International Journal of Internet, Broadcasting and Communication Vol.14 No.1 209-218 (2022)
http://dx.doi.org/10.7236/IJIBC.2022.14.1.209

IJIBC 22-1-26

On Safety Improvement through Process Establishment for SOTIF Application of Autonomous Driving Logistics Robot

Kyoung Lak Choi*, Min Joong Kim**, Young Min Kim**†

** Senior Engineer, Automotive Engineering Service Team, DNV GL Business Assurance Korea*
*** Department of Systems Engineering, Ajou University, Korea*
kyoung.lak.choi@dnvgl.com, aquamjkim@ajou.ac.kr, pretty0m@ajou.ac.kr

Abstract

Today, with the development of the Internet and mobile technology, consumers' purchasing patterns have shifted from offline to online. In addition, due to the recent COVID-19, online purchases have significantly increased, and accordingly, the courier industry for logistics delivery has also grown significantly. Various logistics robots are being operated in many industrial and can reduce the labor intensity and physical and mental fatigue of workers. However, if the logistics robot does not properly recognize the people or environment around it, it can lead to a serious accident. We conducted that how logistics robots can perform safe work in a working environment such as a logistics warehouse through the application of ISO/DIS 21448 (SOTIF) to autonomous logistics transport robots. This result is expected to contribute to the operation of unmanned logistics warehouses using AGV.

***Keywords:** ISO/DIS 21448 (SOTIF), Automated Guided Vehicle (AGV), Logistics Robot, Safety Analysis, Hazards, Safety*

1. Introduction

Research is being actively conducted to increase the mobility and autonomy of autonomous robots so that they can perform services in various environments. As factories converting to a smart factory system and highly automated logistics warehouses increase due to COVID-19, a significant number of personnel are being replaced by robots [1]. Robot systems that can reduce the labor intensity and physical and mental fatigue of workers in various industrial fields are increasing interest in improving safety between workers and robots as mobility and collaboration functions with humans are emphasized recently. As Simultaneous Localization and Mapping (SLAM) technology is applied to Autonomous Mobile Robot (AMR) in an Automated Guided Vehicle (AGV) that moves along a fixed path, the range of movement of the robot has become wider, and as interest in faster movement in the existing indoor and outdoor environments increases, it can lead to a major accident if it cannot process a lot of sensing information in a much more diverse environment and predict the movement of surrounding obstacles compared to indoors. In order to derive design requirements optimized for urban railway platforms, the concept of operation of AGV-based vertical and horizontal transportation

Manuscript Received: January. 17, 2022 / Revised: January. 20, 2022 / Accepted: January. 25, 2022
Corresponding Author: pretty0m@ajou.ac.kr (YoungMin KIM)
Tel: +82-31-219-3949, Fax: +82-31-219-2334
Dept. of Systems Engineering, Ajou University, Korea

machines and cargo lifting platforms was designed [2]. A technology was proposed for autonomous mobile logistics robots to recognize workers working in the same space using laser sensors [3]. As shown in Figure 1, the autonomous driving logistics transfer robot used in the logistics system is mainly used for the purpose of transporting or sorting materials for product assembly, mail, or parcel delivery in factories or warehouses, etc. Figure 1 (a) is a KIVA robot operated by Amazon that can carry a load shelf. Figure 1 (b) shows that by mounting a conveyor on the head, the existing conveyor system can automatically load and unload goods on and off the robot. Figure 1 (c) is a mobile cooperative robot that transports products to the manufacturing line and delivers them to workers. Figure 1 (d) can be used for a wide range of towing operations using hooks. Figure 1(e) can perform a variety of tasks such as firefighting, farm work and sports training support, and its off-road capability allows autonomous driving on rugged terrain such as farms and mountains. Figure 1(f) is an autonomous vehicle capable of transporting containers.

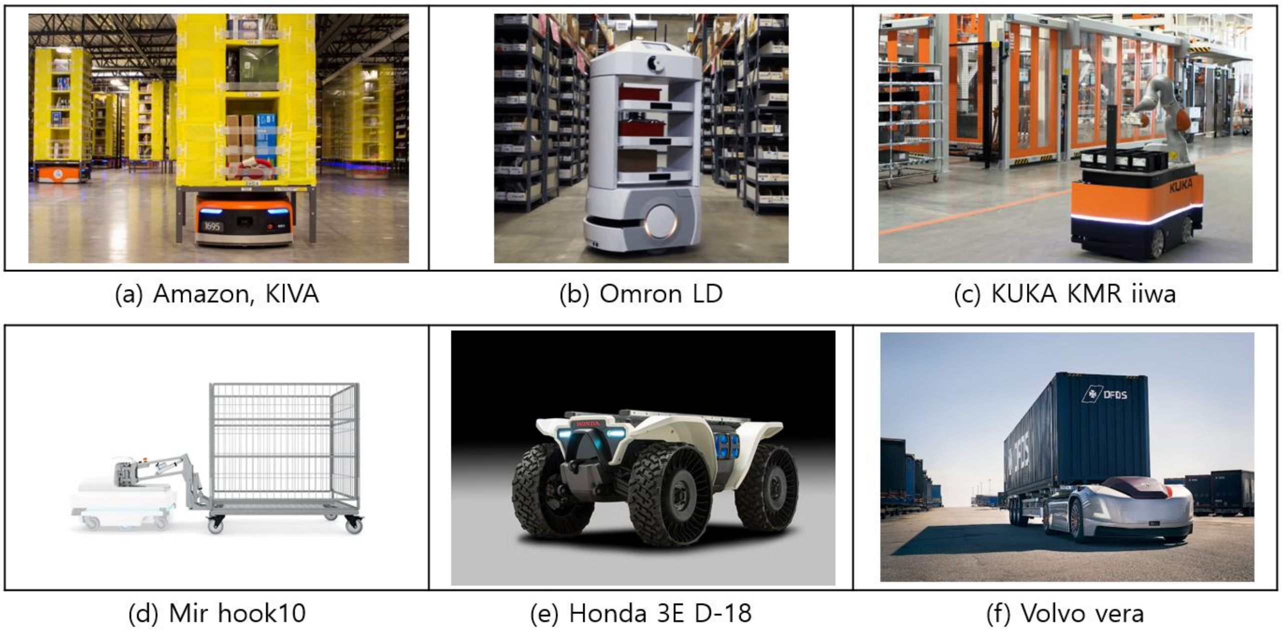
(a) Amazon, KIVA
(b) Omron LD
(c) KUKA KMR iiwa
(d) Mir hook10
(e) Honda 3E D-18
(f) Volvo vera

Figure 1. Various type of industrial Automated Guided Vehicle (AGV)

In particular, since a large number of robots move in this case, a centralized control method using a separate physical server can be used for real-time control, but there is a problem that all robots are affected due to increased server load, errors, and breakdowns. Research is being conducted on a method in which each robot independently calculates and moves an optimal path, and tries to judge the situation between robots by sharing the surrounding situation including obstacle information with other robots in real time. However, even in this case, there is a limit to predicting various scenario situations on the driving route in advance and responding more actively, and even if there is no functional failure of the robot or surrounding system, the response to the occurrence of dangerous situations due to performance limitations is insufficient to be.

2. Necessity of SOTIF Application of Autonomous Driving Logistics Robot

ISO 21448 Safety of The Intended Functionality (SOTIF) aims to reduce areas of risk (Area 2) and unknown risk (Area 3) known as the impact of the surrounding environment, limitations of situational perception according to technology or performance, rather than accidents caused by failure, as shown in Figure 2.

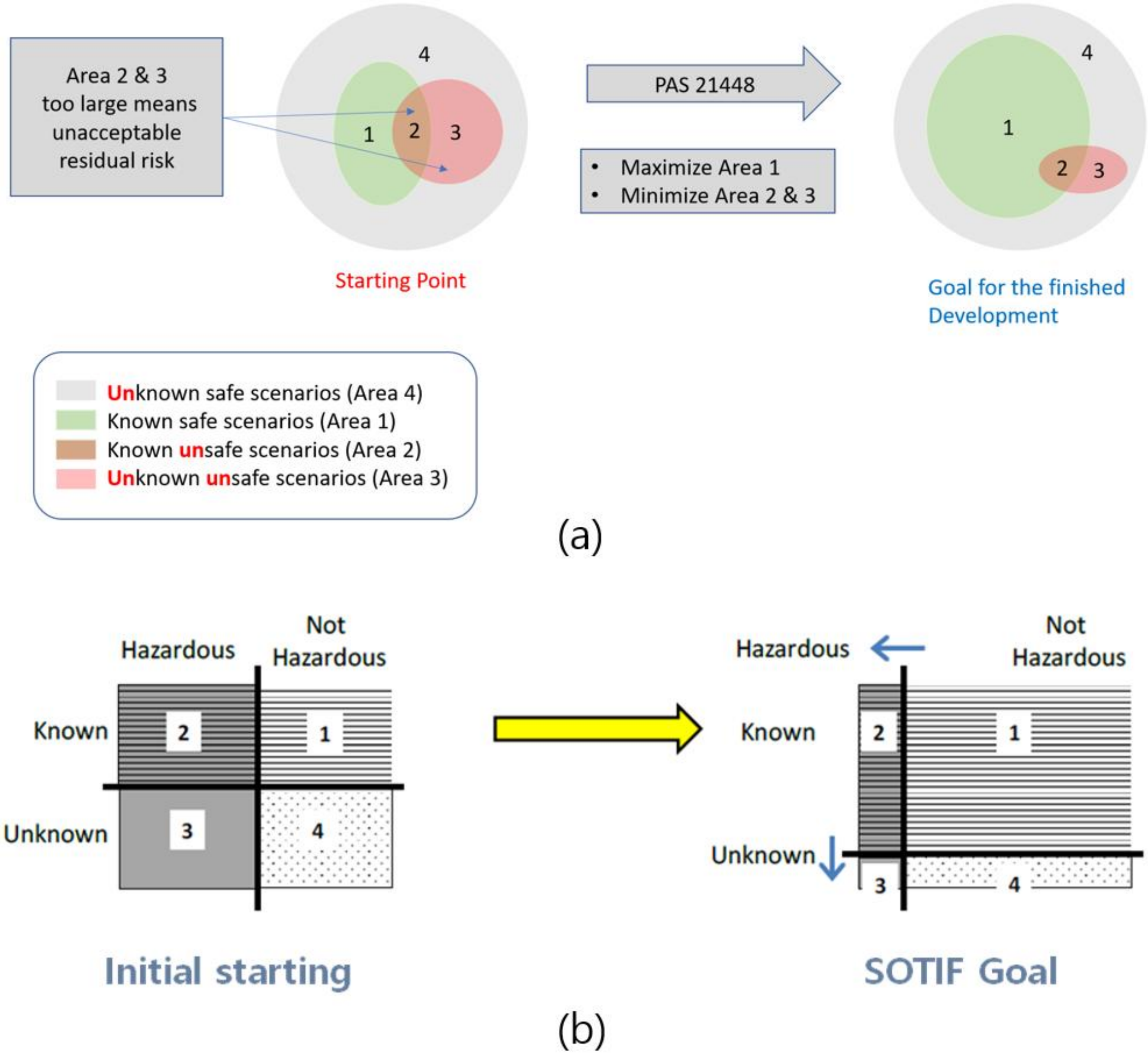
Area 2 & 3 too large means unacceptable residual risk
4
1
2
3
Starting Point
PAS 21448
• Maximize Area 1
• Minimize Area 2 & 3
4
1
2
3
Goal for the finished Development
Unknown safe scenarios (Area 4)
Known safe scenarios (Area 1)
Known unsafe scenarios (Area 2)
Unknown unsafe scenarios (Area 3)
(a)
Hazardous
Not Hazardous
Known
Unknown
2
1
3
4
Initial starting
Hazardous
Not Hazardous
Known
Unknown
2
1
3
4
SOTIF Goal
(b)

Figure 2. The goal of SOTIF

Figure 2 (a) shows a visualization of the SOTIF scenario and Figure 2 (b) shows the final goal of SOTIF, minimizing area 2 and area 3, and maximizing area 1. SOTIF deals with situations that are not failures. SOTIF is divided into four main areas. 1) Known safe scenarios (area1), 2) Known unsafe scenarios (area2), 3) Unknown safe scenarios (area4), and 4) Unknown unsafe scenarios (area3). Figure 1 shows a visualization of the four areas of SOTIF. The purpose of SOTIF is to reduce unknown or unsafe situations. In the case of recent autonomous vehicles, it is assumed that the intended function is safe, and following the application of the ISO 26262 automotive functional safety standard to prevent accidents due to defects, errors, and breakdowns of internal/external systems that may cause dangerous behavior, there is an increasing interest in ISO 21448 SOTIF to prevent accidents due to wrong perceptions or judgments about performance limitations and situations. In addition, research is being conducted to improve the safety of autonomous vehicles by applying the Responsibility Sensitive Safety (RSS) model based on the camera sensor [4]. Similarly, in the case of autonomous robots, the application of SOTIF or RSS models should be considered in order to achieve a specific service purpose while securing safety in moving and driving environments in outdoor spaces in various environments in a limited indoor space.

2.1 Safety Issues for Use in Humans and Future Logistics Robot Environments

In the case of the logistics environment, various conditions may be considered depending on the logistics service or logistics system, and in the case of outdoor logistics transport considering long-distance transport, more severe environmental changes should be considered. For the optimization or efficiency of logistics services, the transport robot system will have an optimized form according to the service more and more, and it is expected to develop into a form that can overcome various environments at a faster speed. In the outdoor logistics environment of these multiple occurrence variables, if various scenarios for unexpected obstacles or sudden changes in the work and transport environment are not considered in advance, there may be a limit to actively coping with the algorithm performance of the driving robot itself at each time. For example, a rollover accident may occur if a scenario in which a rough road or a low friction road environment with a lot of slippage is not considered is predicted in advance and countermeasures are not prepared [5]. In addition, even with the same robot system, various unexpected safety issues may occur depending on the connection condition with the operator or the indoor/outdoor environment, which can be considered according to the work environment specialized for each service.

2.2 The Need to Supplement the Current International Standards for Logistics Robots

Mobility is a key factor in logistics robots, and various types of mobile robots are being developed based on this. In the case of non-mobile-type logistics support manipulator type robots, most of them are safety systems only fixed indoors in the surrounding barrier, and in the case of mobile robots, systems to cope with changes in the surrounding environment or fast-moving surroundings are technically and legally insufficient. Although many discussions are being made to prevent safety issues according to the current logistics environment, standards for the safety of mobile robots suitable for current service characteristics have not been made. In general, it specifies safety requirements for collaborative industrial robotic systems and work environments, supplements the requirements and guidelines [6], describes the basic risks associated with bots, and provides requirements for eliminating or appropriately reducing the risks associated with these risks [7]. And recently standards such as specify requirements and guidelines for intrinsically safe designs, safeguards and information for the use of personal care robots such as mobile servant robot, physical assistant robot, and person carrier robot [8], specify safety requirements and verification means for unmanned industrial trucks such as AVG, AMR, automated guided cart, under car etc. [9], and specifies safety requirements for industrial mobile robots (IMRs) [10] are starting to be used in domestic and foreign industries. In addition to standards for outdoor autonomous robot safety evaluation, in the United States, following ANSI/RIA R15.08 for mobile manipulator standards, international standards for mobile collaborative robots are being discussed at home and abroad [11]. Therefore, only with the currently applied international standards for logistics robots, problems caused by unexpected environmental changes lead to safety problems due to collisions with surrounding objects or people or animals. In particular, in the case of mobile cooperative robots, the current logistics robot standards alone may not only limit the universality of the standard itself but also the insufficient function and performance of various scenarios depending on the service sector.

2.3 Definition of the Problem

As shown in Figure 3, several potential risk scenarios that may arise in various logistics environments by service should be identified in advance in the pre-requirement stage, and specifications of the robot should be designed according to the identified safety requirements, in addition to general safety requirements.

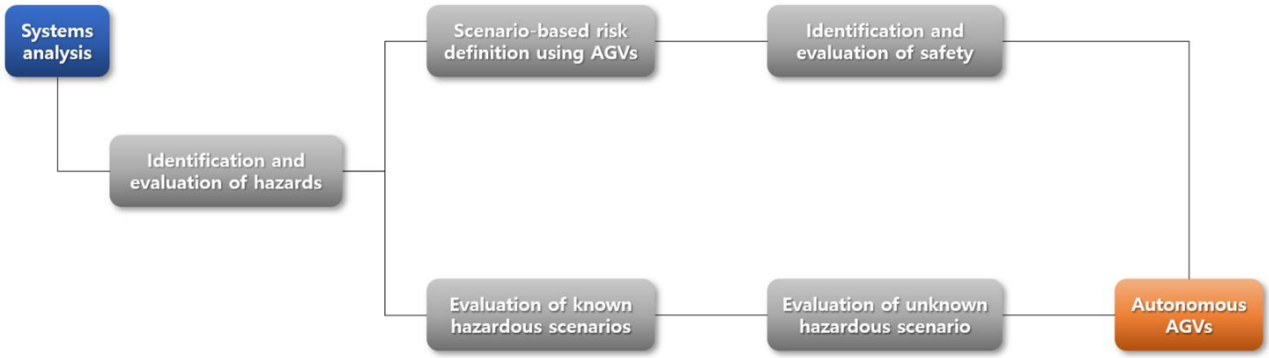
Systems analysis
Identification and evaluation of hazards
Scenario-based risk definition using AGVs
Identification and evaluation of safety
Evaluation of known hazardous scenarios
Evaluation of unknown hazardous scenario
Autonomous AGVs

Figure 3. Research object and scope

3. Establishment of Process for Securing Safety of Autonomous Driving Logistics Robot Reflecting SOTIF

3.1 Definition of Autonomous Driving Logistics Robot Operating Environment and Constraints

In this paper, in order to check whether the safety of SOTIF reflection is secured, the operating environment of the logistics robot is difficult to predict and is limited to a specific area of the indoor logistics environment as shown in Figure 4 rather than the outdoor environment where more conditions are considered. Constraints are as follows.

- **Logistics Robot**: It should have autonomous driving function and be able to sort and select goods and safely transport them to their destination.
- **Work Environment**: The work of mobile robots required in the logistics environment can be broadly divided into autonomous driving technology that allows the robot to drive itself and worker tracking technology for collaboration between the robot and the operator. In order to avoid collision with other workers or AGVs during movement, it should be able to detect obstacles and change routes or stop and wait.
- **Road Surface Condition**: The slope of the workplace should be kept to a minimum, and the road surface should not be irregular.

Figure 4. Working environment using AGVs in warehouse

3.2 Identification and Definition of Safety Factors for Autonomous Driving Logistics Robots

Safety issues were identified based on the scenario of the autonomous driving logistics robot operating system in the warehouse, and safety-related errors and events could be identified based on the identified requirements to increase the safety of the system. The scenario of the autonomous driving logistics robot system in the logistics warehouse performs the process of loading, transporting, and unloading cargo. Table 1 shows errors that can occur in an autonomous logistics transport robot system and their effects.

Table 1. Scenario-based hazard definition

Step	Error definition	Hazard identification
Load	Damage to standard cargo transport container	Cargo omission, fall, damage, etc. may occur during cargo transportation through standard cargo containers
	Cargo fixture error	The fixture after cargo loading is completed, cargo may fall or AGV may overturn during transportation
	Sensor error	Perception is crashed due to an error, damage to cargo and equipment may occur.
Transfer	Collision between AGVs	Overlapping movement paths, it may cause a collision if other AGVs are not recognized or an error occurs.
	Collision between AGV and person	Failure to recognize a person working during transportation or to respond to a person appearing suddenly can lead to a collision
	Unloading device error	Product damage may occur due to an unloading device error

Unloading	Sensor error	The product cannot be unloaded in the correct position due to a sensor error and the product may fall

3.3 Establishment of Process to Reflect SOTIF of Autonomous Driving Logistics Robot

It is the process according to ISO/DIS 21448 SOTIF standard and Figure 2, and the detailed output is as Table 2. Figure 5 shows the procedure performed by SOTIF [12].

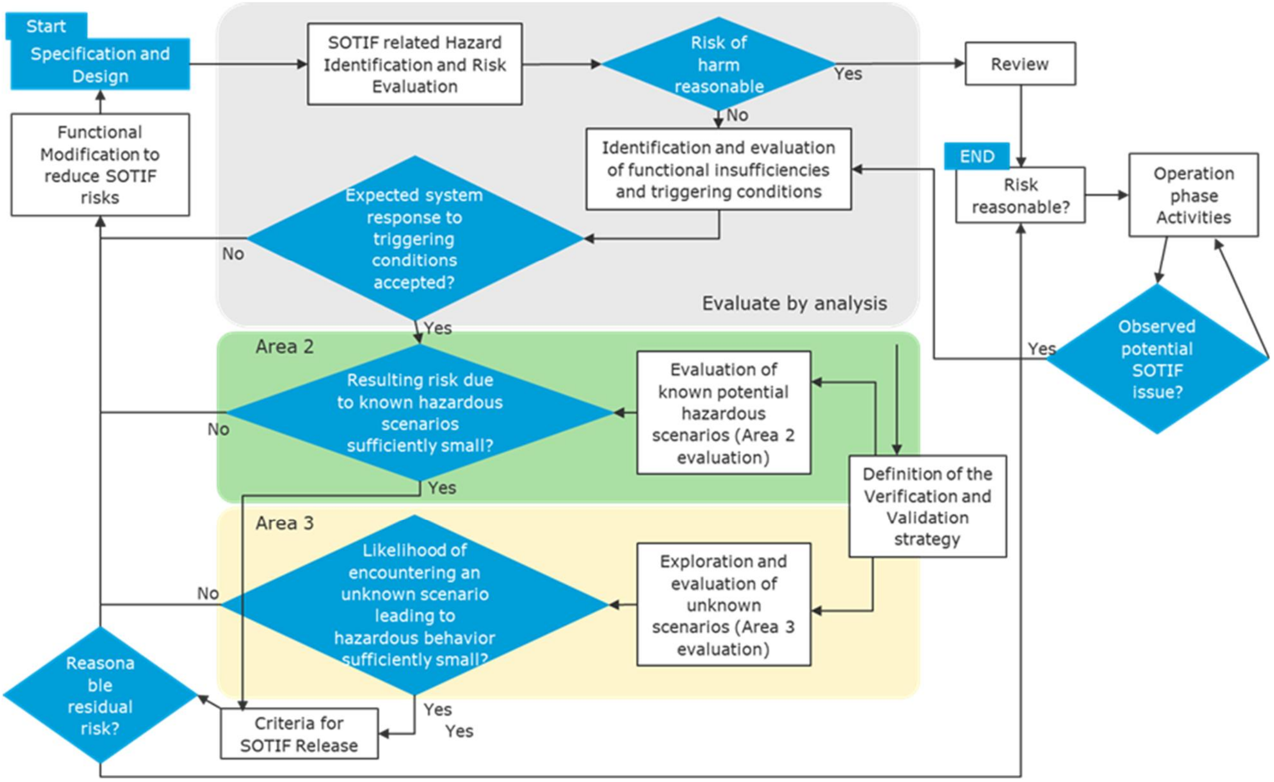
Start
Specification and Design
SOTIF related Hazard Identification and Risk Evaluation
Risk of harm reasonable
Yes
Review
No
Identification and evaluation of functional insufficiencies and triggering conditions
Functional Modification to reduce SOTIF risks
END
Risk reasonable?
Operation phase Activities
Expected system response to triggering conditions accepted?
No
Evaluate by analysis
Yes
Area 2
Resulting risk due to known hazardous scenarios sufficiently small?
No
Evaluation of known potential hazardous scenarios (Area 2 evaluation)
Yes
Observed potential SOTIF issue?
Definition of the Verification and Validation strategy
Yes
Area 3
Likelihood of encountering an unknown scenario leading to hazardous behavior sufficiently small?
No
Exploration and evaluation of unknown scenarios (Area 3 evaluation)
Reasonable residual risk?
Criteria for SOTIF Release
Yes
Yes

Figure 5. ISO/DIS 21448 SOTIF process

Table 2. Work products of SOTIF process

Clause		Work Products
5	Specification and design	- Documentation detailing the specification and design
6	Identification and evaluation of hazards	- Hazards at the vehicle level - Risk evaluation of hazardous behaviours - Acceptance criteria
7	Identification and evaluation of potential functional insufficiencies and triggering conditions	- Identified potential insufficiencies of specification, performance limitations and triggering conditions (including reasonably foreseeable direct misuse) - Evaluation of the response of the system to the identified triggering conditions for their acceptability

		with respect to the SOTIF
8	Functional insufficiencies and triggering conditions	- Specification of SOTIF measures
9	Definition of the verification and validation strategy	- Definition of the verification and validation strategy
10	Evaluation of known hazardous scenarios (Area 2)	- Verification results to show that the intended functionality behaves as expected in the known scenarios
11	Evaluation of unknown hazardous scenarios (Area 3)	- Validation results for unknown hazardous scenarios - Evaluation of the residual risk
12	Criteria for SOTIF release	- SOTIF release argumentation
13	Operation phase activities	- Field monitoring process

Table 2 shows the performance output for each step of the SOTIF. SOTIF clause 5 is to define and describe the functions, dependencies and interactions of the environment and other functions of the autonomous logistics robot, and to help the understanding of the functions so that they can carry out the activities of the subsequent steps. Therefore, it is essential to clearly define the scope of the intended function of the system by creating detailed descriptions of the concepts, roles, and limitations of cognitive and judgment technologies that constitute the system as the most important part to establish the scope of system development. In particular, similar to the consideration of driver misuse in autonomous vehicles, 'Operator Misuse' related to erroneous operation and mistakes of the robot operator that may occur in operating the robot system may also be included in the scope of this SOTIF. Therefore, defining the main use-cases from the operator's point of view during driving can also be considered, and static and dynamic obstacles including people on the driving path, other autonomous robots during platoon driving, environmental infrastructure on the driving path, and other systems Interactions, etc., need to be mentioned as well.

SOTIF clause 6 can be analyzed to perform HARA from the SOTIF perspective to identify risk events that may occur due to unintended actions and potential consequences (risks). At this time, Systems Theoretic Process Analysis (STPA) methodology is applied to identify risk sources and corresponding causal scenarios. STPA complements traditional methods such as Hazard and Operability study (HAZOP), Fault Tree Analysis (FTA), and Failure Mode and Effect Analysis (FMEA). In addition to problems caused by failure of specific functions or components, interactions or control problems between system components are considered as hazards, and are effective in identifying the hazards based on unsafe control actions between components constituting the system and deriving accident scenarios. Since the goal of SOTIF functional safety activities is to address all risk events related to failure to perform the intended function, the severity, exposure, and controllability of risk events are determined by operating situation. S and C are used as inequalities to describe only severity and controllability of the driver, and do not determine the ASIL grade.

The main goal of SOTIF clause 7 is to analyze the causes of risk situations defined in SOTIF clause 6 for the analysis of potential functional deficiencies and triggering conditions. The main task is to analyze the triggering event, which is a risk action factor, and this is to identify the limitations of the algorithm in the sensor or controller and the situations that may lead to the violation of safety goals. The process of defining and analyzing the triggering event, which is the factor that causes this, is thoroughly performed.

The purpose of SOTIF clause 8 is to define measures to overcome the occurrence factors analyzed in the triggering event analysis work of clause 7 in the situation where the risk derived from clause 6 occurs. The functional concept in which the functional changes are reflected in the system architecture defined in Section 5 is derived, and again it leads to the contents of the system specification in Section 5 through SOTIF iterative activities. Functional change methods and actions to avoid, reduce or mitigate SOTIF risk may include the introduction of HMI technology that mitigates SOTIF risk, depending on the authority or operating scope of the system, or the change in function to the level of communicating information to the operator.

SOTIF clause 9 deals with the verification plan of the function change technology developed so far. V&V on the risk of safety violation in the absence of faults in the system should be performed for the following items. SOTIF clause 10 derives known use-cases for verification of robot systems and individual elements (sensors, controllers, actuators) and performs verification. SOTIF clause 11 aims at sufficient verification to prevent robot systems and elements from causing irrational risk levels, that is, sufficient verification of unknown causes that may occur in real life through long driving, etc., or verification according to a new approach. V&V should be performed to sufficiently verify the residual SOTIF risk. SOTIF clause 12 aims to confirm whether the residual SOTIF risk of a robot system considering functional safety from the SOTIF perspective is an acceptable level before it is distributed to customers through mass production.

4. Design of Autonomous Driving Logistics Robot Reflecting SOTIF

As shown in Figure 2 above, the meaning of having many Unknown situations means that the probability of an unintended operation is high, and the Unsafe situation can be reduced through SOTIF activities. To this end, when designing the autonomous driving logistics robot, as mentioned in clause 8 of Table 2, it means that the SOTIF risk that can occur in the mobile logistics robot system is eliminated as much as possible through the functional modification process that solves the SOTIF-related risks.

4.1 Design Application of Autonomous Driving Logistics Robot

According to the process presented above, the design and application of the autonomous driving logistics robot should be applied. As suggested in this study, related products should be derived and applied by performing each STEP focusing on clause 5 to 8. In particular, in order to be applied to the autonomous driving logistics robot, the subject of this study, the following constraints must be observed. In this paper, when implementing the design of autonomous logistics robots within a specific logistics environment, the SOTIF process methodology is applied to identify risk sources considering the environmental conditions of robots that are difficult to handle in existing robot standards. In this way, through SOTIF design activities in the initial autonomous driving system architecture, we derive a new SOTIF improvement architecture that reflects the concept of functional improvement and functional change measures in five categories (hardware/software system improvement, function limitation, operator authority delegation, operator monitoring). For example, in the case of system improvement from a software perspective, technology application in terms of artificial intelligence can be considered, for example, with the aim of continuously improving signal quality or measuring effective obstacles in images.

5. Conclusion

Recently, as the spread of vehicles equipped with autonomous driving technology has increased, standards such as ISO 21448 have been established, and an RSS model for securing safety has been proposed. As autonomous driving technology advances, the gap between the concept of robots and automobiles is narrowing. In this paper, we applied the process and methodology according to the SOTIF standard developed only for automobiles were applied based on the ISO/DIS 21448 SOTIF standard established this year, considering the indoor and outdoor logistics autonomous driving robot that will be a concept similar to a fully autonomous vehicle in the near future. By applying SOTIF to an autonomous logistics transport robot, we investigated risk factors and ways to avoid and reduce the identified risk factors. In addition, it was confirmed that safety can be improved by applying SOTIF to the autonomous logistics transport robot. Through this result, it is expected that it will contribute to the operation of an unmanned logistics sensor using an autonomous logistics transport robot.

Acknowledgement

This work was supported by a grant from R&D program of the Korea Evaluation Institute of Industrial Technology (20014470)

References

[1] T. S. Kim, S. H. Kim, K. H. Kim, Y. T. Oh, J. H. Lee, W. B. Jo, and K. H. Kim, "Logistics Sorting System using Autonomous Driving Robot," *In Proceedings of the Korean Society of Computer Information Conference*, 29(2), pp. 491-492, 2021.

[2] S. M. Lee, J. M. Park, Y. M. Kim, and J. U. Kim, "On the Needs of Vertical and Horizontal Transportation Machines for Freight Transportation Standard Containers to Derive Design Requirements Optimized for the Urban Railway Platform Environment,*" International Journal of Internet, Broadcasting and Communication*, 13(4), pp.112-120, 2021.
DOI: https://doi.org/10.7236/IJIBC.2021.13.4.112

[3] J. M. Kim, J. H. Jo, C. B. Moon, "People Tracking using the Grid and CAD Map in the Large Scale Logistics Environments," *In Proceedings of the Korean Society for Precision Engineering*, 12, pp.291-292, 2017.

[4] M. J. Kim, S. H. Yu, T. H. Kim, J. U. Kim, and Y. M. Kim, "On the Development of Autonomous Vehicle Safety Distance by an RSS Model Based on a Variable Focus Function Camera," *Sensors* 21, No. 20: 6733. 2021.
DOI: https://doi.org/10.3390/s21206733

[5] J. B. Han, S. S. Kim, H. J. Song, "Development of Real-Time Digital twin model of Autonomous Field Robot for Prediction of Vehicle Stability," *Journal of Institute of Control, Robotics and Systems* 27(3), 190-196, 2021.
DOI: https://doi.org/10.5302/J.ICROS.2021.20.0181

[6] "ISO TS 15066:2016 Robots and robotic devices - Collaborative robots"

[7] "ISO 10218-1:2011 Robots and robotic devices - Safety requirements for industrial robots"

[8] "ISO 13482:2014 ROBOTS AND ROBOTIC DEVICES — SAFETY REQUIREMENTS FOR PERSONAL CARE ROBOTS"

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

[10] "ANSI/RIA R15.08-1-2020 Industrial Mobile Robots - Safety Requirements - Part 1: Requirements For The Industrial Mobile Robot"

[11] A. Markis, M. Papa, D. Kaselautzke, M. Rathmair, V. Sattinger, and M. Brandstotter. "Safety of mobile robot systems in industrial applications," *In Proceedings of the ARW & OAGM Workshop*, pp. 26-31, 2019.

[12] "ISO/DIS 21448:2021 Road vehicles-Safety of the intended functionality"