CIGI QUALITA MOSIM 2023
Revealing the importance of estimating required reliability levels in cobotics safety

SABRINA JOCELYN[1], DAMIEN BURLET-VIENNEY[1], SEYED HOSSEIN HAJ ZARGARBASHI[2], CHANTAL GAUVIN[1], BERTRAND GALY[1], CHUN HONG LAW[1]

[1] INSTITUT DE RECHERCHE ROBERT-SAUVÉ EN SANTÉ ET EN SÉCURITÉ DU TRAVAIL (IRSST)
505 De Maisonneuve Blvd. West, Montreal, Quebec H3A 3C2, Canada
sabrina.jocelyn@irsst.qc.ca

[2] AEROSPACE MANUFACTURING TECHNOLOGIES CENTRE, NATIONAL RESEARCH COUNCIL CANADA (NRC)
2107 Chemin de Polytechnique, Montreal (Quebec), QC H3T 1J4, Canada
Seyedhossein.Hajzargarbashi@cnrc-nrc.gc.ca

***Résumé* – L'estimation du niveau de fiabilité requis d'une fonction de sécurité est une étape essentielle lorsque la réduction d'un risque est basée sur le système de commande d'une machine. Le "niveau de performance (PL)" de la norme ISO 13849 ou le "niveau d'intégrité de sécurité (SIL)" de la norme CEI 62061 sont des termes normatifs traduisant ce niveau de fiabilité. Plus le niveau de risque est élevé, plus le niveau de fiabilité requis le sera. Les systèmes de fabrication agile, comme les applications collaboratives, sont particulièrement concernés par cette problématique. En comparant les résultats de deux études en cobotique, cet article montre comment l'estimation du PL ou du SIL requis guide le choix des composants de sécurité externes responsables du déclenchement d'actions sécuritaires du robot (ex., arrêt du robot). Cette comparaison met également en évidence l'importance d'estimer le PL ou le SIL requis par une évaluation complète des risques de l'application collaborative afin de déterminer si l'automate dédié à la sécurité du robot dispose des spécifications nécessaires pour respecter le niveau de fiabilité requis. Dans le cas contraire, des mesures supplémentaires sont nécessaires pour atteindre un niveau de risque acceptable.**

***Abstract* – Estimating the required reliability level of a safety function is an essential step when risk reduction is based on a machine's control system. That reliability level is reflected in the terms "Performance Level (PL)" in ISO 13849 and "Safety Integrity Level (SIL)" in IEC 62061. The higher the risk level, the higher the level of reliability required. Agile manufacturing systems, such as collaborative applications, are particularly affected by this issue. By comparing the results of two studies in cobotics, this paper shows how the estimation of the required PL or SIL guides the choice of external safety components responsible for triggering the robot's safety actions (e.g., stopping the robot). This comparison also highlights the importance of estimating the required PL or SIL through a comprehensive risk assessment of the collaborative application to determine whether the robot's safety-related Programmable Logic Controller (PLC) has the necessary specifications to meet the required reliability level. If not, additional measures are needed to achieve an acceptable level of risk.**

***Mots clés* – Robotique collaborative, fonction de sécurité, niveau de performance, sécurité des machines.**
***Keywords* – Collaborative robotics, Safety function, Performance level, Safety of machinery.**

1 INTRODUCTION

Considered as one of the levers of Industry 4.0, due to the flexibility they can add, so-called collaborative robots (cobots) have spread since they appeared in industry around 2010 [Fryman et al., 2012]. The market share of cobots grew steadily from 2017 to 2021 [IFR, 2022], and industry watchers believe "[t]he period out to 2026 will see further strong expansion in sales" [Xiao, 2022]. With this forecast expansion, the availability of safety modules allowing conventional robots to be used for collaboration with humans and because cobotics relies heavily on safety functions (SF) to protect people in their surroundings, integrators should make sure each SF provides the required risk reduction to prevent accidents. An SF is a "function of a machine whose failure can result in an immediate increase of the risk(s)" [ISO, 2010] (e.g. Figure 1).

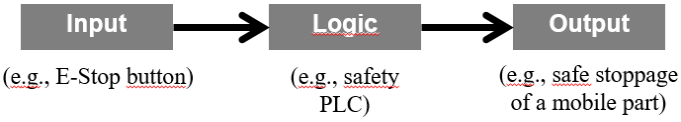


Figure 1. General structure of a safety function (E-Stop: Emergency stop; PLC: Programmable Logic Controller)

An emergency stop function is an example of a safety function. If an SF cannot reduce the risk as it should, supplementary measures should be used to manage that lack of risk control.

Relying on two research studies, this paper underscores the importance of estimating the reliability level required for safety functions in human-robot collaboration. In Industry 4.0, people seek flexibility in an agile (constantly changing) manufacturing system. It is therefore of the utmost importance to know the required reliability level of a safety function after a change. Monitoring the required reliability level, which is a complex task, will help verify whether the reliability level after the change still complies with the new required reliability level. Estimating the required reliability level is important to make sure the combination of components chosen to achieve the safety function maintains or surpasses this required level.

The paper highlights the aspects of a cobotic integration process that require vigilance to ensure reliable safety functions. These aspects were extracted from six industrial case studies that explored how four integrators from different companies considered safety in the design of collaborative

applications. The critical aspect of the checkpoints is explained through the integration of a collaborative application in a research laboratory. A collaborative application is a process comprising at least "a portion of the robot sequence where both the robot application and operator are within the same safeguarded space" [ISO, 2022].

Section 2 of this paper presents the evidence supporting the research by showing the key importance of safety functions in collaborative applications and the lack of cobotics studies focusing on the implementation of safety functions through an integration process. Section 3 sets out the methodology applied to achieve the research objective. Section 4 presents the main results. In section 5, they are discussed in a comparison of the companies on the field and the research laboratory. Section 6 concludes the paper.

2 RATIONALE

2.1 Reliable safety functions are crucial in cobotics

Risk is the combination of the severity of harm and the probability of that harm [ISO, 2010]. To reduce the risk, one must act upon the severity or the probability of the harm. After inherently safe design measures, such as the round shapes of a cobot, safety functions represent the main risk reduction measures to ensure an operator's safety in collaborative applications, since guards are often meant to be completely or partially absent. Thus, ISO 10218-1 [ISO, 2011a] prescribes four possible methods to control the risk associated with collaborative operations based mainly on the use of SFs. The technical specification ISO/TS 15066 [ISO, 2016] describes these methods in detail:

Method 1: Safety-rated monitored stop: if someone is detected in the collaborative workspace, the robot stops while remaining energized;

Method 2: Hand guiding: the operator uses a hand-operated device that sends his or her movement intention to the control system;

Method 3: Speed and separation monitoring: the robot avoids the operator by maintaining a certain speed and separation distance;

Method 4: Power and force limiting by inherent design (e.g., padded joints) or control (e.g., configuration of force limitation): the robot's kinetic energy is limited.

Two standards provide discrete levels to estimate the required reliability level of a safety function:

- The safety integrity level (SIL) in IEC 62061 [IEC, 2021]. Three discrete levels describe the SIL in machinery safety: SIL 1 for the lowest reliability to SIL 3 for the highest;
- The performance level (PL) in ISO 13849-1 [ISO, 2015]. Five discrete levels describe the PL: a, b, c, d and e, from least to most reliable.

SIL and PL are interchangeable using an equivalence chart available in the standards. A risk assessment allows one to estimate the required PL or SIL. Risk assessment is the iterative process starting with the determination of the limits of the machinery (i.e., mainly the use, space and time conditions associated with it), followed by hazard identification and risk estimation (i.e., attribution of risk indexes), and ending with risk evaluation (i.e., judgment of whether or not the estimated risk is acceptable). The safety functions designed for collaborative applications should comply with ISO 10218-1:2011, which requires a PL of d, category 3 (or cat. 3), unless the risk assessment has shown otherwise. The category is the "classification of the safety-related parts of a control system in respect of their resistance to faults and their subsequent behaviour in the fault condition, and which is achieved by the structural arrangement of the parts, fault detection and/or by their reliability" [ISO, 2015]. Five categories exist: B, 1, 2, 3 and 4, from the least to the most robust. The PL depends on the category, among other things.

When a collaborative application is to be implemented, the effective performance level of an SF should be greater than or equal to the required performance level (PL_r), allowing for the necessary risk reduction in the human-robot interaction (HRI). To meet that requirement, the components combined to form the SF must be chosen with care. Indeed, choosing a component with a PL lower than the required one increases the risk of injury and therefore means that further risk reduction measures must be added. Moreover, some characteristics, such as the components' response time are critical for safety, as Sghaier et al. [2015] explain.

2.2 Machinery-related accidents reveal the importance of reliable safety functions

An industrial robot by itself (cobot or conventional robot) is a partly completed machine [Directive 2006/42/EC]. When integrated with its robotic tool and into its auxiliary equipment, the whole becomes a machine. Consequently, the reliability of the equipment's SFs in its surroundings is also important. The literature reveals the need to prevent control system failures and faults by listing incidents or accidents related to them [Villard, 2003; Chinniah et al., 2019]. For example, 54 out of 144 accidents related to machine operation in Poland were found to be due to improper functioning of machine control systems (Dźwiarek, 2004). The 144 accidents represent a fraction of the 700 accidents from 1996 to 2002 related to various causes. The 54 accidents happened for different reasons:

- Lack of safety function (58%)
- Incorrect choice of the category of control system (26%)
- Error in controller software (6%)
- Devices not hardy enough for environmental impacts (6%)
- Incorrect definition of safety function (4%).

The 58% rate shows the importance of SFs in machinery-related accident prevention. Meanwhile, the 26% rate tells how crucial the choice of the correct category leading to the SF's performance level is, to contribute sufficiently to the required risk reduction. The right choice of category helps prevent the loss of an SF. That loss can result in a dangerous failure and, ultimately, in an accident.

In the case of collaborative applications where human and robot share the same workspace, possibly with auxiliary equipment as well, and where physical contact with the robot is possible at any time, reliable SFs are crucial. An occupational accident involving a cobot in a collaborative application happened at an aerospace company [Moulières-Seban, 2017]; however, the exact causes of the accident were not revealed. A boy suffered a finger fracture playing chess with a little industrial robot in a collaborative space [Henley, 2022] (the reference does not specify whether it was a cobot or a conventional robot); a software error was suspected, among other possible causes. Similar circumstances could arise in the workplace. Apart from those circumstantial events, no accidents associated with cobotics have been reported so far, to the best of the authors' knowledge. In the meantime, some authors [Malm et al., 2010; Charpentier & Sghaier, 2012] have

transposed conventional-robot-related accident analysis to the case of robots used in a collaborative application in order to anticipate the need for safety in that new field. For instance, most of the 25 severe robot-related accidents that happened in Finland from 1989 to 2006, involved the operator getting crushed by a solid object [Malm et al., 2010]. Those authors anticipated that the operator's proximity to the robot in the collaborative workspace would likely increase the risk of getting injured, by increasing the human's exposure and reducing the possibility of avoiding harm. These authors favour the use of safety devices to prevent human-robot collisions, which entails the need for reliable SFs applied to every safety device to achieve the risk reduction required. The three-dimensional movements of a robot combined with the unpredictability of human gestures make risk management particularly complex in the collaborative workspace. It is often necessary to combine several of the ISO 10218 methods listed in Section 2.1 to achieve an acceptable risk. Consequently, SFs must be implemented appropriately to achieve the reliability required in order to reduce risks adequately during HRIs.

2.3 Studies of integration in cobotics do not cover the implementation of safety functions

Some cobotics-related studies address the integration of collaborative applications. For example, Gopinath & Johansen [2016] propose a task-planning-based method to guide the risk assessment carried out at the beginning of the integration process. The main tasks and sub-tasks anticipated in the collaborative workspace are listed; then the hazards and risk factors for each sub-task are identified and estimated. Askarpour et al. [2017] suggest a non-deterministic framework revolving around the operator's behaviour. Their model allows one to identify hazardous situations created by human errors in the collaborative workspace. A hazardous situation is a "circumstance in which a person is exposed to at least one hazard" [ISO, 2010]. Gualtieri et al. [2022] propose some guidelines that enhance workstation features and interaction conditions to improve the operator's cognitive response to HRI as well as the assembly's performance. The strength of these studies is their consideration of the human operator in the risk analysis, task planning or activity analysis. However, they do not consider the implementation of SFs in cobotics.

3 METHODOLOGY

The methodology presented is twofold. Part 1 was an exploratory study undertaken in four different companies in Quebec (Canada) (Section 3.1). The majority of the companies contacted were part of a group of original equipment manufacturers in industrial automation (reai.ca/en/). The others were associated with a bipartite occupational health and safety association in the field of transportation equipment and machinery manufacturing (http://asfetm.com/). Part 2 was carried out in a robotics laboratory at the National Research Council Canada (NRC) (Section 3.2).

3.1 Interviews with four integrators about six collaborative applications

Six cases in four companies, coded A, B, C and D for confidentiality purposes, were visited. The team interviewed one integrator at each company, for two or three hours depending on the complexity of the application and their numbers. The four semi-structured interviews were guided by a data collection form, which questioned the integrators about:

- what collaborative application was integrated and why;
- the integration process in general:
  - the standards used,
  - the risk assessment procedure performed,
  - the estimation of the required performance level,
  - the safeguards used to protect workers interacting with the collaborative application,
  - the validation of the collaborative application;
- the consideration of production and safety requirements, as well as other requirements;
- the challenges faced.

In accordance with the aim of this paper, the results in Section 4 present only the information regarding the "integration process in general."

3.2 Integration of a collaborative application in NRC's laboratory

Industrial members of METALTec (a consortium funded by the NRC to support innovation in METAL product manufacturing Technologies) commissioned the NRC to develop and implement a TRL-5 (TRL: Technology Readiness Level) cyber-physical finishing cobotic platform providing a high interactivity level with the operator (Figure 2). Manual finishing tasks include polishing, sand blasting, edge breaking, grinding, deburring, etc. The main factors driving this METALTec project are: (1) the need to alleviate the musculoskeletal disorders the finishing operators had been experiencing; (2) the labour shortage and the decreasing interest in this type of manual operation; and (3) the flexibility required by low-volume high-mix productions necessitates keeping the operator in the loop. Since then, the NRC and its partners from different research centres have been integrating a platform to showcase a finishing collaborative application including a cobot. While the cobot performs a finishing task, the human operator supervises the process, controls the quality of the parts, and indicates through a gesture recognition system which production lot should start. As one of the NRC's research partners, the IRSST oversaw the occupational health and safety (OHS) aspects of the platform.

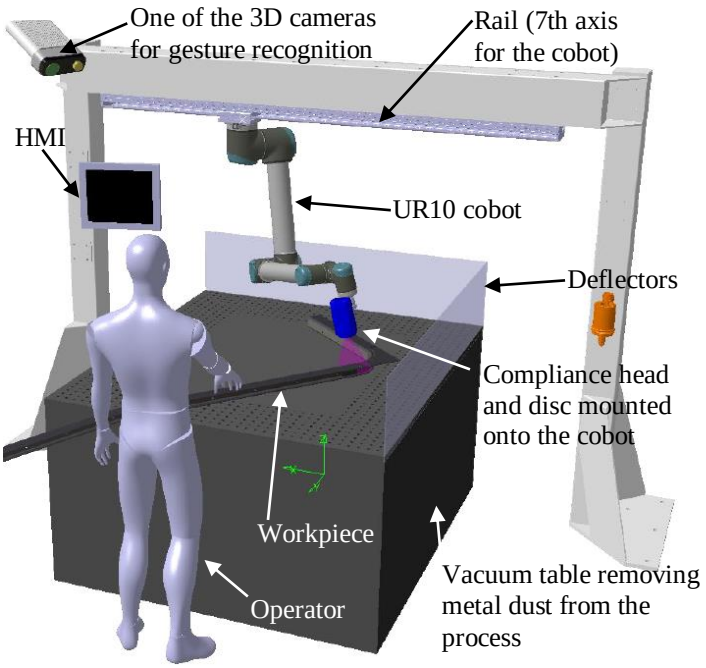


Figure 2. Sketch of the cobotic finishing platform

Collaborating with some NRC employees, the IRSST's team performed a risk assessment of the platform in order to support its integration and make sure its use remains safe. This is a continuing endeavour throughout the technological evolution

of the application until the TRL-5 platform is ready for transfer to the metal industry. The risk assessment applies a holistic approach: it takes into account not only the cobot but also the humans and auxiliary equipment in the vicinity, as well as the surrounding environment. For the risk assessment, the team allocated the risk indexes using the risk estimation tool available in the current confidential draft of ISO 10218-2 [ISO, 2022] and considering the worst and most probable harm associated with each hazardous situation identified. That estimation tool comprises five risk indexes obtained by combining the severity of harm and the qualitative probability of harm. A PL_r corresponds to each risk index (Table 1). The team chose this estimation tool over the ISO 13849-1:2015 PL_r estimation tool because it comprises more than two levels of severity of harm, unlike the ISO 13849-1 tool. That difference makes the next ISO 10218-2 tool less biased than ISO 13849-1:2015, considering the construction rules set out in an IRSST report [Chinniah et al., 2011].

Table 1. Correspondence between risk index and PL_r according to the risk estimation tool used for this project

Risk Index (1: lowest risk level; 5: highest risk level)	**Corresponding required Performance Level (PL_r)** (a: lowest PL_r, so lowest reliability needed; e: highest PL_r, so highest reliability needed)
1	**a**
2	**b**
3	**c**
4	**d**
5	**e**

Following the risk assessment, the team chose the risk reduction measures for the unacceptable risks, namely risk indexes 3 to 5. To do so, the team consulted finishing experts from two plants in the consortium. This consultation occurred at a virtual meeting, then at two on-site visits. The experts discussed the acceptability of the risks and the acceptance of some risk reduction measures to prevent the bypassing of safety measures. The experts' input was very helpful in decide which personal protective equipment (PPE) to choose. They also demonstrated some finishing processes so the team could have a better sense of the hazards in the workplace and verify what PPE would be most useful to protect operators.

The team chose risk reduction measures involving safety devices (e.g., sensitive skin, laser scanner, E-Stop button). Each safety device, as a component, triggers a safety function (Figure 1) such that their addition to the cobot safety PLC results in an overall performance level complying with the PL_r needed to mitigate the corresponding risk (i.e., verifying that the overall PL is $\geq PL_r$). Each component of the SF may have its own PL. Consequently, the SF's overall PL depends on the combination of PLs of each component achieving the safety function. Using Table 11 of ISO 13849-1:2015, the team was able to calculate the overall PL for each SF triggered by the safety device. For example, according to that table, PLd can be achieved in the following two situations:

- In the overall SF chain (Figure 1), the lowest PL among the components is "e" and there are more than three PLe components;
- In the overall SF chain, the lowest PL among the components is "d" and there are no more than three PLd components.

Here, knowing that the cobot's safety PLC has a PLd, cat. 3:

- With a PLe E-Stop button, triggering the "emergency stop" signal through the safety PLC or a PLe sensitive skin that triggers a "protective stop" signal through the safety PLC, the overall PL will be "d" according to the logic of Table 11 from ISO 13849-1:2015. One can observe that the component with the lowest performance level (here, "d") in the functional chain prevents the whole chain from having a higher PL, whence the importance of selecting the safety components of the functional chain with caution for compliance with the PL_r.
- Following the Table 11 guidelines, if a PLd laser scanner triggers a "protective stop" signal through that safety PLC, the overall PL will be "d."

When the safety function is entirely taken care of by the safety PLC (e.g., in the case of the reduced speed safety function), the performance level is that of the safety PLC, that is PLd.

4 Results

4.1 Highlights from the field

The robots associated with five of the six cases were inherently designed for collaborative applications. Consequently, they were cobots and complied with the safety requirements of ISO 10218-1:2011, specifically regarding PLd, cat. 3. However, the safety requirements mentioned in section 5.11 of ISO 10218-2:2011 related to integration were only partially taken into account, specifically concerning the risk assessment. This happened because most of the integrators interviewed for those cases relied substantially on the robot's performance characteristics and prioritized production over safety. On the other hand, the sixth case was a conventional robot transformed for a collaborative application.

Tables 2 to 4 present an overview of the main results regarding the six cases studied. In the cases that used Method 3 – Speed and separation monitoring to control the risk associated with collaborative operations, the separation between the worker and the robot was monitored by installing a presence detecting device at a fixed distance. In those cases, speed monitoring involves changing the velocity once a presence is detected in the collaborative workspace, decreasing from production speed to a reduced speed. In the field, methods 1, 3 and 4 were the main risk controls noted for collaborative operations (Section 2.1 describes those methods). Moreover, the robot was always the main focus of risk identification.

4.2 Highlights from the NRC finishing application

The risk assessment of the platform involved 55 risks, that is, 55 combinations of severity of harm and probability of harm corresponding to 55 hazardous situations. In the finishing collaborative application, six kinds of hazards generated these 55 risks (Figure 3). **Mechanical risks** came from the cobot arm, compliance head, rotating disc and workpiece. **Chemical risks** came from the metallic particles and fumes in the finishing process. **Thermal risks** came from the explosive metallic dust, as well as the warm or hot workpiece during and right after the finishing process. **Electrical risk** affected the whole platform since all the appliances and equipment are supplied with that type of energy. **Pneumatic risk** came from the compliance head's energy supply. Finally, **noise** came from the functioning of all the equipment: the cobot and the vacuum table.

Table 2. Documentation used and risk assessment – Overview of the main results

Company	Case	Documents used	Reason if no document was used	Risk assessment performed?	Required performance level (PL_r) estimated?
A	A_1	CSA Z434-2003	---	Partially: risk identification only	No, and no PL_r assumed
	A_2				
	A_3				
B	B_1	None	Not aware of them	Partially: risk identification only	No, and no PL_r assumed
C	C_1	ISO 12100:2010, ISO 13849-1:2015 and 2:2012, ISO 10218-1 and 2, EN 954	---	Completely: risk identification, risk estimation, and risk evaluation	Yes: PL_rd
D	D_1	ANSI/RIA R15.06-2012, SISTEMA software	---	Partially: risk identification, risk estimation	Yes: PL_re

Table 3. Risk reduction – Overview of the main results

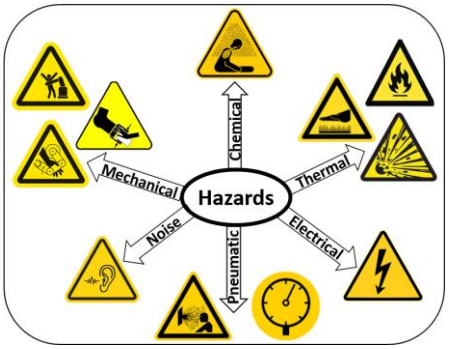
Co.	Case	Method for risk control associated with collaborative operations	The PL_r guided the safeguarding	The category guided the safeguarding	Validation of the collaborative application
A	A_1	3 and 4	No	Yes*	Yes
	A_2				
	A_3				
B	B_1	4	No	No	Was planned
C	C_1	1 and 3	Yes	No	Yes
D	D_1	1, 3 and 4	Yes	No	Was planned

*In that situation, the integrator did not estimate the PL_r but had a specific category in mind. He made his choice by simply assuming that it was the best category for the cobot installation.

Table 4. Details regarding the methods companies used, planned or were testing for risk control associated with collaborative operations

Method **	Case	Measures used to implement the method to control the risk associated with collaborative operations	Initial (I) or added (A) means
1	C_1	The transformed conventional robot stops whenever there is someone in the collaborative workspace's safety zone. It restarts automatically when the person leaves that zone as well as the workspace's warning zone. A combination of 6 laser scanners and 4 colour-sensing cameras detect the person's presence. A safety-related PLC manages the safety functions.	A
	D_1	A light curtain triggers a safety-rated monitored stop if one of its beams is blocked.	A
3	A_1, A_2, A_3	Two laser scanners installed at a fixed distance from the cobot trigger reduced speed when they detect a presence.	A
	C_1	A combination of laser scanners and cameras triggers an alarm and reduced speed when a presence is detected in the collaborative workspace's warning zone. A safety-related PLC manages the safety functions.	A
	D_1	A laser scanner installed at a fixed distance from the cobot triggers reduced speed when it detects a presence.	A
4	A_1, A_2, A_3	Force limitation according to the thresholds the integrator has selected.	I
	B_1	Force limitation by means of the spring in the cobot's joints.	I
	D_1	Force limitation according to the thresholds the integrator has selected.	I

**Section 2.1 provides the definitions of those methods.



(Sources: www.compliancesigns.com | istockphoto.com)

Figure 3. The six kinds of hazards identified in the finishing collaborative application

Table 5. Summary of the analysis of the mechanical risks requiring safety functions to protect people in the vicinity

No.	Hazard	Hazardous situation	Possible harm	Risk index ***	PL_r	Risk reduction measures (RRM) installed or commissioned, presented according to the efficiency hierarchy in ISO 12100:2010 (with 1 being the most efficient)	Overall PL achieved by each safety function
1	moving cobot	body part between the back of the platform and a wall	contusion, crushing, fracture, entrapment, shearing	3	c	**1)** Reduced speed of 16 mm/s (PL = d, cat. 3) **2)** Protective stop triggered by an Airskin sensitive skin (PL = e, cat. 3) in case of contact **3)** Emergency stop triggered by an E-Stop button (PL = e, cat. 4) *Note:* The safety functions here are RRM 1, 2 and 3.	PLd > PL_r ⇒ **each safety function provides the risk reduction required**
2	moving cobot OR moving compliance head	body part in the path of the cobot OR of the compliance head	contusion, crushing, entrapment	4	d	**1)** Reduced speed of 16 mm/s (PL = d, cat. 3) **2)** Protective stop triggered by an Airskin sensitive skin (PL = e, cat. 3) in case of contact **3)** Emergency stop triggered by an E-Stop button (PL = e, cat. 4) *Note:* The safety functions here are RRM 1, 2 and 3.	PLd = PL_r ⇒ **each safety function provides the risk reduction required**
3	disc at a standstill moved by the moving cobot	body part between disc and table	contusion, crushing, entrapment AND abrasion, irritation	3	c	**1)** Reduced speed of 16 mm/s (PL = d, cat. 3) **2)** Emergency stop triggered by an E-Stop button (PL = e, cat. 4) **3)** Pay attention to moving parts. *Note:* The safety functions here are RRM 1 and 2.	PLd > PL_r ⇒ **each safety function provides the risk reduction required**
4	rotating disc mounted onto the moving or stationary cobot	body part between disc and table when performing quality control near the process	contusion, crushing, entrapment AND abrasion, irritation, cuts, sectioning, entanglement	5	e	**1)** Reduced speed of 16 mm/s (this RRM concerns only the case where the cobot is moving) (PL = d, cat. 3) **2)** Protective stop triggered by a laser scanner if the operator comes too close to the disc (PL = d, cat. 3) **3)** Emergency stop triggered by an E-Stop button (PL = e, cat. 4) **4)** Flashing light **5)** Tie hair back and keep hands behind back to limit contact with the process **6)** Wear safety glasses (e.g., category 1A) and safety visor, both complying with CSA Z94.3-2020 and protective gloves resistant to heat (if > 80°C), abrasion and cutting to withstand the risk posed by the rotating disc (protection specifications to be determined through testing) *Note:* The safety functions here are RRM 1, 2 and 3.	PLd < PL_r ⇒ **each safety function provides an insufficient risk reduction**
5	ejected compliance head	body part in the trajectory of the ejection	contusion, fracture, concussion	4	d	**1)** Pneumatic locking system (PL = e, cat. 4) **2)** Reduced speed of 16 mm/s (this RRM concerns only the case where the cobot is moving) (PL = d, cat. 3) **3)** Appropriate safety shoes *Note:* The safety functions here are RRM 1 and 2.	PLd = PL_r ⇒ **each safety function provides the risk reduction required**

***Considering the application without its initial risk reduction measures

Note: In the far right column of Table 5, the overall PL achieved is estimated using the simplified theoretical method from Table 11 of ISO 13849-1:2015. That theoretical aspect represents a methodological limit of the paper.

According to the risk reduction process following the risk assessment, the use of safety functions was relevant to control the risks associated with the hazardous situations listed in Table 5, which summarizes the 36 risks (out of the 55 identified) for which the use of SFs was deemed necessary. Each of the five rows of this table represents a group of risks that required the same reduction measures.

5 DISCUSSION

Normally, a needs analysis paired with a risk assessment indicates whether a collaborative application is possible. However, in the NRC's laboratory application, the exact opposite was done. The search for innovative solutions to increase flexibility in finishing activities required that approach in order to push the limits of technology and see what can and cannot be done. For the NRC finishing application, a special case where the overall PL achievable is lower than the PL_r estimated in the risk assessment process (Table 5, line 4), the easiest solution would have been to install the finishing platform in an enclosure that no one can enter during production. However, due to the METALTec members' innovative request to find a way to share the same workspace safely with the cobot, supplementary Risk Reduction Measures (RRM) were added to RRM 1, 2 and 3, to cope with the insufficient overall PL. As line 4 of Table 5 shows, those supplementary measures rely on warning signs, safe working procedures and PPE that guards against abrasion, irritation, and cuts. In line 4 of Table 5, unlike RRM 1, which reduces the severity of harm by reducing the cobot arm's speed, or RRM 2 and 3, that remove the hazard by stopping the process, RRM 4 to 6 only limit the harm or help to avoid it when keeping the disc rotating is necessary for quality control. In line 4, PPE was added because the safety functions could not ensure sufficient risk reduction on their own and also to address the uncertainties related to the stopping time of the disk. In line 5, appropriate safety footwear is suggested in case the pneumatic locking system fails, which would result in the ejected compliance head falling on the operator's foot. Even though the overall PL achieved was estimated theoretically (see note below Table 5), proceeding that way is enough to fulfill the aim of this paper, which is about showing the importance of estimating the required reliability levels of safety functions in cobotics. The complete estimation of the overall PL, i.e. the validation tests of the safety functions using ISO 13849-2 (ISO, 2012) would have been necessary, for example, if the purpose of the paper was about proving that the safety functions are ready to play their role after the industrial partners brought the finishing platform to TRL 9. The finishing platform presented is currently in progress towards TRL 5.

The NRC's case also reminds us that buying a cobot complying with the minimum PL_rd does not guarantee that the SF triggered by a safety device will provide an overall PL complying with this minimum. In other words, the cobot may be safe on its own, but once integrated into the collaborative application, it may no longer be safe if an SF's overall PL is insufficient. Consequently, relying only on the robot's performance specifications is not adequate. It is important to consider the effect of the external safety components.

ISO 10218 allows safety functions to comply with a lower PL_r than "d" as long as a thorough risk assessment has confirmed it. For example, in the NRC's case, if the risk in line 1 of Table 5 were the only risk to control with RRM 1 to 3, a safety function providing an overall PLc would be sufficient. In this case, because some SFs required a PL of "c" while others required the higher PL of "d," the team sought to achieve an overall PL of "d." PLe was not considered because the cobot's PLd safety PLC makes it impossible to achieve, based on the calculation logic of Table 11 in ISO 13849-1:2015.

The results from the field emphasize that not all cobotics integrators are aware of the state of the art in machinery safety, namely the existing standards in industrial robotics (Table 2, company B). Tables 2 and 4 show that integrators in two companies visited had chosen safety devices (e.g. laser scanners) without estimating a required performance level to comply with (companies A, and B). The case of the finishing platform at the NRC (Table 5, line 4) showed that the risk assessment could require a PL_r higher than the minimum "d" required by the actual ISO 10218. This fact emphasizes the paramount importance of assessing risks, especially those that will be reduced by the use of safety functions. Assuming a PL_r instead of estimating it might put a company in a situation where the assumption made it overestimate the PL_r. Such overestimation would entail higher expenses for safety components. In addition, choosing safety devices by relying only on their category (as Company A did) has not been accepted since the 2006 version of ISO 13849-1. Indeed, a single category can contribute to different performance levels. One can achieve PLd with category 3, as well as with category 2, for instance. Consequently, relying on the PL or its equivalent SIL is the way to go.

Table 4 shows how much the power-and-force-limited method by design or by control helped secure the cobotic applications visited. That method is also available for the cobot used at the NRC. However, it does not always detect a collision with a human depending on the person's size. To make sure any operator would be safe in case of a collision, Airskin sensitive skin was mounted on the cobot. If it collides with an obstacle, the air pressure underneath changes. That change triggers a protective stop. Adding that solution proved more reliable in the NRC's case. Even though cobots come with inherently designed safety measures such as padded or round joints, or their safety PLC in which various safety functions can transit, those design principles are not always self-sufficient. The field and the NRC examples showed that an external safety device was often needed to reduce the risk to an acceptable level. The safety PLC alone cannot always do the whole job. It needs sensors to trigger different actions in the cobot: a stop or reduced speed, for instance. Lastly, line 4 (Table 5) mentions that the required protection specifications for the gloves will be revealed through testing. The reason is that since there are different types of finishing tasks, as mentioned in Section 3.2, as well as various rotating speeds and diverse kinds of discs depending on the finishing task, the PPE expert on the team will have to assess the behaviour of different protective gloves under different conditions, including the risk of entrapment in rotating parts. The glove that withstands the worst-case scenario will be suggested for quality control, and its ability to provide a suitable protection will be assessed. That necessity for testing the different possible discs raises the following points:

- Given that the consortium is searching for a flexible finishing platform, favouring risk reduction measures that will protect against the worst-case scenario allows the platform to remain agile;
- Anticipating as much as possible the different robotic tools and workpieces that will be involved in the finishing

platform allows integrators to assess the safety-related risks they generate for the operator, and therefore help plan how to control them. For example, a trajectory optimization expert at the NRC is planning optimal safe movements of the cobot depending on the workpiece and the robotic tools available in the library of discs and parts.

6 Conclusion

This paper clearly revealed the importance of estimating the required reliability level of every safety function in a collaborative application. It also highlighted the need to perform a risk assessment, considering the human, the cobot and the auxiliary equipment while dealing with all the possible hazards they and their environment might generate. An assessment is important for any kind of equipment where the human's safety relies on a safety function. In cobotics, human safety relies crucially on safety functions and so the required reliability level of that function is a key element to consider as a reference level to judge if the risk controlled is acceptable. If not, then the necessary actions must be taken.

At the NRC, the risk assessment and risk reduction for the finishing platform are still evolving since the process is a continuous improvement exercise. The next steps will seek more agility in safety to respond to the need for flexibility in the process by introducing a safe gesture recognition system.

7 Acknowledgements

We thank the IRSST for funding the two studies. We also thank the companies visited in the first study, as well as Laurent Giraud (researcher at IRSST), who participated in some of those visits. The second study was conducted as part of a project supported by the NRC's METALTec industrial research group and National Program Office and the Metal Transformation Research and Innovation Consortium (CRITM). We thank Michaël Lessard-Poulin, Product Expert at Prevost, and Gabriel Caron-Guillemette, Project Engineer at Alstom, who provided valuable ongoing technical support. We acknowledge the NRC team who participated in the various aspects of this study: Christian Corbeil, Julien-Mathieu Audet, and Gabriel Côté, and the METALTec industrial research group members that supported this investigation and publication.

8 References

Askarpour, M., Mandrioli, D., Rossi, M. & Vicentini, F. (2017). Formal model of human erroneous behavior for safety analysis in collaborative robotics. *Robotics and Computer-Integrated Manufacturing*, 57, 465-476.

Charpentier, P. & Sghaier, A. (2012). Industrial robotic: Accident analysis and human-robot coactivity. [Conference]. Safety of Industrial Automated Systems (SIAS), Montreal, Quebec.

Chinniah, Y., Gauthier, F., Lambert, S., & Moulet, F. (2011). *Experimental analysis of tools used for estimating risk associated with industrial machines* (Report R-684) [Research Report]. IRSST.

Chinniah, Y., Nix, D.S.G., Jocelyn, S., Burlet-Vienney, D., Bourbonnière, R., Karimi, B., & Ben Mosbah, A. (2019). Safety of machinery: Significant differences in two widely used international standards for the design of safety-related control systems. *Safety*, 5(4), 1-16.

Directive 2006/42/EC - new machinery directive. https://osha.europa.eu/en/legislation/directives/directive-2006-42-ec-of-the-european-parliament-and-of-the-council

Dźwiarek, M. (2004). An analysis of accidents caused by improper functioning of machine control systems. International Journal of Occupational Safety and Ergonomics, 10 (2), 129-136.

Fryman, J., Arbor, A., & Matthias, B. (2012). *Safety of industrial robots: From conventional to collaborative applications* [Conference]. SIAS, Montreal, Quebec.

Gopinath, V., & Johansen, K. (2016). Risk Assessment Process for Collaborative Assembly – A Job Safety Analysis Approach. *Procedia CIRP 44*, 199-203.

Gualtieri, L., Fraboni, F., De Marchi, M., & Rauch, E. (2022). Development and evaluation of design guidelines for cognitive ergonomics in human-robot collaborative assembly systems. *Applied Ergonomics*, 104, 1-15.

Henley, J. (2022). *Moscow incident occurred because child 'violated' safety rules by taking turn too quickly, says official*. The Guardian. https://www.theguardian.com/sport/2022/jul/24/chess-robot-grabs-and-breaks-finger-of-seven-year-old-opponent-moscow

IEC (International Electrotechnical Commission). (2021). *Safety of machinery - Functional safety of safety-related control systems* (Standard IEC 62061). IEC.

IFR (International Federation of Robotics). (2022). *World Robotics 2022* [Presentation of the Report]. https://ifr.org/downloads/press2018/2022_WR_show_version.pdf

ISO (International Organization for Standardization). (2010). *Safety of Machinery – General Principles for Design – Risk Assessment and Risk Reduction* (Standard ISO 12100). ISO.

ISO. (2011a). *Robots and Robotic Devices – Safety Requirements for Industrial Robots – Part 1: Robots.* (Standard ISO 10218-1). ISO.

ISO. (2011b). *Robots and Robotic Devices – Safety Requirements for Industrial Robots – Part 2: Robot Systems and Integration.* (Standard ISO 10218-2). ISO.

ISO. (2012). *Safety of machinery – Safety-related parts of control systems — Part 2: Validation.* (Standard ISO 13849-2). ISO.

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

ISO. (2016). *Robots and robotic devices – Collaborative robots*. (Technical Specification ISO/TS 15066). ISO.

ISO. (2022). *Robotics – Safety Requirements for Robot Systems in an Industrial Environment – Part 2: Robot Systems, Robot Applications and Robot Cells Integration*. (Draft of standard ISO 10218-2). ISO.

Malm, T., Viitaniemi, J., Latokartano, J., Lind, S., Venho-Ahonen, O., & Schabel, J. (2010). Safety of interactive robotics – Learning from accidents. *International Journal of Social Robotics*, 2, 221-227.

Moulières-Seban, T. (2017). *Conception de systèmes cobotiques industriels: Approche cognitique – Application à la production pyrotechnique au sein d'Ariane Group* [Doctoral thesis, Université de Bordeaux].

Sghaier, A., Jocelyn, S., Burlet-Vienney, D., & Giraud, L. (2015). *A Study of main safety-related functions available to collaborative robotics*. [Conference]. SIAS, Königswinter, Germany.

Villard, J. (2003). *Accidents caused by the failure of safety components* [Conference]. SIAS, Nancy, France.

Xiao, M. (2022). *Cobot Market Sees 40% Growth Rebound In 2021*. Interact Analysis. https://www.interactanalysis.com/cobot-market-sees-40-growth-rebound-in-2021/