout the system's life cycle, suitability for complex systems, analysis of functional requirements in relation to each potential hazard, systematic hazard identification at the functional level, avoidance of redundant work, and integration with the recommendations of ISO 12100. The F-CHIA outputs inform the functional safety analysis, assessing the required performance level and deriving specific requirements for software, hardware, and human operators using FTA. The functional requirements derived from F-CHIA are more systematic than traditional methods and serve as effective inputs for functional safety analysis in human–robot collaboration applications. The proposed framework enables design teams to focus on enhancing factors that improve functional safety performance levels, resulting in a more thorough and effective safety design process.

Author Contributions: Conceptualization, J.W.; methodology, J.W. and J.R.; validation, J.R.; formal analysis, J.W. and J.R.; writing—original draft preparation, J.W. and J.R.; writing—review and editing, O.R. and L.N.; Supervision, O.R. and L.N. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A

Table A1. Function-centric hazard identification for the front zone for typical tasks in the design phase.

Function-Centric Hazard Identification									
HRCA: autonomous agricultural tractor					Hazard zone: Front zone				
The phase of the life cycle: design phase					Analyst:				
Task 1: In the autonomous mode, lift the pruner to the same level of detected leaves and cut. Task 2: Manually disassemble and install attachments.									
Task	Function	Realization	Properties	Guide word	Deviation	Causes	Consequences	Functional requirements	No.
1	Detect and locate the specific leaves that need to be pruned.	Determine the target object and define the effector target pose according to the perception result. Normally, vision-based algorithms are used to detect the leave type.	1. Surrounding scene 2. Distance between the tractor and the target	Other than	Instead of the actual target, the tractor recognizes the wrong object, such as wrong leaves, branches, and even stand-by humans.	The implemented target detection algorithms are not precise enough.	Wrong target object positions input to the next function.	1. Set up use limits on bystanders when the tractor is in autonomous mode. 2. Redundant object detection algorithms are required to compensate for the failure in the primary algorithm. 3. Test and validate the software before implementation. Record the test conditions and review the software documentation.	2.1.1
				Part of	The system can detect partial targets and determine the target pose within a certain error range.	As above	Rough position information input to the next function.	1. As above, test and validate software before implementation. Record the test conditions and review the software documentation. 2. Enable dynamic setting to switch the detection between high sensitivity (low false negative detection rate) and high robustness (high false negative detection rate but power saving).	2.1.2

Table A1. *Cont.*

Function-Centric Hazard Identification									
	The tractor stops in front of the target and lifts the effector close to the target.	The effector is moved toward the target detected in the previous function.	1. Tractor pose 2. Effector target pose 3. Effector current pose	Other than	Instead of the actual target, the tractor effector goes toward the wrong object, such as a human.	1. Wrong input from the previous function. 2. Faults in the effector control system.	1. Bystanders get injured due to crushing by the effector or other components. 2. Other surrounding objects are damaged by the effector.	1. Regularly test, validate, and calibrate the effector control system according to standards. 2. Set space limit on bystanders when the effector is working. 3. Set an independent emergency stop function to reduce the risk of standby human injury. Different from 1.1.2, this is an additional emergency stop function that can be installed on a remote control panel to reduce the risk to the surroundings in an emergency.	2.1.3
				Part of	1. The effector is able to get close to the target but with some errors.	1. Inaccurate input from the previous function. 2. Errors from the effector control system.	Damage to the objects around the target leads to cost loss.	Regularly test, validate, and calibrate the effector control system according to standards.	2.1.4
	Execute actions on the target.	The pruner is controlled to cut leaves. The action stops when the target is clear.	1. Surrounding scene 2. Effector target pose 3. Effector current pose	Part of	Pruned objects accidentally fall from the effectors.	Faults from the effector control system.	Human injury due to falling down parts.	1. As above 2. Set limits on the maximum lifting weight.	2.1.5
2	Technician staff disassemble the agricultural	Technicians and maintenance personnel help with changing the agricultural implements for particular tasks.	Usage, installation, and disassembly information about the attachments.	Other than	The wrong implement is installed or disassembled.	Inadequate knowledge of the type of attachments	The mistaken use of the components could lead to hazards such as unbalanced load and structural failure.	1. Provide a full list of attachments compatible with the equipment in the front zone with the manual. 2. Provide regular training to technicians and maintenance personnel.	2.2.1

Table A1. *Cont.*

Function-Centric Hazard Identification						
	Part of	The disassembly or installation process is improper.	Personnel lack experience.	1. Human's fingers, hands, or other body is caught by the pinch points between moving parts such as hydraulic cylinders, linkages, and joints. 2. Severe injury would be caused when the human is caught by the tractor's power take-off (PTO) system.	1. Provide detailed, 100% knowable implements installation instructions with the manual. 2. Provide regular training to technicians and maintenance personnel. 3. Provide full protective measures for the maintenance personnel.	2.2.2

Table A2. Function-centric hazard identification for the electrical system zone for typical tasks in the design phase.

Function-Centric Hazard Identification									
HRCA: autonomous agricultural tractor					Hazard zone: Electrical system zone				
The phase of the life cycle: design phase					Analyst:				
Task 1: Enable multiple sensors for perception and localization in the autonomous mode. Task 2: Enable USB sockets for attaching electrical devices.									
Task	**Function**	**Realization**	**Properties**	**Guide word**	**Deviation**	**Causes**	**Consequences**	**Functional requirements**	**No.**
1	Sensors work simultaneously in the autonomous mode.	Sensors are selected based on system requirements and their features. They are connected to the processor, powered by the electrical system.	Sensor specifications	No	Sensors cannot cooperate collaboratively	1. Poor computational capability of the processor. 2. Interference between sensors. 3. Sensors are not powered properly.	Poor sensor output could lead to failure in the perception system, which will then cause inaccurate or wrong target detection.	1. Select sensors following instructions of standards. 2. Design mechanical structures to eliminate interference between sensors. 2. Test the electrical power exchange between components.	3.1.1
2	USB sockets support electrical devices communicating with the tractor.	USB sockets are powered by the electrical system.	Electricity power	No	USB sockets cannot enable the connection.	Electrical system faults due to malfunctions such as short circuits, exposed wires, or improper grounding.	Electrical shocks or electrical fires could cause the operator injury or tractor damage.	1. Test the electrical power exchange between components. 2. Provide proper electrical insulation, grounding, and regular inspection of electrical components.	3.1.2

Table A3. Function-centric hazard identification for the surrounding zone for typical tasks in the design phase.

Function-Centric Hazard Identification									
HRCA: autonomous agricultural tractor					Hazard zone: Surrounding zone				
The phase of the life cycle: design phase					Analyst:				
Task 1: The tractor is working together on the field in autonomous mode, with other personnel around. Task 2: The tractor is working together on the field in manual mode, with other personnel around.									
Task	**Function**	**Realization**	**Properties**	**Guide word**	**Deviation**	**Causes**	**Consequences**	**Functional requirements**	**No.**
1	The tractor is working in autonomous mode while human workers work around it.	The tractor is working in autonomous mode. Assume there is no physical contact between the human and the tractor.	Distance between humans and the tractor.	Part of	Some non-physical hazards could happen to humans when working around the tractor.	1. low-quality emissions 2. vibrations 3. noise	1. Facilities/mechanical damage due to the large vibrations during tractor working. 2. Human health such as hearing problems and pulmonary diseases are caused by long-term working in noisy and dirty environments.	1. A test on the machine's emission, vibration, and noise level regarding the distance should be conducted under instructions. 2. Provide full protective measures to nearby workers to reduce the risk of emission, vibration, and noise.	4.1
2	The tractor is working on a specific task in manual mode while allowing other personnel to work around it.	The tractor is controlled by the operator.	/	Part of	Emission, vibration, and noise hazards are directly introduced to the operator.	As above	1. Severe hazards, as mentioned above, would happen to the operator. 2. Discomfort of the operator during working due to mechanical vibration.	1. As above 2. Tests on emission, vibration, and noise levels should be conducted in the control cab. 3. Provide protective measures to the operator to reduce the risk of emission, vibration, and noise.	4.2

Appendix B

Table A4. Identified directives, regulations, and standards for all of the functional hazardous situations associated with functional requirements for the selected tasks in hazard zones.

Related Functional Requirements	Legislation Reference	Reference Number	Standard Title
All	Machinery Regulation 2023/1230/EU	ISO 12100:2011 [12]	Safety of machinery—General principles for design—Risk assessment and risk reduction
1.3.1	Machinery Regulation 2023/1230/EU	EN 614-1:2006 + A1:2009 [55] EN 614-2 +A1:2008 [56]	Safety of machinery—Ergonomic design principles
1.3.1	Machinery Regulation 2023/1230/EU	EN 894-1:1997 + A1:2008 [57] EN 894-2:1997+ A1:2008 [58] EN 894-3:2000 + A1:2008 [59] EN 894-4:2010 [60]	Safety of machinery—Ergonomics requirements for the design of displays and control actuators
4.1, 4.2	Machinery Regulation 2023/1230/EU	EN ISO 14123-1:2015 [61] ISO 14123-2:2015 [62]	Safety of machinery—Reduction of risks to health resulting from hazardous substances emitted by machinery
1.1.1, 1.1.2	Machinery Regulation 2023/1230/EU	EN ISO 14118: 2018 [36]	Safety of machinery—Prevention of unexpected start-up
1.1.2,1.2.1, 1.2.2, 1.2.3, 1.2.6	Machinery Regulation 2023/1230/EU	EN ISO 13850:2015 [37]	Safety of machinery—Emergency stop function
2.1.3, 2.1.4, 2.1.5	Machinery Regulation 2023/1230/EU	EN ISO 4413:2010 [63]	Hydraulic fluid power—General rules and safety requirements for systems and their components
1.2.1	Machinery Regulation 2023/1230/EU	EN 1837:2020 [38]	Safety of machinery—Integral lighting of machines
1.2.6, 1.3.2, 2.1.3, 2.1.4	Machinery Regulation 2023/1230/EU	EN ISO 13849-1:2023 [39] EN ISO 13849-2:2014 [40]	Safety of machinery—Safety-related parts of control system
4.1, 4.2	Machinery Regulation 2023/1230/EU	EN 13490 + A1:2008 [64]	Mechanical vibration—Industrial trucks—Laboratory evaluation and specification of operator seat vibration
1.2.6, 1.3.2, 2.1.3, 2.1.4	Machinery Regulation 2023/1230/EU	EN ISO 25119-1: 2023 [41] EN ISO 25119-1: 2023/A1: 2023 [42] EN ISO 25119-2: 2023 [43] EN ISO 25119-3: 2023 [44] EN ISO 25119-3: 2023/A1: 2023 [45] EN ISO 25119-4: 2023 [46] EN ISO 25119-4: 2023/A1: 2023 [47]	Tractors and machinery for agriculture and forestry—Safety-related parts of control systems

Table A4. *Cont.*

Related Functional Requirements	Legislation Reference	Reference Number	Standard Title
1.1.1, 1.1.2, 1.2.1, 1.2.2, 1.2.3, 1.2.4, 1.2.5, 1.2.6, 2.1.1, 2.1.2, 2.1.3, 2.1.4	Machinery Regulation 2023/1230/EU	EN ISO 18497:2018 [48]	Agricultural machinery and tractors–Safety of highly automated agricultural machines—Principles for design
2.1.5, 2.2.1, 2.2.2	Machinery Regulation 2023/1230/EU	EN ISO 16231-1:2013 [65] EN ISO 16231-2:2015 [66]	Self-propelled agricultural machinery—Assessment of stability
2.2.1, 2.2.2	Machinery Regulation 2023/1230/EU	EN ISO 16230-1:2015 [67]	Agricultural machinery and tractors—Safety of higher voltage electrical and electronic components and systems—Part 1: General requirements
2.2.2	Machinery Regulation 2023/1230/EU	EN 12965:2019 [68]	Tractors and machinery for agriculture and forestry—Power take-off (PTO) drive shafts and their guards—Safety
1.2.3, 1.2.4	The Low Voltage Directive (LVD) 2014/35/EU	EN ISO 11252:2013 [49]	Lasers and laser-related equipment—Laser device—Minimum requirements for documentation
1.2.3, 1.2.4	The Low Voltage Directive (LVD) 2014/35/EU	DS/EN 60825:2014 [50]	Safety of laser products
3.1.1, 3.1.2	The Low Voltage Directive (LVD) 2014/35/EU	EN 61010-1:2010 [69]	Safety requirements for electrical equipment for measurement, control, and laboratory use
1.1.1, 1.1.2	The Low Voltage Directive (LVD) 2014/35/EU	EN IEC 60947-1:2021 [51]	Low-voltage switchgear and control gear
1.1.1, 1.1.2, 1.2.1, 1.2.2, 1.2.3, 1.2.4, 1.2.5, 1.2.6, 2.1.1, 2.1.2, 2.1.3, 2.1.4, 3.1.1	The Low Voltage Directive (LVD) 2014/35/EU	EN IEC 62368-1:2024 [52] IEC TR 62368-2: 2019 [53] EN IEC 62368:3-2020 [54]	Audio/video, information and communication technology equipment
3.1.1	The Electromagnetic Compatibility (EMC) Directive 2014/30/EU	EN ISO 14982:2009 [70]	Agricultural and forestry machinery—Electromagnetic compatibility—Test methods and acceptance criteria

Table A4. *Cont.*

Related Functional Requirements	Legislation Reference	Reference Number	Standard Title
3.1.2	The Low Voltage Directive (LVD) 2014/35/EU	EN IEC 61204-7:2018 [71]	Low-voltage switch mode power supplies—Part 7: Safety requirements
2.1.3	The Radio Equipment Directive 2014/53/EU	ETSI EN 303 413 V1.2.1:2021 [72]	Satellite Earth Stations and Systems (SES); Global Navigation Satellite System (GNSS) receivers; Radio equipment operating in the 1164 MHz to 1300 MHz and 1559 MHz to 1610 MHz frequency bands

References

1. Franklin, C.S.; Dominguez, E.G.; Fryman, J.D.; Lewandowski, M.L. Collaborative Robotics: New Era of Human–Robot Cooperation in the Workplace. *J. Safety Res.* **2020**, *74*, 153–160. [CrossRef] [PubMed]
2. Adriaensen, A.; Costantino, F.; Di Gravio, G.; Patriarca, R. Teaming with Industrial Cobots: A Socio-Technical Perspective on Safety Analysis. *Hum. Factors Ergon. Manuf.* **2022**, *32*, 173–198. [CrossRef]
3. Lincoln, J.M.; Elliott, K.C. Emerging Technology in Agriculture: Opportunities and Considerations for Occupational Safety and Health Researchers. *J. Saf. Res.* **2023**, *86*, 92–95. [CrossRef]
4. Mcalinden, J.J. Using robotics as an occupational-health and safety control strategy. *Ind. Robot* **1995**, *22*, 14–17. [CrossRef]
5. Aven, T. Foundational Issues in Risk Assessment and Risk Management. *Risk Anal.* **2012**, *32*, 1647–1656. [CrossRef] [PubMed]
6. Dhillon, B.S.; Fashandi, A.R.M.; Liu, K.L. Robot Systems Reliability and Safety: A Review. *J. Qual. Maint. Eng.* **2002**, *8*, 170–212. [CrossRef]
7. Huck, T.P.; Münch, N.; Hornung, L.; Ledermann, C.; Wurll, C. Risk Assessment Tools for Industrial Human-Robot Collaboration: Novel Approaches and Practical Needs. *Saf. Sci.* **2021**, *141*, 105288. [CrossRef]
8. Giallanza, A.; La Scalia, G.; Micale, R.; La Fata, C.M. Occupational Health and Safety Issues in Human-Robot Collaboration: State of the Art and Open Challenges. *Saf. Sci.* **2024**, *169*, 106313. [CrossRef]
9. Berx, N.; Decré, W.; Morag, I.; Chemweno, P.; Pintelon, L. Identification and Classification of Risk Factors for Human-Robot Collaboration from a System-Wide Perspective. *Comput. Ind. Eng.* **2022**, *163*, 107827. [CrossRef]
10. Franklin, C. The Role of Standards in Human–Robot Integration Safety. In *Intelligent Systems, Control and Automation: Science and Engineering*; Springer Science and Business Media B.V.: Berlin/Heidelberg, Germany, 2022; Volume 81, pp. 155–171. ISBN 22138994, 22138986.
11. Berx, N.; Adriaensen, A.; Decré, W.; Pintelon, L. Assessing System-Wide Safety Readiness for Successful Human–Robot Collaboration Adoption. *Safety* **2022**, *8*, 48. [CrossRef]
12. *ISO 12100:2010*; Safety of Machinery—General Principles for Design—Risk Assessment and Risk Reduction. ISO: Geneva, Switzerland, 2011.
13. *ISO/TS 15066:2016*; Robots and Robotic Devices—Collaborative Robots. ISO: Geneva, Switzerland, 2016.
14. *ISO 10218-1:2011*; Robots and Robotic Devices—Safety Requirements for Industrial Robots—Part 1: Robots. ISO: Geneva, Switzerland, 2011.
15. *ISO 10218-2:2011*; Robots and Robotic Devices—Safety Requirements for Industrial Robots—Part 2: Robot Systems and Integration. ISO: Geneva, Switzerland, 2011.
16. Chemweno, P.; Pintelon, L.; Decre, W. Orienting Safety Assurance with Outcomes of Hazard Analysis and Risk Assessment: A Review of the ISO 15066 Standard for Collaborative Robot Systems. *Saf. Sci.* **2020**, *129*, 104832. [CrossRef]
17. Chang, Y.; Khan, F.; Ahmed, S. A Risk-Based Approach to Design Warning System for Processing Facilities. *Process Saf. Environ. Prot.* **2011**, *89*, 310–316. [CrossRef]
18. Saenz, J.; Bessler-Etten, J.; Valori, M.; Prange-Lasonder, G.B.; Fassi, I.; Bidard, C.; Lassen, A.B.; Paniti, I.; Toth, A.; Stuke, T.; et al. An Online Toolkit for Applications Featuring Collaborative Robots Across Different Domains. *IEEE Trans. Hum.-Mach. Syst.* **2022**, *53*, 657–667. [CrossRef]

19. Krishnan, R.; Bhada, S.V. An Integrated System Design and Safety Framework for Model-Based Safety Analysis. *IEEE Access* **2020**, *8*, 146483–146497. [CrossRef]
20. Lind, M. *Foundations for Functional Modeling of Technical Artefacts*; Springer: Berlin/Heidelberg, Germany, 2023; ISBN 3031459172, 3031459180, 9783031459177, 9783031459184.
21. Broy, M.H.B. From System Requirements Documents to Integrated System Modeling Artifacts. In Proceedings of the 9th ACM Symposium on Document Engineering, Munich, Germany, 15–18 September 2009.
22. Brown, D.C.; Chandrasekaran, B. *Design Problem Solving*; Morgan Kaufmann: Burlington, MA, USA, 1989; ISBN 0273087665, 1322471142, 1483258882, 9780273087663, 9781322471143, 9781483258881.
23. U.S. Congress. Government Performance and Results Act of 1993. In *103rd Congress*; Congressional Record: Washington, DC, USA, 1993.
24. Saji, G. Safety Goals in "risk-Informed, Performance-Based" Regulation. *Reliab. Eng. Syst. Saf.* **2003**, *80*, 163–172. [CrossRef]
25. Laurie, G.; Harmon, S.H.E.; Arzuaga, F. Foresighting Futures: Law, New Technologies, and the Challenges of Regulating for Uncertainty. *Law Innov. Technol.* **2012**, *4*, 1–33. [CrossRef]
26. Center for Chemical Process Safety (CCPS). *Guidelines for Risk Based Process Safety*; CCPS: Hoboken, NJ, USA, 2007.
27. Van Eerd, D. Knowledge Transfer and Exchange in Health and Safety: A Rapid Review. *Policy Pract. Health Saf.* **2019**, *17*, 54–77. [CrossRef]
28. Chakrabarti, A.; Bligh, T.P. A Scheme for Functional Reasoning in Conceptual Design. *Des. Stud.* **2001**, *22*, 493–517. [CrossRef]
29. Li, R.; Wu, J.; Ravn, O.; Zhang, X. Analyzing Hazards in Process Systems Using Multilevel Flow Modelling: Challenges and Opportunities. In Proceedings of the 32nd European Safety and Reliability Conference, Dublin, Ireland, 28 August–1 September 2022; pp. 1441–1448.
30. Guiochet, J. Hazard Analysis of Human-Robot Interactions with HAZOP-UML. *Saf. Sci.* **2016**, *84*, 225–237. [CrossRef]
31. Wu, J.; Lind, M. Management of System Complexity in HAZOP for the Oil &Gas Industry. *Ifac-Pap.* **2018**, *51*, 211–216. [CrossRef]
32. Inam, R.; Raizer, K.; Hata, A.; Souza, R.; Forsman, E.; Cao, E.; Wang, S. Risk Assessment for Human-Robot Collaboration in an Automated Warehouse Scenario. In Proceedings of the 2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA), Torino, Italy, 4–7 September 2018; Volume 1, pp. 743–751.
33. Aby, G.R.; Issa, S.F. Safety of Automated Agricultural Machineries: A Systematic Literature Review. *Safety* **2023**, *9*, 13. [CrossRef]
34. Modarres, M. Functional Modeling of Complex Systems with Applications. In Proceedings of the IEEE Annual Reliability and Maintainability Symposium, Washington, DC, USA, 18–21 January 1999; pp. 418–425.
35. *IEC 61882:2016*; Hazard and Operability Studies (HAZOP Studies)—Application Guide. International Electrotechnical Commission: Geneva, Switzerland, 2016.
36. *EN ISO 14118:2018*; Safety of Machinery—Prevention of Unexpected Start-Up. CEN: Brussels, Belgium, 2018.
37. *EN ISO 13850:2015*; Safety of Machinery—Emergency Stop Function—Principles for Design. CEN: Brussels, Belgium, 2015.
38. *EN 1837:2020*; Safety of Machinery—Integral Lighting of Machines. CEN: Geneva, Switzerland, 2020.
39. *EN ISO 13849-1:2023*; Safety of Machinery—Safety-Related Parts of Control Systems—Part 1: General Principles for Design. CEN: Brussels, Belgium, 2023.
40. *EN ISO 13849-2:2012*; Safety of Machinery—Safety-Related Parts of Control Systems—Part 2: Validation. CEN: Brussels, Belgium, 2023.
41. *EN ISO 25119-1:2023*; Tractors and Machinery for Agriculture and Forestry—Safety-Related Parts of Control Systems—Part 1: General Principles for Design and Development. CEN: Brussels, Belgium, 2023.
42. *EN ISO 25119-1:2023/A1:2023*; Tractors and Machinery for Agriculture and Forestry—Safety-Related Parts of Control Systems—Part 1: General Principles for Design and Development—Amendment 1. CEN: Brussels, Belgium, 2023.
43. *EN ISO 25119-2:2023*; Tractors and Machinery for Agriculture and Forestry—Safety-Related Parts of Control Systems—Part 2: Concept Phase. CEN: Brussels, Belgium, 2023.
44. *EN ISO 25119-3:2023*; Tractors and Machinery for Agriculture and Forestry—Safety-related parts of Control Systems—Part 3: Series Development, Hardware and Software. CEN: Brussels, Belgium, 2023.
45. *EN ISO 25119-3:2023/A1:2023*; Tractors and Machinery for Agriculture and Forestry—Safety-Related Parts of Control Systems—Part 3: Series Development, Hardware and Software—Amendment 1. CEN: Brussels, Belgium, 2023.
46. *EN ISO 25119-4:2023*; Tractors and Machinery for Agriculture and Forestry—Safety-Related Parts of Control Systems—Part 4: Production, Operation, Modification and Supporting Processes. CEN: Brussels, Belgium, 2023.
47. *EN ISO 25119-4:2023/A1:2023*; Tractors and Machinery for Agriculture and Forestry—Safety-Related Parts of Control Systems—Part 4: Production, Operation, Modification and Supporting Processes—Amendment 1. CEN: Brussels, Belgium, 2023.
48. *EN ISO 18497:2018*; Agricultural Machinery and Tractors—Safety of Highly Automated Agricultural Machines—Principles for Design. CEN: Brussels, Belgium, 2018.
49. *EN ISO 11252:2013*; Lasers and Laser-Related Equipment—Laser Device—Minimum Requirements for Documentation. CEN: Brussels, Belgium, 2013.
50. *EN ISO 60825:2014*; Safety of Laser Products—Part 1: Equipment Classification and Requirements. CEN: Brussels, Belgium, 2014.

51. *EN IEC 60947-1:2021*; Low-Voltage Switchgear and Controlgear—Part 1: General Rules. CEN: Brussels, Belgium, 2021.
52. *EN IEC 62368-1:2024*; Audio/Video, Information and Communication Technology Equipment—Part 1: Safety Requirements. CEN: Brussels, Belgium, 2024.
53. *IEC TR 62368-2:2019*; Audio/Video, Information and Communication Technology Equipment—Part 2: Explanatory Information Related to IEC 62368-1:2018. IEC: Geneva, Switzerland, 2019.
54. *EN IEC 62368-3:2020*; Audio/Video, Information and Communication Technology Equipment—Part 3: Safety Aspects for DC Power Transfer Through Communication Cables and Ports. CEN: Brussels, Belgium, 2020.
55. *EN 614-1:2006+A1:2009*; Safety of Machinery—Ergonomic Design Principles—Part 1: Terminology and General Principles. CEN: Brussels, Belgium, 2009.
56. *EN 614-2:2000+A1:2008*; Safety of Machinery—Ergonomic Design Principles—Part 2: Interactions Between the Design of Machinery and Work Tasks. CEN: Brussels, Belgium, 2008.
57. *EN 894-1:1997+A1:2008*; Safety of Machinery—Ergonomics Requirements for the Design of Displays and Control Actuators—Part 1: General Principles for Human Interactions with Displays and Control Actuators. CEN: Brussels, Belgium, 2008.
58. *EN 894-2:1997+A1:2008*; Safety of Machinery—Ergonomics Requirements for the Design of Displays and Control Actuators—Part 2: Displays. CEN: Brussels, Belgium, 2008.
59. *EN 894-3:2000+A1:2008*; Safety of Machinery—Ergonomics Requirements for the Design of Displays and Control Actuators—Part 3: Control Actuators. CEN: Brussels, Belgium, 2008.
60. *EN 894-4:2010*; Safety of Machinery—Ergonomics Requirements for the Design of Displays and Control Actuators—Part 4: Location and Arrangement of Displays and Control Acturators. CEN: Brussels, Belgium, 2010.
61. *EN ISO 14123-1:2015*; Safety of Machinery—Reduction of Risks to Health Resutling from Hazardous Substances Emitted by Machinery—Part 1: Principles and Specifications for Machinery Manufacturers. CEN: Brussels, Belgium, 2015.
62. *EN ISO 14123-2:2015*; Safety of Machinery—Reduction of Risks to Health Resutling from Hazardous Substances Emitted by Machinery—Part 2: Methodology Leading to Verfication Procedures. CEN: Brussels, Belgium, 2015.
63. *EN ISO 4413:2010*; Hydraulic Fluid Power—General Rules and Safety Requirements for Systems and Their Components. CEN: Brussels, Belgium, 2010.
64. *EN 13490:2001+A1:2008*; Mechanical Vibration—Industrial Trucks—Laboratory Evaluation and Specification of Operator Seat Vibration. CEN: Brussels, Belgium, 2008.
65. *EN ISO 16231-1:2013*; Self-Propelled Agricultural Machinery—Assessment of Stability—Part 1: Principles. CEN: Brussels, Belgium, 2013.
66. *EN ISO 16231-2:2015*; Self-propelled Agricultural Machinery—Assessment of Stability—Part 2: Determination of Static Stability and Test Procedures. CEN: Brussels, Belgium, 2015.
67. *EN ISO 16230-1:2015*; Agricultural Machinery and Tractors—Safety of Higher Voltage Electrical and Electronic Components and Systems—Part 1: General Requirements. CEN: Brussels, Belgium, 2015.
68. *EN 12965:2019*; Tractors and Machinery for Agriculture and Forestry—Power Take-Off (PTO) Drive Shafts and Their Guards—Safety. CEN: Brussels, Belgium, 2019.
69. *EN 61010-1:2020*; Safety Requirements for Electrical Equipment for Measurement, Control, and Laboratory Use—Part 1: General Requirements. CEN: Brussels, Belgium, 2010.
70. *EN ISO 14982:2009*; Agricultural and Forestry Machinery—Electromagnetic Compatibility—Test Methods and Acceptance Criteria. CEN: Brussels, Belgium, 2009.
71. *EN IEC 61204-7:2018*; Low-Voltage Switch Mode Power Supplies—Part 7: Safety Requirements. CEN: Brussels, Belgium, 2009.
72. *ETSI EN 303 413 V1.2.1:2021*; Satellite Earth Stations and Systems (SES); Global Navigation Satellite System (GNSS) Receivers; Radio equipment Operating in the 1164 MHz to 1300 MHz and 1559 MHz to 1610 MHz Frequency Bands; Harmonised Standard for Access to Radio Spectrum. ETSI: Sophia-Antipolis, France, 2009.