中國機械工程學刊第四十一卷第二期第 199~209 頁(民國一百零九年)
Journal of the Chinese Society of Mechanical Engineers, Vol.41, No.2, pp 199~209 (2020)

# Safety of Human–Robot Interaction: Concepts and Implementation Based on Robot-Related Standards

Hsiang-Yuan Ting*, Huan-Kun Hsu*, Ming-Bao Huang* and Han-Pang Huang**

**Keywords**： Human–robot collaboration, ISO 13849, ISO 15066, physical human–robot interaction, pre-collision safety strategy.

## ABSTRACT

In this article, the core concepts of the safety standards of machinery and robots are introduced, and the pre-collision safety strategies that integrate operating speed adjustments and motion trajectory modifications in order to guarantee the safety of humans are explored. We propose a safety strategy based on risk assessment and speed reduction procedures to avoid collisions between robots and humans. The proposed strategy uses a Kinect sensor to estimate the distance between a human and the robot to slow the robot down or to calculate the virtual force in the risk space to further modify the motion of the robot. The strategy is validated by experiment results. Particularly, the proposed strategy can meet the requirements of the ISO 15066 guidelines for the robot in a human–robot collaboration. Additionally, the loop structure of safety function included in the proposed strategy can meet performance level e of ISO 13849.

## INTRODUCTION

In recent decades, human–robot collaboration (HRC) and physical human–robot interaction (pHRI) issues have received a lot of attention (Huang and Huang, 2019). Blending the advantages of the high levels of flexibility and sensitivity of human beings with the high precision and speed of robots to advance the synergy of human–robot co-performance in manufacturing facilities and daily tasks of life have been extensively explored and studied (Goodrich and Schultz, 2008; Krüger et al., 2009; Wang et al., 2017). However, the closer the proximity of human beings and robots in a space has, the higher the risk of unexpected collisions potentially occurs. This means that safety issues should be more seriously considered (Lasota et al., 2017; Villani et al., 2018).

Robot safety is regarded by both the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) as part of mechanical safety, and therefore, the safety standard guidelines for robots based on risk management are also developed according to the ISO/IEC Guide 51 (ISO/IEC, 2014). In these guidelines, the definition of safety is that the hazard risk has been reduced to a tolerable level. Since risk assessment and reduction are the core ideas of the safety standards of robots, the ISO/IEC has exerted a lot of effort to establish a comprehensive and strict framework of standards for robot safety in recent years (Moon et al., 2013). For example, the technical specifications ISO/TS 15066 (ISO/TS, 2016) based on ISO 12100 guidelines (ISO, 2010) for collaborative operating systems with robots have been established.

Due to past limitations of sensors and controllers, the most effective method, which was recommended by ISO 10218 (ISO, 2011; ISO, 2011), was to minimize risks during operation by separating the robots from human operators. Under these standards, when human operators or any objects enter the workspace of robots, the robots must immediately stop operating, but this means that the efficiency of production is reduced. In order to develop an efficient HRC system, the elimination of this separation of human operators and robots, without creating any hazards to humans, is necessary.

The safety strategy for HRC can be roughly divided into two approaches: post-collision and pre-collision. The post-collision approach is aimed at minimizing or confining any impacts of a collision by means of mechanical designs and control measures to

*Paper Received June, 2019. Revised September, 2019, Accepted October, 2019, Author for Correspondence: Han-Pang Huang.*

** Student, Department of Mechanical Engineering, National Taiwan University, No. 1, Sec. 4, Roosevelt Rd., Taipei 10617, TAIWAN (R.O.C.).*

***Professor, Department of Mechanical Engineering, National Taiwan University, No. 1, Sec. 4, Roosevelt Rd., Taipei 10617, TAIWAN (R.O.C.).*

ensure that the collision will not result in serious and irreversible damage to humans or robotic systems, e.g., the use of visco-elastic materials to envelop robots (Yamada et al., 1997) or the redesign of variable stiffness joint (Vanderborght et al., 2013). Equipping robots with sensors is another post-collision safety approach. In using sensors, robots can detect collisions and react appropriately (Golz et al., 2015). It is worth noting that these post-collision strategies have limitations that make it impossible to guarantee that any injury caused by an impact will be tolerable to the human body.

On the other hand, the purpose of a pre-collision strategy is to apply related parameters, such as distance and relative speed between robots and human operators, to predict the occurrence of collisions and enhance the capacity of robots to avoid them. One of the most notable methodologies that can be applied to the pre-collision approach is the potential field method (Khatib, 1985), which generates a virtual repulsive or attractive force based on the calculation of the distance between the robot and human operators, obstacles, and target objectives. This can help robots to prevent collisions with obstacles while still approaching their target position (Lacevic and Rocco, 2010; Flacco et al., 2012). The introduction of a risk index in the safety control strategy is another common approach. Whenever the risk index exceeds a set threshold, a decrease in speed or an alternative trajectory of robots can then be carried out (Kulić and Croft, 2007). Furthermore, for the purposes of allowing the robot to perform the dodging action with the least interruption to the original task, the vector space of the potential collision point is defined as a risk space, and the collision-avoidance plans are designed through virtual impedance control in the risk space (Lo et al., 2016).

According to ISO 15066 guidelines, at least one appropriate safety strategy should be selected when performing HRC operations. So it is crucial to conduct a systematic study of relevant mechanical safety standards to meet the safety requirements proposed by ISO 15066 for four types of HRC operations. In this study, we researched risk assessment and reduction procedures from the standards side to define the conditions and requirements for performing HRC tasks, and we further propose a control strategy to reduce speeds or avoid collisions when the distance between a human operator and robot is narrowing. This pre-collision strategy can also meet the requirements for speed and separation monitoring presented in the ISO 15066 guidelines.

The rest of this article is laid out as follows: Section II discusses the safety standards of mechanical aspects to elaborate the core concept and scheme on the basis of risk management, and then introduces the procedures and methodologies for performing functional safety assessments. Next, an introduction to current industrial robot standards and the requirements of ISO 15066 for four types of HRC are discussed in Section III. In Section IV, our proposed pre-collision safety strategy that can conform to ISO 15066 guidelines is described. The experimental verification and validation of the proposed strategy are presented in Section V. Finally, the conclusions are in Section VI.

## 2. THE RISK-BASED GUIDELINE OF MACHINERY

In order to build an architecture and provide a guide for the standard of mechanical safety, ISO and IEC jointly released the ISO/IEC Guide 51 document which defines the concept of safety. According to the concept of risk management, the safety of machinery is determined in a relative fashion.

**Risk Assessment and Risk Reduction**

According to Guide 51, the concept of industrial machinery safety is meant to ensure that the risks generated by the operation of machinery are acceptable. There are two major problems: one is how to assess the risks that may be caused by the machinery, and the other is to guarantee the risk value is reduced to an acceptable range. In order to introduce the concept of risk management in the design stage, the ISO has proposed a Type-A standard in ISO 12100, which not only defines the core concepts, terms, and definitions of the safety of machinery but also provides the principles and measures of risk assessment and risk reduction. The complete flow chart of risk management of machinery in the design stage is presented in Fig. 1 and divided into two parts, risk assessment and risk reduction.

The whole process starts at the risk assessment stage and passes through four steps to evaluate the quantified risk, and if the quantified risk cannot be accepted, the process enters the risk reduction stage and passes through three steps to reduce the risk to an acceptable range.

*(1) Risk assessment*

In ISO 12100, the standards for risk assessment recommend sequential completion of the following assessment process in the early stages of the design of a mechanical product. The designer uses appropriate and reasonable assessment tools to estimate and quantify the risk, such as the probability of producing a dangerous state and the severity of the hazard. If the risk value is not acceptable, the risk reduction process must be completed.

*(2) Risk reduction*

After risk assessment, the quantified risk is divided into three levels, as shown in Fig. 2. Three levels include an intolerable region; a tolerable, or “as low as reasonably practicable” (ALARP) region; and an acceptable region. If the risk value is too high to tolerate, the process of risk reduction must be carried out. It is important to note that the risk always exists regardless of efforts at reduction. When the risk value

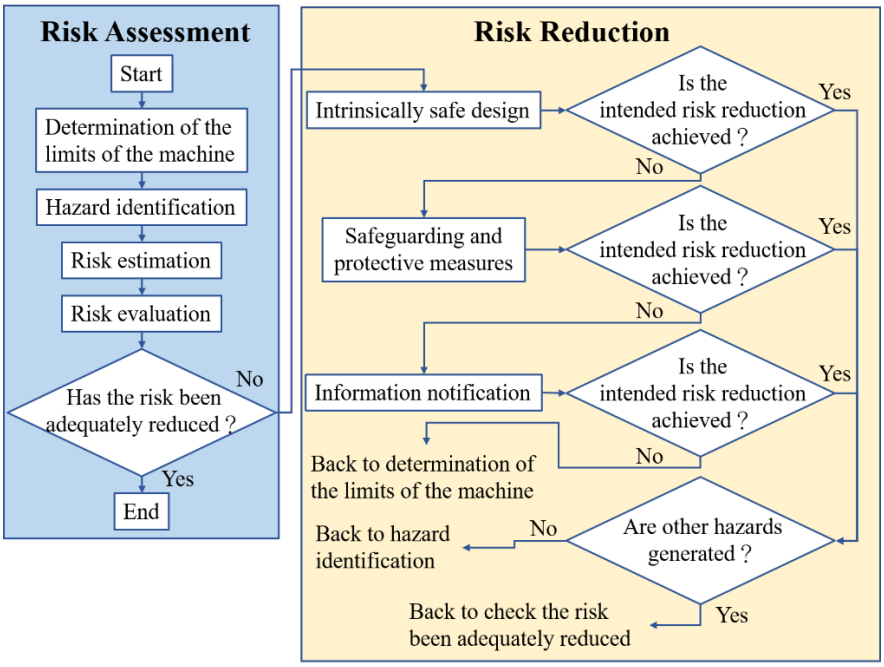


Fig. 1. The flow chart of risk management of machinery in the design stage.

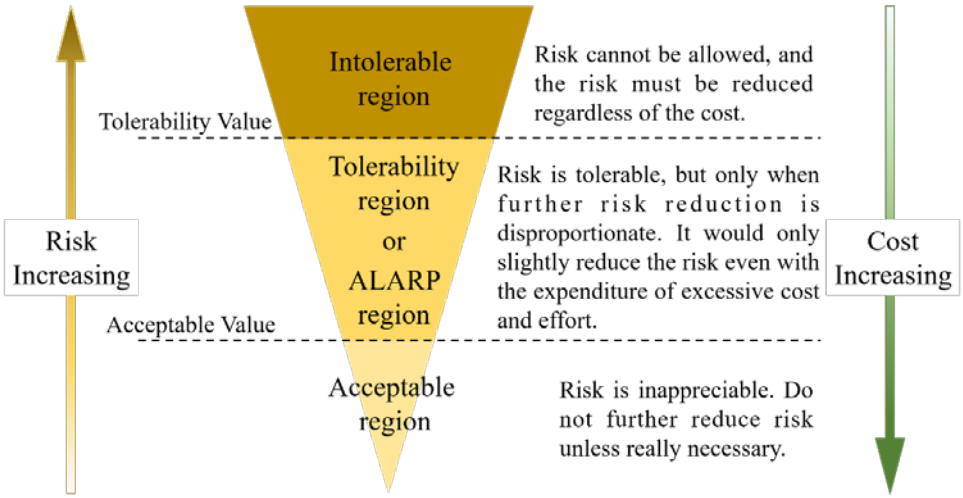


Fig. 2. Levels of risk and the ALARP principle.

falls below a certain threshold, the required costs to reduce the risk to that level will substantially increase. Therefore, the main purpose of risk reduction is to reduce risk to a reasonable allowable threshold and cost, which are determined by risk assessment or specifications.

It is noteworthy that risk reduction methods in HRI can be considered two different kinds of approaches. One is to reduce the risk probability before hazards or collisions occur, and the other is to mitigate the severity when collisions are inescapable. They are so-called pre-collision and post-collision safety strategies, respectively.

**Safety-Related Parts of Control Systems: Functional Safety**

The safety-related parts of the control system (SRP/CS) on a robot can adequately regulate the risk to stay below a predefined safety level and maintain the robot in a protected status. The concept of functional safety is, therefore, presented to ensure that the SRP/CS can be correctly executed. In other words, functional safety provides a guide for evaluating and classifying the ability of the SRP/CS to perform safety functions and, thus, represents the performance and reliability levels of the mechanical safety functions.

Generally, the types of SRP/CS are divided into two categories. The common and complex type is

composed of electrical/electronic/programmable electronic (E/E/PE) safety-related systems, and the other is mechanical safety protection devices, including hydraulic or pneumatic components. In an effort to validate and regulate SRP/CS, the IEC and ISO released the most commonly used international standards, IEC 61508 (IEC, 2010) and ISO 13849-1 (ISO, 2015), respectively, where IEC 61508 is specifically concerned with E/E/PE safety-related systems.

*(1) IEC 61508*

The process of analysis and evaluation of functional safety can be roughly divided into three steps. First, identify and analyze all the risks and hazards of faults in the system. Second, based on the identified results, specify the required safety integrity level (SIL) for functional safety. Finally, according to the overall failure rate of the SRP/CS, validate whether the required SIL meets the specifications.

*(2) ISO 13849-1*

As noted, IEC 61508, or IEC 62061 (IEC, 2005), is a validation guideline for E/E/PE safety-related function assessments. It is mainly applicable to the evaluation of complex electronic systems. On the other hand, ISO 13849 is focused on the analysis of the structure of control circuits, which includes not only the analysis of electrical and electronic systems but also that of hydraulic and pneumatic components.

Although both IEC 62061 and ISO 13849 guidelines are applicable to functional safety validation in the mechanical field, the difference in scope is still obvious. IEC 62061 is apt to have a greater degree of complexity because of the safety-related control elements that are composed of integrated circuits and software. Whereas ISO 13849 is suitable for applications with less complexity, such as simple control equipment systems composed of breakers, contactors, relays, positional limit switches, buttons, emergency stop buttons, and so on.

In terms of functional safety validation, ISO 13849, similar to IEC 62061, requires an evaluation to specify the appropriate level of functional safety. ISO 13849 calls the functional safety level the performance level (PL), which is further subclassified into five different levels labeled from a to e, in alphabetical order. The required performance level (PLr) can be determined using the assessment shown in Fig. 3. The higher the alphabetical label, the greater the indicated risk, which requires a higher level of functional safety.

The compliance of actual PL to PLr in the verification system is determined by the considerations of the system behavior for categories (Category), mean time to dangerous failure ($MTTF_d$), diagnostic coverage (DC) and common cause failures (CCF). The possible combinations for achieving the PL are indicated in Fig. 4, and the acquired PL value can be checked to determine if it meets the requirements for PLr. Category means the different requirements and structures of the loops of safety function, which can be classified into five categories, Category B and Category 1 through Category 4. Category B contains the most basic requirements, and Category 4 holds the most stringent requirements. In addition, Category 3 and Category 4 both require a dual loop structure for the safety function to ensure that the failure of a single component in one loop does not invalidate the entire signifies the ability of the control system of diagnose dangerous failures, and it is divided into the four

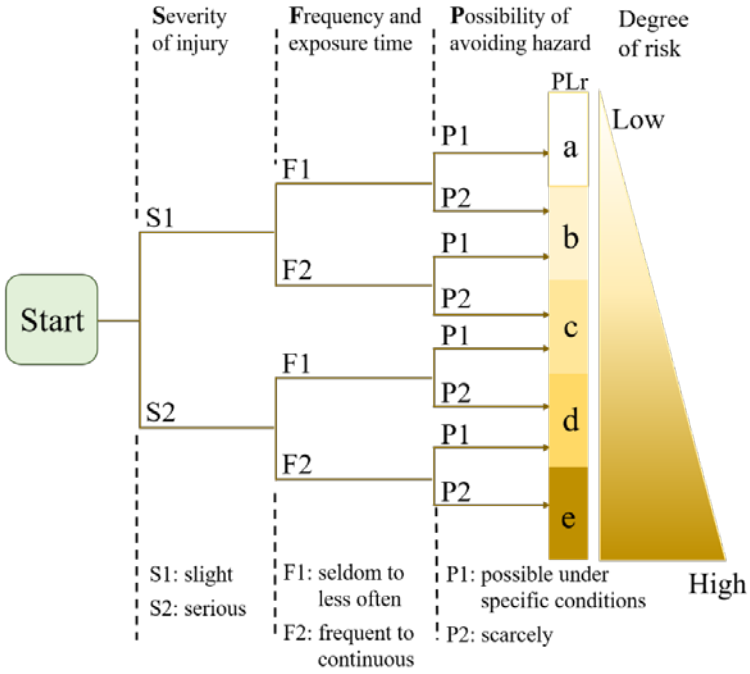


Fig. 3. Classification process diagram of PLr. The classification conditions include severity of injury, frequency, length of exposure, and the possibility of avoiding the hazard.

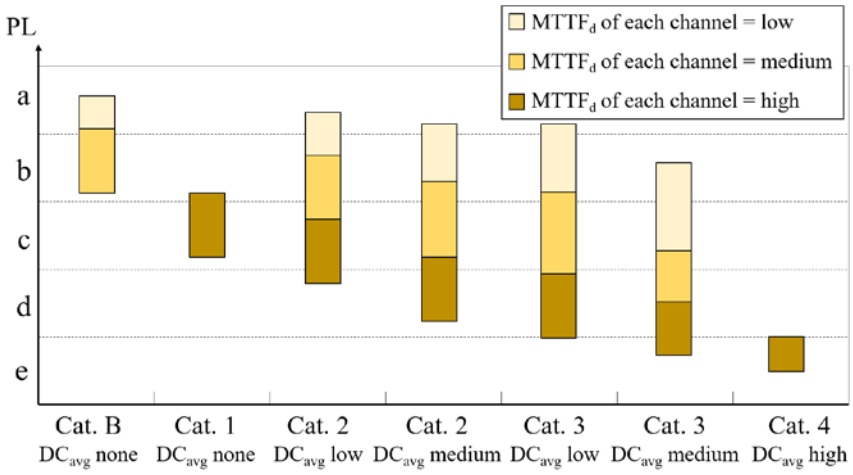


Fig. 4. Relationships among the categories of DCavg, MTTFd of each channel, and PL. The columns represent the combinations of categories (including CCF) and the average of the DCs (DCavg). In each column, the corresponding PL can be acquired by the different MTTFd of each channel, which means the safety function loop.

grades of none, low, medium, or high. The CCF gives a kind of evaluation score by quantifying the CCF using the evaluation table in Appendix F of ISO 13849-1. It essentially means that failure is caused by several different individual failures where each failure has no causal relationship with any other.

## INDUSTRIAL ROBOT AND ROBOTIC DEVICE SAFETY REQUIREMENTS

Due to the characteristics of stability, precision, and agility, industrial robots are widely applied to the field of industrial production. Taking the safety designs, installation requirements, and safety assessment standards into consideration, safety guidelines for industrial robots were developed and proposed in 2011 with ISO 10218. The frameworks of the guidelines consist of two parts, ISO 10218-1 and ISO 10218-2. Part 1 is the safety requirements for industrial robots and the safety measures for the integration of industrial robots, and industrial robotic systems are defined in part 2. The requirements to eliminate or adequately reduce the risks associated with robots are also described and recommended in this standard.

However, there may be an attendant greater potential risk to human operators due to the closer proximity in the workspace of robots and human operators such that the previously mentioned ISO 10218 guidelines become insufficient to ensure the safety of both humans and robots while performing collaborative operations.

Therefore, ISO defined collaborative workspaces and collaborative operations in the latest version of ISO 10218-1, which proposes four operating methods to complement the safety requirements of HRC. Further, the ISO/TS 15066 technical standard was established in 2016 to elaborate on the concept, terminology, and functional safety requirements of collaborative robots. Additionally, the technical supplementation for industrial robots in ISO/TS 15066 specifies that the basic safety requirements of collaborative robots (i.e., risk assessment and safety designs or construction) shall also meet the requirements of both ISO 10218-1 and ISO 10218-2. Four types of HRC operations will be further introduced and explored below.

### Four Modes of Human–Robot Collaborative Operation

Four modes of HRC operations and their corresponding safety measures are described in Fig. 5. To achieve safety guidelines, industrial robots are required to use at least one of the modes while operating in the HRC environment, in accordance with ISO 15066 guidelines. In fact, a certain degree of collaboration can be achieved through simple retrofitting modifications of current industrial robots. For example, the safety-rated monitored stop mode takes advantages of visual or optical proximity sensor technology to trigger the protective stop action of robots.

*(1) Safety-rated monitored stop*

The first mode is a safety-rated monitored stop, as shown in Fig. 5(a). This is the most traditional and pragmatic way because a standstill of the robot is required whenever an operator enters the collaborative workspace. The most common implementation of this mode is to remove the fences and to define the safety range of a collaborative workspace by the means of visual or optical sensing technology.

*(2) Hand guiding*

Hand guiding is another common implementation in collaborative operations, where

human operators guide the actions or movements of robots in the collaborative workspace through teaching pendants or bare hands. Robots keep in the safety-rated monitored stop mode in front of any human operators entering the workspace.

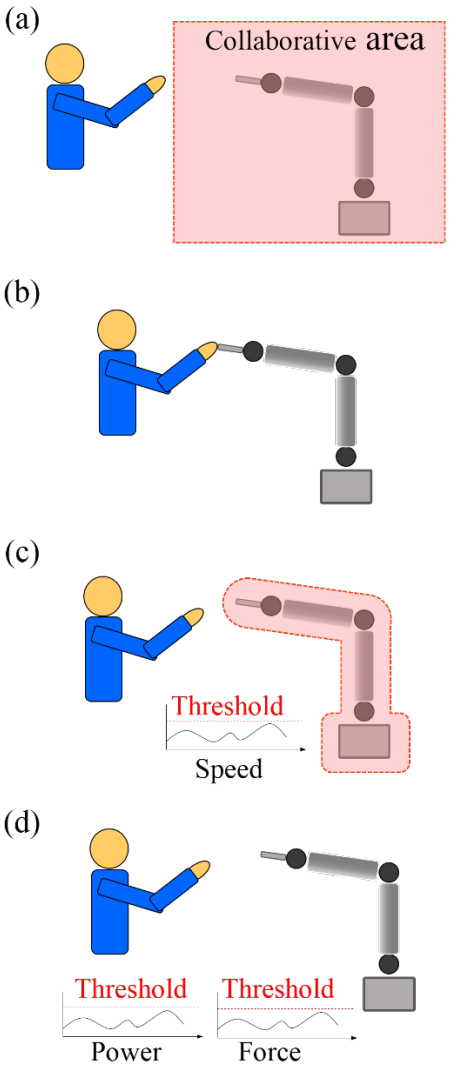


Fig. 5. Four modes of HRC operation. (a) Safety-rated monitored stop; (b) hand guiding; (c) speed and separation monitoring; and (d) power and force limiting by inherent design or control.

When encountering hazards, manipulators should stop immediately unless robots are under safety supervision status. In this case, robots will usually be equipped with post-collision protective measures when unexpected actions by robots result in collisions with an object.

*(3) Speed and separation monitoring*

The safety-rated monitored stop mode can be further controlled and designed to include a speed and separation monitoring mode in collaborative operations. Robots and human operators can perform tasks concurrently in a collaborative operating space. In this mode, the moving distance and speed between robots and human operators will be continuously monitored to ensure a minimum safe distance is kept. When the distance is approaching the lower limit of a threshold, the risk reduction safety operation should be immediately triggered until a safe distance is again achieved. The safety threshold is correlated to the moving speed of the robot such that a decrease in the moving speed of a robot results in a corresponding decreasing safety distance.

In this mode, two safety measures are introduced to reduce the risks. One is to reduce the robot's speed and keep the required distance greater than the threshold. The other alternative is to modify the original path of the robot within the safety distance. These two measures can be implemented separately or concurrently to ensure the safety of a collaboration. When the actual distance achieves or exceeds the minimum safety distance, the robot can resume normal operating status.

*(4) Power and force limiting by inherent design or control*

This mode is to protect human operators by the safety designs for injuries or hazards when a collision has occurred.

Physical contact of a human body with moving components of a robot can be classified as either quasi-static contact or transient contact. In this mode, the power and force must be lower than the value that can cause injury or hazard to the human body, bearing in mind that different areas of contact on the human body can lead to different levels of tolerable contact force. The force limit values for different parts of the human body are recommended in the ISO 15066 guidelines.

## RISK AND DANGER CONTROL FOR SPEED AND SEPARATION MONITORING

As previously mentioned, dynamic and real-time monitoring of the distance between human operators and a robot within the safety threshold of the integrated robot system is required in a speed and separation monitoring collaboration mode. Referring to the method (Ikuta et al., 2003), we define the hazard and risk as a function that can be transformed quantitatively to the danger index (DI) and the risk function (RF), respectively. A strategy for the safety control of pre-collision is then established. Parameters such as distance or the mental status of the user can be grouped and selected to perform the DI and RF analysis in accordance with the purpose of the system's use.

In this article, a pre-collision safety strategy is proposed based on the shortest distance between human operators and robots. The strategy is divided

into two steps. The first step is to decrease the operating speed of the robot while a human operator is approaching. The second step is to modify the original trajectory of the robot to avoid a collision when a human operator is very close to the robot. This safety strategy is depicted in Fig. 6. When a human operator enters the blue area, the controller will adjust the weight $K_{qd}$ to slow the speed of the robot according to the DI as

$$v_{command} = K_{qd} \cdot v_{original}, \quad (1)$$

where $v_{command}$ means the output speed of the robot, $K_{qd}$ is the control weight, and $v_{original}$ means the original control speed of the robot. Further, $K_{qd}$ is regarded as a sigmoid function, and $K_{qd}$ decreases when the DI increases, as shown in

$$K_{qd} = 1 - K_r\left(1 - \frac{1}{1+e^{\alpha(2\mathrm{DI}-1)}}\right), \quad (2)$$

where α is a function adjustment parameter, $K_r$ whose value from 0 to 1 represents the maximum value of the velocity adjustment ratio; and DI is the danger index.

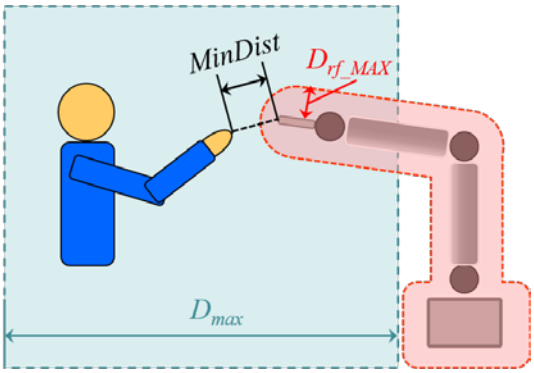


Fig. 6. Scheme diagram of the proposed pre-collision safety strategy. $D_{rf\_MAX}$ is the distance used to build the red area in which the robot can generate the virtual force. *MinDist* is the minimum distance between the human and the robot. $D_{max}$ is the distance used to construct the blue area, where the robot begins to slow down.

When DI is closer to 1, the value of $K_{qd}$ will be approximately close to 1-$K_r$. When the DI is close to 0, $K_{qd}$ will approach 1, indicating that the robot will perform the task in its original state. DI can indicate the severity of a hazard such that the closer a human operator is to a robot, the higher the DI value is. The DI calculation can be shown as

$$\mathrm{DI} = \begin{cases} 1, & MinDist \le D_{\min} \\ \dfrac{D_{\max} - MinDist}{D_{\max} - D_{\min}}, & D_{\min} < MinDist \le D_{\max} \\ 0, & MinDist > D_{\max} \end{cases}, \quad (3)$$

$$MinDist = \min\left\{\left\| p^H - p^R \right\|\right\} \quad (4)$$

where $D_{max}$ represents the distance at which the robot begins to slow down, $D_{min}$ shows the distance that makes the DI its maximum, and *MinDist* means the minimum distance between the two points $p^H$ and $p^R$, which represent the human and the robot, respectively.

When the robot starts to decrease operating speed, the human operator is still approaching, and the robot should then properly modify its original trajectory in order to avoid collisions. Referring to the method of virtual impedance control in a risk space (Lo et al., 2016; Wang et al., 2017), a simple safety strategy for modifying the trajectory is developed in this paper. The basic principle of this strategy is to establish a safe area surrounding the robot, as shown by the red area in Fig. 6. When a human operator enters the red area, a virtual force will be generated to push the robot away from the original trajectory to avoid collisions. The robot will be rebounded back and continue the task once the human operator leaves the area. First, the RF, $R_+$, is formulated using the *MinDist* as

$$R_+ = \left(\frac{D_{rf\_MAX} - MinDist}{D_{rf\_MAX}}\right)^3, \text{ if } D_{rf\_MAX} \ge MinDist, \quad (5)$$

where $D_{rf\_MAX}$ stands for the distance at which a virtual force is initiated. When the *MinDist* is less than $D_{rf\_MAX}$, $R_+$ is calculated and deployed to the risk space. The risk space can be defined as the span of RF. $R_+$ is regarded as twice continuously differentiable with respect to time. Then

$$\dot{R}_+ = J\dot{q}, \quad (6)$$

$$\ddot{R}_+ = J\ddot{q} + \dot{J}\dot{q}, \quad (7)$$

where $\dot{R}_+$ and $\ddot{R}_+$ represent the velocity and acceleration, respectively, in the risk space. $J$ and $\dot{J}$ are the Jacobian matrix and the derivative of the Jacobian matrix, respectively, between the risk space and the joint space. $\dot{q}$ and $\ddot{q}$ are the joint velocity vector and the joint acceleration vector of the robot. As a result, virtual impedance control is designed and formulated as

$$\ddot{R}_+ = -b_r\dot{R}_+ - k_r R_+, \quad (8)$$

where $k_r$ and $b_r$ as positive scalar parameters represent the stiffness and damping values, respectively. A virtual force, $\ddot{q}_r$, will then be derived from Eq. (6) to Eq. (8) as

$$\ddot{q}_r = -J^+(k_r R_+ + \dot{J}\dot{q}) - b_r\dot{q}, \quad (9)$$

where $J^+$ means the pseudo inverse of $J$. Once a virtual force is generated, the robot is immediately enabled to escape from the original trajectory to avoid collisions, and it tries to keep a safe distance. The detailed mathematical derivations can be referred to in a previous publication (Lo et al., 2016).

## EXPERIMENTS AND VALIDATIONS

### Experiments

In this section, we describe an experiment that

was performed to verify the proposed control measures on a robot's distance and speed, as discussed in this article. A Kinect sensor was applied as a tool for retrieving environmental information and was installed on the front of a robot equipped with a six-axis manipulator, as illustrated in Fig. 7. Snapshots of the experiment are provided in Fig. 8. At the beginning, the manipulator is performing the movements in three consecutive points. Firstly, the human operator approaches the manipulator gradually and then tries to physically touch the manipulator. Finally, the human operator moves away from the manipulator.

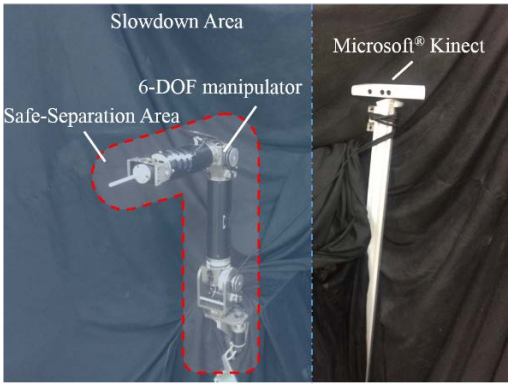


Fig. 7. Experimental environment setup. Blue and red areas enclosed by blue and red dotted lines show the slowdown and safe separation areas, respectively.

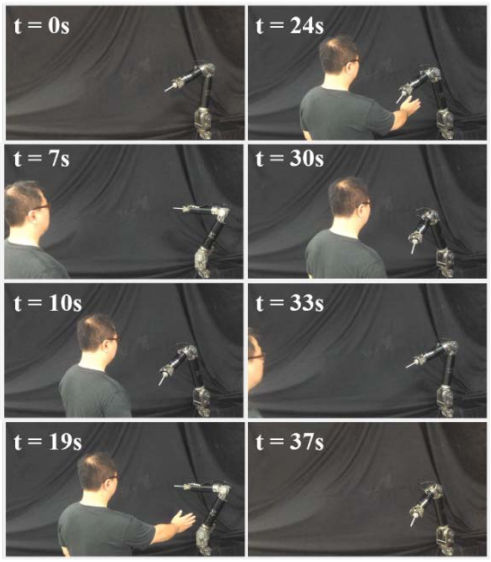


Fig. 8. Snapshots of the experiment during repeated execution of a three-point movement task making the robot simultaneously avoid collisions with the human. The first point is at 0 s, the second point is at 7 s, and the third point is at 10 s.

In the experiment, $D_{max}$, $D_{min}$, and $D_{rf\_MAX}$ were set as 1.5 m, 0.1 m, and 0.2 m, respectively. The result of *MinDist* is shown in Fig. 9, where it can be seen that the *MinDist* gets smaller while the human operator is approaching the robot. The line accompanied by a small wave curve resulted from natural swings of the hand. When the *MinDist* is less than 1.5 m, the control strategy slows the speed of the robot in the slowdown area. Further, when the *MinDist* is less than 0.2 m, the control strategy generates the virtual force to modify the motion of the robot into a safe separation area. Thus, the proposed strategy presented good performance in the HRC, where the minimum distance between the human and robot could still be kept over 0.15 m through the protective collision-avoidance action, even when the operator intends to continuously approach the robot.

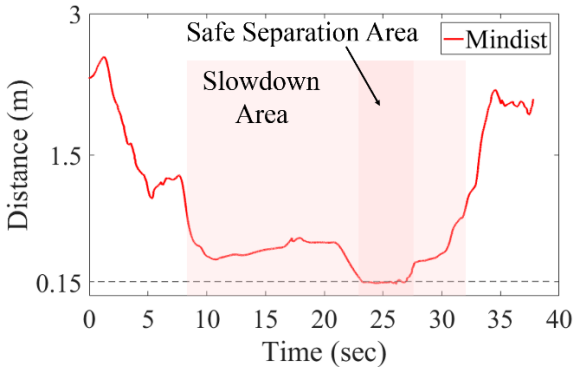


Fig. 9. The minimum distance between human and the manipulator. The light red area shows the slowdown area, and the deeper red area is the safe separation area.

According to Eq. (3), DI value increases while *MinDist* decreases to less than 1.5 m. Then the decrease in velocity adjustment parameter $K_{qd}$ calculated from Eq. (2) causes the $v_{command}$ of Eq. (1) to decrease gradually, and the joint velocity, $\dot{q}$, of each joint of the manipulator is simultaneously also obviously slowed, as indicated in Fig. 10(b) and Fig. 10(c), respectively. As shown in Fig. 10(a) and Fig. 10(b), the DI value is zero in the beginning, and the manipulator keeps the original speed for the task operation. Then DI over 0.3 at about 8.1 s resulted from the decrease of $K_{qd}$, obviously, and Fig. 10(b) shows that the value of $K_{qd}$ continues to decrease to 0.5 at 10.3 s. In the meantime, the speed of the manipulator is slowed to half the original speed, as shown in Fig. 10(c). In addition, Eq. (2) can also be drawn as Fig. 11, with $K_r = 0.5$ and $\alpha = 12.5$, respectively, in this experiment, and we can see that $K_{qd}$ is very close to 1 when the DI is lower than 0.3. Once the human operator moves away from manipulator, the $K_{qd}$ returns to 1, and the speed of the manipulator is also returned to the original value (see the video in supplementary materials https://youtu.be/_xPC24MrU_E and Fig. 8).

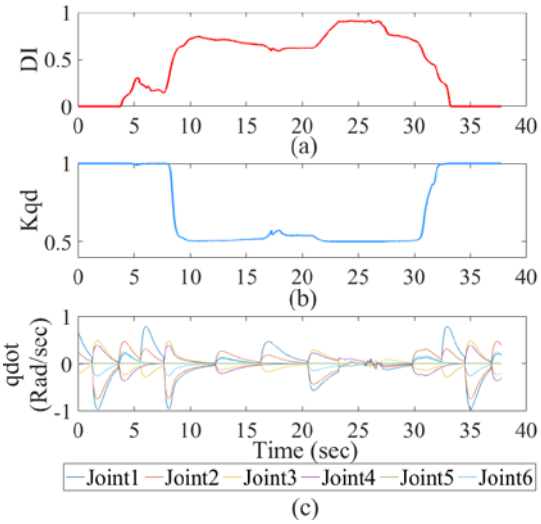


Fig. 10. Results of the experiment. (a) Danger index (DI), (b) $K_{qd}$, and (c) angular velocity ( $\dot{q}$ ) of each joint.

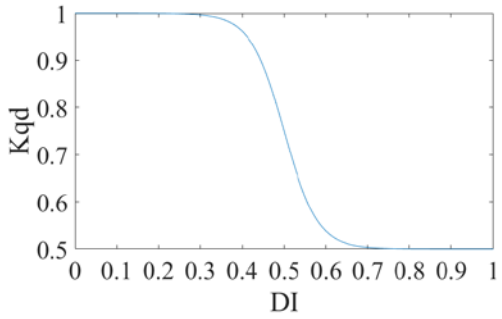


Fig. 11. The relationship between DI and $K_{qd}$.

When the *MinDist* value continues to decrease below $D_{rf\text{-}MAX}$, the $R_+$ is derived from Eq. (5); this area is also the safe separation area in Fig. 9. Fig. 12 shows the values of $R_+$ and $\ddot{q}_r$ corresponding to each joint generated from the controller by Eq. (5) and Eq. (9). In the safe separation area, the robot will give away the original task to keep the desired safe distance.

**Validation**

The results of the experiment indicate that the proposed strategy can slow the robot to half its original speed when a human approaches. Once the *MinDist* is under the desired safety threshold, the original trajectory of the robot can be modified further to avoid the human body, and the *MinDist* is always kept over 0.15 m. Once the human moves away from the robot, the trajectory of the robot is automatically recovered. These behaviors validate the proposed strategy as being able to meet the requirements of the speed and separation monitoring mode in ISO 15066 for HRC.

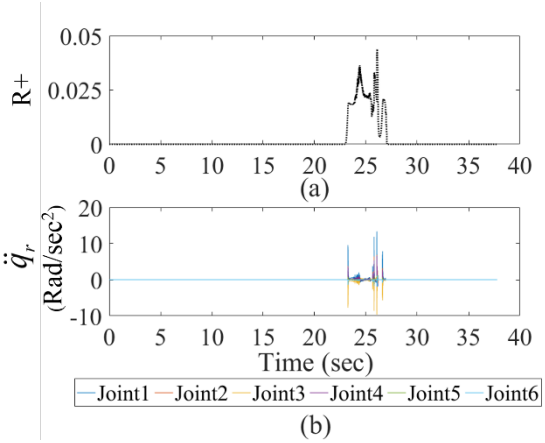


Fig. 12. Results of the experiment in the safe separation area. (a) the value of $R_+$ and (b) the value of $\ddot{q}_r$ .

We used the safety integrity software tool SISTEMA, which was developed by the German Institute for Occupational Safety and Health, to validate our designed safety function. We adopted Category 3 in the loop structure of our safety function, which includes two modules, the emergency stop button and the proposed speed and separation monitoring with safe torque OFF module, as shown in Fig. 13. In terms of hardware, a XW1E-BV401MFR manufactured by IDEC was used for the emergency stop button, and iPOS4808 controllers developed by TECHNOSOFT were used to control the motors of our robot. After inputting the relevant failure rate parameters, the related safety parameters of this system can be calculated. $MTTF_d$ was up to 100 years, DC was 95% (medium), CCF was 85, and PFHD was 6.2E-8[1/hour]. These results ensure that our designed safety function can meet PL e in ISO 13849 and this was validated by SISTEMA, as shown in Fig. 14.

## CONCLUSIONS

In this article, the frameworks and core concepts of international standards were comprehensively reviewed and elaborated upon, including the concepts of risk management and the procedures and methods for functional safety assessments. Furthermore, the safety requirements of four types of HRC in the ISO 15066 guideline were also summarized.

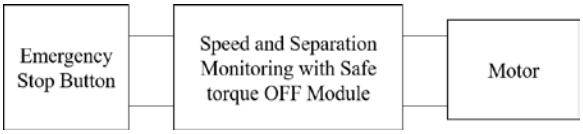


Fig. 13. Loop structure of our safety function.

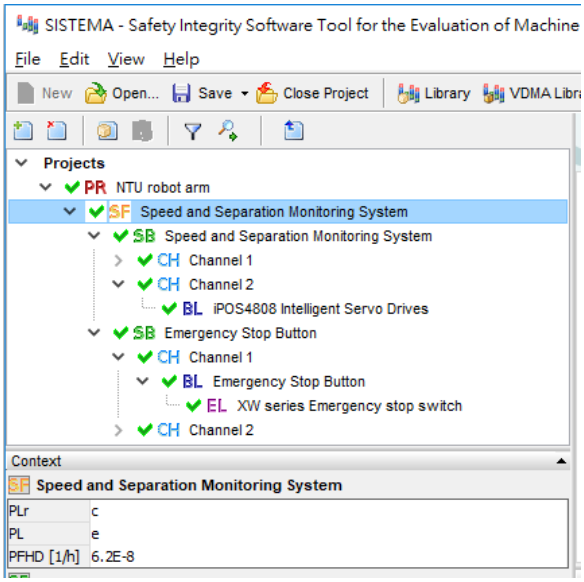


Fig. 14. The validation results by SISTEMA

Then we proposed a pre-collision safety strategy to easily integrate speed adjustment and trajectory modification during movements to meet the speed and separation monitoring mode introduced in ISO 15066. The experimental results showed that the control strategy decreased the speed of a robot to effectively avoid collisions when a human operator tried to physically make contact with a robot. Consequently, the controlled distance between a human operator and a robot within the safety threshold is achievable, and the proposed strategy meets the requirements of ISO 15066. Further, this solution can be easily implemented in all kinds of robotic systems with only one low-cost external sensor without the need to modify the robot at all. In addition, our designed safety function is also validated to meet PL e of ISO 13849.

## REFERENCES


Flacco, F., Kröger, T., De Luca, A., and Khatib, O., "A depth space approach to human-robot collision avoidance," Proceeding of IEEE International Conference on Robotics and Automation, pp. 338–345 (2012).

Golz, S., Osendorfer, C., and Haddadin, S., "Using tactile sensation for learning contact knowledge: Discriminate collision from physical interaction," Proceeding of IEEE International Conference on Robotics and Automation, pp. 3788–3794 (2015).

Goodrich, M. A. and Schultz, A. C., "Human-robot interaction: A survey," *Foundations and Trends® in Human-Computer Interaction*, Vol. 1, No. 3, pp. 203–275, (2008).

Huang, M.-B. and Huang H.-P., "Innovative human-like dual robotic hand mechatronic design and its chess-playing experiment," *IEEE Access*, Vol. 7, No. 1, pp. 7872–7888 (2019).

IEC, "Functional safety of electrical/electronic/ programmable electronic safety-related systems – Part 1: General requirements," IEC 61508-1 (2010).

IEC, "Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems," IEC 62061 (2005).

Ikuta, K., Ishii, H., and Nokata, M., "Safety evaluation method of design and control for human-care robots," *The International Journal of Robotics Research*, Vol. 22, No. 5, pp. 281–297 (2003).

ISO, "Robots and robotic devices – Safety requirements for industrial robots – Part 1: Robots, International Organization for Standardization," ISO 10218-1 (2011).

ISO, "Robots and robotic devices – Safety requirements for industrial robots – Part 2: Robot systems and integration, International Organization for Standardization," ISO 10218-2 (2011).

ISO, "Safety of machinery – General principles for design – Risk assessment and risk reduction," ISO 12100 (2010).

ISO, "Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design," ISO 13849-1 (2015).

ISO/IEC, "Safety aspects – Guidelines for their inclusion in standards," ISO/IEC Guide 51 (2014).

ISO/TS, "Robots and robotic devices – Collaborative robots, International Organization for Standardization," ISO/TS 15066 (2016).

Khatib, O., "Real-time obstacle avoidance for manipulators and mobile robots," Proceeding of IEEE International Conference on Robotics and Automation, St. Louis, MO, USA, pp. 500–505 (1985).

Krüger, J., Lien, T. K., and Verl, A., "Cooperation of human and machines in assembly lines," *CIRP Annals – Manufacturing Technology*, Vol. 58, No. 2, pp. 628–646 (2009).

Kulić, D. and Croft, E., "Pre-collision safety strategies for human-robot interaction," *Autonomous Robots*, Vol. 22, No. 2, pp. 149–164 (2007).

Lacevic, B. and Rocco, P., "Kinetostatic danger field – a novel safety assessment for human–robot interaction," Proceeding of IEEE/RSJ International Conference on Intelligent Robots and Systems, Taipei, Taiwan, pp. 2169–2174 (2010).

Lasota, P. A., Fong, T., and Shah, J. A., "A survey of methods for safe human–robot interaction," *Foundations and Trends in Robotics*, Vol. 5, No. 3, pp. 261–349 (2017).

Lo, S.-Y., Cheng, C.-A., and Huang, H.-P., "Virtual

impedance control for safe human–robot interaction," *Journal of Intelligent Robotic Systems*, Vol. 82, No. 1, pp. 3–19 (2016).

Moon, S., Rhim, S., Cho, Y.-J., Park, K.-H., and Virk, G. S., "Summary of recent standardization activities in the field of robotics," *Robotica*, Vol. 31, No. 2, pp. 217–224 (2013).

Vanderborght, B., Albu-Schaeffer, A., Bicchi, A., Burdet, E., Caldwell, D. G., Carloni, R., Catalano, M., Eiberger, O., Friedl, W., Ganesh, G., Garabini, M., Grebenstein, M., Grioli, G., Haddadin, S., Hoppner, H., Jafari, A., Laffranchi, M., Lefeber, D., Petit, F., Stramigioli, S., Tsagarakis, N., Van Damme, M., Van Ham, R., Visser, L. C., Wolf, S., "Variable impedance actuators: A review," *Robotics and Autonomous Systems*, Vol. 61, No. 12, pp. 1601–1614 (2013).

Villani, V., Pini, F., Leali, F., and Secchi, C., "Survey on human–robot collaboration in industrial settings: Safety, intuitive interfaces and applications," *Mechatronics*, Vol. 55, pp. 248-266 (2018).

Wang, X. V., Kemény, Z., Váncza, J., and Wang, L., "Human–robot collaborative assembly in cyber-physical production: Classification framework and implementation," *CIRP Annals – Manufacturing Technology*, Vol. 66, No. 1, pp. 5–8 (2017).

Yamada, Y., Hirasawa, Y., Huang, S., Umetani, Y., and Suita, K., "Human–robot contact in the safeguarding space," *IEEE/ASME Transactions on Mechatronics*, Vol. 2, No. 4, pp. 230–236 (1997).

## NOMENCLATURE

| | |
|---|---|
| $b_r$ | damping value |
| $D_{\max}$ | the distance at which the robot begins to slow down |
| $D_{\min}$ | the distance that makes the DI its maximum |
| $D_{rf\_MAX}$ | the distance at which a virtual force is initiated |
| DI | danger index |
| $J$ | the Jacobian matrix between the risk space and the joint space |
| $J^+$ | the pseudo inverse of $J$ |
| $\dot{J}$ | the first order derivative of $J$ |
| $K_{qd}$ | the control weight of the original control speed of the robot |
| $k_r$ | stiffness value |
| $K_r$ | the maximum value of the velocity adjustment ratio |
| *MinDist* | the minimum distance between the two points $p^H$ and $p^R$ |
| $p^H$ | one point of the human |
| $p^R$ | one point of the robot |
| $\dot{q}$ | the joint velocity vector of the robot |
| $\ddot{q}$ | the joint acceleration vector of the robot |
| $\ddot{q}_r$ | virtual force |
| $R_+$ | risk function |
| $\dot{R}_+$ | the first order derivative of $R_+$ |
| $\ddot{R}_+$ | the second order derivative of $R_+$ |
| $v_{command}$ | the output speed of the robot |
| $v_{original}$ | the original control speed of the robot |
| $\alpha$ | the adjustment parameter of sigmoid function |

# 人機交互安全：基於機器人相關標準的概念與實現

丁相元　許煥坤　黃明寶　黃漢邦
國立台灣大學機械工程學系

## 摘 要

本研究詳述了機器人安全標準的核心概念，並以此探討整合速度調節與軌跡修正的碰撞前安全策略。本研究使用 Kinect 估計人和機器人間的距離，依據距離減緩機器人運行速度或以虛擬排斥力調整機器人軌跡，提出基於風險評估及速度調節的安全策略。經實驗證實本研究提出的安全策略除了符合 ISO15066 的要求，在安全功能驗證方面亦達到 ISO13849 的性能水平 e。