“Safety-rated monitored stop” collaborative operation function for industrial robots: a simple model for functional analysis purposes

GIOVANNI LUCA AMICUCCI, FABIO PERA, ERNESTO DEL PRETE

Dept. of Technological Innovations and Safety of Plants, Products and Anthropic Settlements
INAIL – National Institute for Insurance against Accidents at Work
Via Roberto Ferruzzi, 38 – 00143 Roma – ITALY

Abstract: - Collaborative robot operations are standardized since, in consideration of the shared workspace, operators are exposed to possible contact with moving parts of robots. Collisions with humans can be extremely hazardous: for this reason, “safety functions”, based on sensors, actuators and control systems, are adopted. If there is a failure in one of these components, an accident can happen. Among the safety functions used, depending on the collaborative application, there is the “safety-rated monitored stop”. Functional safety analysis can help system designers and integrators to certify the achievement of the required objectives for the chosen safety function. In the present paper, a similar analysis is carried out for the safety-rated monitored stop function. The method chosen, depicted with an example, is based on applicable standards.

Key-Words: - Collaborative robot operation, safety-rated monitored stop, average frequency of dangerous failures (*PFH*), failure rate, safe failures, dangerous failures, safe failure fraction (*SFF*), diagnostic coverage (*DC*), common cause failures (*CCF*), reliability model.

Received: April 21, 2021. Revised: March 17, 2022. Accepted: April 18, 2022. Published: May 19, 2022.

1 Introduction

Industrial robots are used to perform hazardous, difficult, repetitive, or heavy tasks, to increase productivity. Their reliability and safety have been regarded as research topics in the technical literature ([10]) and have been included in regulatory standards ([1–3]).

Robots use mechanical, pneumatic, hydraulic, electrical and electronic components that can be sources of hardware failures. Programming errors can be the source of software malfunctions. Moreover, human misbehavior (bypass of safeguards) and/or light behaviors (improper planning, hazardous conditions and ineffective training of workers) can cause fatal accidents.

The applicable standards [1–3] consider collaborative work between humans and robots as a permitted working procedure when required by the specific task and under appropriate conditions.

However, when entering the robot's workplace, humans are subject to collision with the moving parts of the robot, with additional hazards of being pinched, crushed or pinned down. Safeguarding the perimeter of an industrial robot cell is a widespread way of protecting workers. Instead, when dealing with collaborative robots, sensors are used to detect human presence, and a control system manages the robot's motion to avoid accidents.

If a part of this control chain is misfunctioning, a hazardous event can result in an accident.

Reliability is normally linked to the productivity of the robot cell and to its *availability* when asked to complete a task ([10–12, 18]). While *functional safety* is considered when dealing with the reliability and availability of *safety functions*, i.e. of that part of the control system (including sensors and actuators) that acts as a protective measure to avoid accidents. In such a case, great importance has rightfully been given to *risk assessment* [(14 – 17)]. By harmonizing the suggestions contained in different standards ([1–8]), there is shown a simple method for the functional safety assessment of the safety function known as “*safety-rated monitored stop*”, used during collaborative tasks.

1.1. Background

The technical regulation on industrial robots [1–3] provides safety requirements for manufacturers and integrators. Safety issues are dealt with by an intrinsically safe design, i.e. by reducing the mass of the manipulator, its speed, the force it can exert and by adding soft surfaces or rounded edges. Alternatively, it suggests adopting safety functions (with sensors, a control system and actuators) to recognize and avoid a hazardous situation or to reduce the effects of events that cannot be avoided

[7]. If the safety function does not work correctly and a hazardous event occurs, then the operator is directly exposed to the hazard and an accident can occur [9]. To reduce the probability of such an event, functional safety suggests that redundant architectures can be used to implement the safety function [5, 6]. The degree of redundancy can be inferred from the design specifications [5–7].

1.2. State of the art

In [10] reliability and availability of robots, from the point of view of productivity and accomplishment of tasks, are faced using standard probabilistic methods. In [11] a method that takes into account uncertainties in the quantification of reliability parameters by using fuzzy logic is proposed, obtaining a more restrictive determination of times for cost-effective robot maintenance. In [12] the reliability of a robot production line in an automotive assembly plant is considered. In [18] it is stated that to have a more punctual estimation of robot reliability it is important to integrate field data with manufacturer information. Over the years, the need for human-robot collaboration has developed, since the addition of human capabilities (dexterity, adaptability, problem-solving creativity) permits an increased efficiency of the robot cell. In [13] a survey on the application and safety of human-robot collaboration was considered. In [19] it is noted that the risk assessment of a collaborative robot cell has to take into account new hazards, which are usually not considered when the robot is safeguarded in a traditional robot cell. These hazards arise from the proximity of the robot and the operator and the possibility of contact between them. In [14] it is shown that, for the sake of safety and economy, it is important to previously design the collaborative application before proceeding with its realization. In [15, 16] it is shown that a suitable layout design of the robot cell is important for safety purposes. To accomplish the risk assessment of the human-robot collaborative cell, it is possible to adopt design automation frameworks, as shown in [17].

2 Collaborative operations

Collaborative operation is a special kind of work procedure, in which an operator and a robot share a common workspace [1–3]. It can be used for predetermined tasks that only robot systems specifically designed can accomplish.

The part of the safeguarded space where the operator can interact directly with the robot to perform a task is called *collaborative workspace* (fig. 1). For risk reduction purposes, its location and shape are clearly defined (e.g. floor markings, signs).

In the collaborative workspace, due to the reduction of spatial separation between the human and the robot, physical contact can occur during operations. Hence, the robot cell has to adopt protective measures, to ensure the operator's safety at all times. To provide suitable protective measures, the integrator has to conduct a risk assessment where the entire collaborative task and the workspace have to be considered, taking into account:

- robot characteristics (e.g. load, speed, force, power, paths, orientations),
- end effector and workpiece characteristics (e.g. tool changer, edges, protrusions),
- location characteristics (e.g. building supports, walls, fixtures, layouts, operator location);
- environmental characteristics (e.g. chemical substances, EM disturbances, radiation);
- other machines, which are connected or attached to the robot system and may introduce a hazard;
- application-specific hazards (e.g. hot surfaces, ejected parts, welding splatters);
- design (e.g. ergonomics, modes) and location (e.g. accessibility) of any manually controlled robot guiding device;
- performance criteria of the safety functions;
- protective devices used for safeguarding and presence detection.

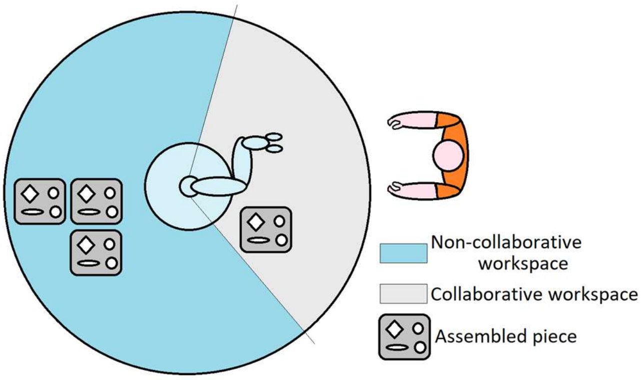


Fig. 1: Collaborative workspace

Perimeter safeguarding is applied to prevent any person from entering the safeguarded space or, to avoid hazards due to unexpected start-up, to detect any presence inside. Conversely, collaborative workspace safeguarding is adopted for operation purposes and to prevent any intrusion from the collaborative workspace into the non-collaborative part. The collaborative workspace has to be designed such that the operator can easily perform all tasks and the location of equipment and machinery should not introduce additional hazards. *Safety-rated soft axes* and *space limiting* can be used to reduce the range of possible free motions, whenever possible.

2.1 Standardized collaborative operations

The standards [1–3] consider four collaborative operation types:

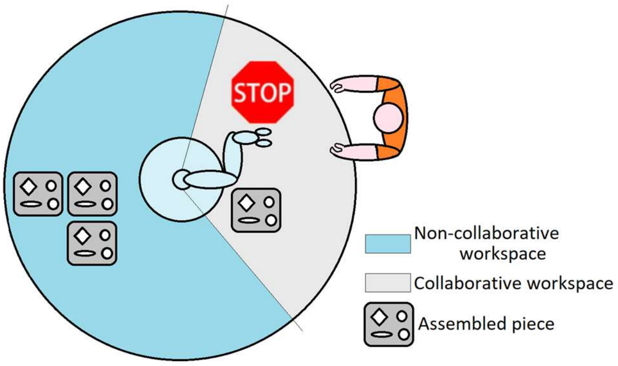


Fig. 2: Safety-rated monitored stop

- *Safety-rated monitored stop* (fig. 2): when in the collaborative workspace there is no person, the robot operates autonomously. When a person enters the collaborative workspace, the robot stops its motion and maintains a safety-rated monitored stop. The stop is issued to allow direct interaction between the operator and the robot (e.g. performing a task on the workpiece or loading a part onto the end-effector). When the operator leaves the collaborative workspace, the non-collaborative robot motion may resume automatically.

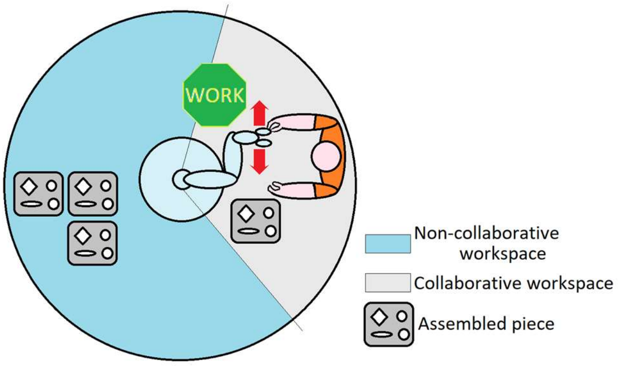


Fig. 3: Hand guiding

- *Hand guiding* (fig. 3): when the robot is ready, it enters the collaborative workspace and reaches the hand-over position. Then a safety-rated monitored stop is issued, waiting for the operator. When the operator has taken control, the safety-rated monitored stop is cleared. The operator transmits motion commands through a hand-operated, guiding device located at or near the end-effector. When the operator releases the guiding device, a safety-rated monitored stop is issued. When the operator leaves the collaborative workspace, the non-collaborative robot motion may resume automatically. If the operator enters the collaborative workspace before the robot system is ready, then a protective stop is issued.

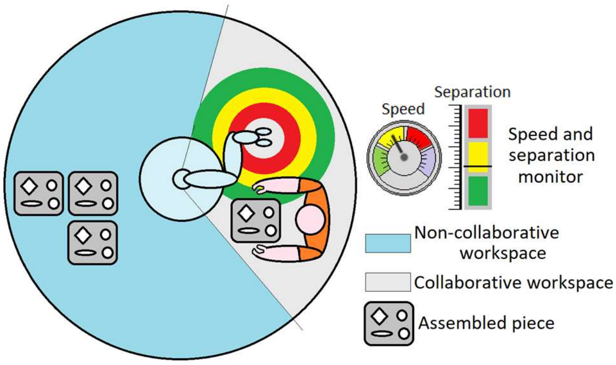


Fig. 4: Speed and separation monitoring

- *Speed and separation monitoring* (fig. 4): the robot and the operator may move concurrently in the collaborative workspace, but the robot never gets closer than the protective separation distance. When the separation distance decreases to a value below such a distance, the robot system stops. When the operator moves away from the robot, beyond the protective separation distance, the robot's motion resumes automatically. When the robot system reduces its speed, the protective separation distance may be decreased correspondingly. Maximum permissible speeds and minimum protective separation distances have to be determined through risk assessment.

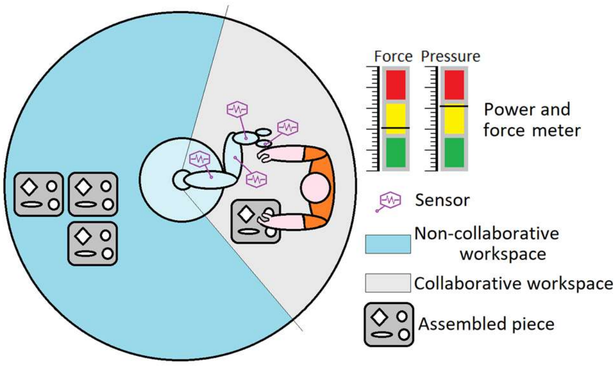


Fig. 5: Power and force limiting

- *Power and force limiting* by design or control (fig. 5): risk reduction can be obtained through inherently safe robot design or through a safety-related control system that keeps the hazards below pre-determined threshold values. Risk reduction measures for contacts can be either passive or active. Passive measures address the mechanical design (smooth surfaces, rounded edges, deformable parts, avoidance of any clamping event or easy and independent escape from it). Active measures address the control design of the robot system (limiting forces or torques, limiting velocities, use of *safety-rated monitored stop* function, sensors to detect proximity and reduce forces).

2.1.1 Target failure measure and performance requirements

The standards ISO 10218-1 [1] and ISO 10218-2 [2] require that the safety-related parts of the robot control system be designed so that:

a) a single fault in any of these parts does not lead to the loss of safety function;
b) a single fault has to be detected at or before the next demand of safety function, whenever reasonably practicable;
c) when a single fault occurs, the safety function is always performed (a safe state is reached and maintained until the detected fault is corrected);
d) the diagnostic system detects all detectable faults; during proof testing all faults are detected (including those that are undetectable by the diagnostic system).

Proof testing is in-depth testing, performed at chosen time intervals, during which the system is restored “as new”. The requirement d) means that the diagnostic system does not perform 100% *diagnostic coverage*. Thus, undetected faults exist and their accumulation can lead to unintended behaviors of the robot and hazardous situations.

Performance level (PL) and *safety integrity level* (SIL) are used to express *target failure measures* such as intervals of the *frequency of dangerous failures on demand* (*PFH*) of the safety function (Table 1).

According to the standard ISO 13849-1 [5], the previous requirements comply with a *performance level* PL=d, with a *category* 3 architecture of the safety-related parts (see § 2.1.2), or, according to the standard IEC 62061 [6], they comply with SIL 2, with a *hardware fault tolerance* (*HFT*) of 1 and a *mission time* T_M of not less than 20 years.

Table 1: Target failure measure in high demand or continuous mode of operation (IEC 61508 [7], IEC 13849-1 [5], IEC 62061 [6])

Safety integrity level (SIL) IEC 61508 [7], IEC 62061 [6]	Performance level (PL) IEC 13849-1 [5]	Average frequency of dangerous failure on demand of the safety function [h^{-1}] (*PFH*)
Not available	a	$10^{-5} \leq PFH < 10^{-4}$
1	b	$3{\cdot}10^{-6} \leq PFH < 10^{-5}$
1	c	$10^{-6} \leq PFH < 3{\cdot}10^{-6}$
2	d	$10^{-7} \leq PFH < 10^{-6}$
3	e	$10^{-8} \leq PFH < 10^{-7}$

A comprehensive risk assessment on the robot system and its use may determine, for the intended application, a different safety-related control system performance, other than the one just recalled (eventually a higher one).

Actually, in certain cases, the target failure measures and performance requirements considered in the standards ISO 10218-1 [1] and ISO 10218-2 [2] are very demanding in terms of complexity and cost.
For such a reason, the next edition of these standards introduces a classification of robots into two classes:

- *Class* I: including robots with a maximum mass per manipulator (mass of moving parts) of 10 kg or less, maximum force per manipulator of 50 N or less and maximum speed of 250 mm/s or less;
- *Class* II: including robots that exceed at least one of the limits for Class I robots.

The minimum performance level for Class I robots is expected to be PL=b (SIL 1), while for Class II robots it is expected to be PL=d. The performance level of the *emergency stop* function is expected to be at least PL=c (SIL 1), for both classes.

2.1.2 Architecture and hardware fault tolerance

A *hardware fault tolerance* (*HFT*) of *N* means that *N*+1 faults could cause a loss of safety function.
The requirements for the single fault tolerance (HFT=1) can be achieved if the safety-related part of the control system has a redundant architecture (fig. 6).
The redundant channels are designed so that the surviving channel performs the safety function when a fault is present in the other channel.

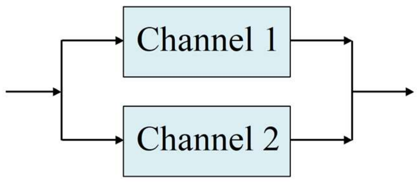
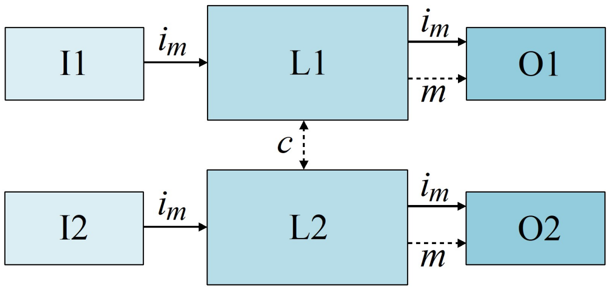


Fig. 6: Redundant architecture

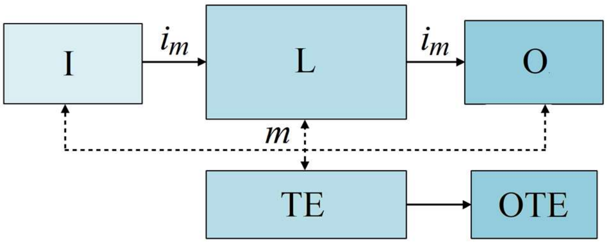
The standard ISO 13849-1 [5] introduces a *category* 3 architecture, as in fig. 7, to represent a redundant safety-related part of the control system with HFT=1.



i_m = interconnecting means m = monitoring c = cross monitoring	I1, I2 = input device/sensor L1, L2 = logic O1, O2 = output device

Fig. 7: Category 3 architecture according to ISO 13849-1 [5]

The next edition of ISO 10218-1 is expected to also permit a relaxation of the architecture requirements. In fact, for Class I robots, the requirements on the target failure measure (PL=b or SIL 1) do not specify the architecture to be adopted. In the same way, for Class II robots, if the requirements on the target failure measure (PL=d or SIL 2) are obtained with a *PFH* that is less than $4.43 \cdot 10^{-7}\ h^{-1}$, nothing is specified about the architecture. In such cases, it is no longer mandatory the adoption of a *category* 3 architecture (according to ISO 13849-1 [5]) or a redundant channel with *HFT*=1 (according to IEC 62061 [6]). Then a non-redundant architecture can eventually be adopted, such as a *category* 2 architecture (as in fig. 8, according to ISO 13849-1 [5]), or a single channel with *HFT*=0 and some diagnostic capability (according to IEC 62061 [6]).



i_m = interconnecting means m = monitoring TE = test equipment OTE = output of TE	I = input device/sensor L = logic O = output device

Fig. 8: Category 2 architecture according to ISO 13849-1 [5]

2.1.3 Stop categories

IEC 60204-1 [4] considers three *categories of stop functions* (not to be confused with the *category* architectures specified in ISO 13849-1 [5]):

- *Stop category* 0: an uncontrolled stop where the machine is stopped by immediately removing the power to its actuators;
- *Stop category* 1: a controlled stop where the power to the machine actuators is available during the stop and is removed afterwards;
- *Stop category* 2: a controlled stop where the power remains available to the machine actuators.

2.1.4 Protective stop

Any robot protective stop function may be initiated manually or by the control logic. The intended performance has to comply with the target failure measure requirements considered in § 2.1.1. When activated, it will cause the stop of all robot motion, the removal or control of the power to the robot actuators, and control of any hazard caused by the robot. It may be *stop category* 0, 1, or 2.

2.1.5 Safety-rated monitored stop

The table of the robot's behavior during the *safety-rated monitored stop* is outlined in Table 2.

Table 2: Safety-rated monitored stop operations [3]

Robot motion or stop function		Operator's proximity to collaborative workspace	
		Outside	**Inside**
Robot's proximity to collaborative workspace	**Outside**	Continue	Continue
	Inside and moving	Continue	Protective stop
	Inside, at safety-rated monitored stop	Continue	Continue

The robot cell has to be equipped with safety-rated devices, which are used to detect the presence of an operator within the collaborative workspace. An operator can enter the collaborative workspace only if (according to ISO/TS 15066 [3]):

- the robot or other hazards are not present in the collaborative workspace, or
- the robot is present in the collaborative workspace and is in a *safety rated-monitored stop*, holding as long as the operator remains (such a stop is a *stop category* 2; according to IEC 60204-1 [4], the drive power is not removed and the standstill condition is monitored), or
- the robot is present in the collaborative workspace and is in a protective stop (*stop category* 0 or 1, according to IEC 60204-1 [4]).

Any violation of these requirements (i.e. an unintended motion of the robot in the monitored standstill condition or a detected failure of the protective stop function) results in a protective stop (*stop category* 0, according to IEC 60204-1 [4]).
The *safety-rated monitored stop* is used by the remaining collaborative operations as a sub-function. For such a reason, in the next edition of standards ISO 10218-1 [1] and ISO 10218-2 [2], it will be considered a conditional safety function (called *monitored standstill*) and it will no longer be considered a collaborative operation type.

3 Method: safety reliability modelling

Some of the *safety function*s perform monitoring tasks while others perform safety-relevant actions.
The triggering of a *safety function* is normal during intended operations (not having a failure or a fault) and it will result in a defined behavior.
Therefore, the specification of the requirements has to clearly state-the reaction when a violation of limits

is detected during the correct operation of the *safety function*, and the reaction when the diagnostics detect a fault within the *safety function*.

The specification of the reaction function shall take into account also the fact that parts of the function may not be functioning if a fault exists.

During the design phase, a safety reliability model can be developed using the information collected by the requirements specification. We propose to do it by following the method suggested in IEC 61508 [7]. The safety system architecture is normally derived by decomposing the safety sub-functions and allocating parts of the safety sub-functions to subsystems. This representation describes the safety-related part of the control system at an architectural level. Such a model is used to combine the failure measures of subsystems and components, to obtain the overall target failure measure, which permits to assess the compliance of the designed safety system with the claimed target failure measure (§§ 4.1–4.4).

The following aspects are extracted from the *safety functions requirements specification* (IEC 61508 [7]):

a) the installation and the operating modes of the safety system (setting, start-up, maintenance, normal intended operation);
b) how the safety system achieves and maintains a safe state;
c) the priority of the simultaneously active functions to avoid conflicts;
d) the required actions on detection of a violation of limits during the correct operation;
e) the behavior of the fault reaction functions;
f) the maximum fault reaction time to enable the corresponding fault reaction before a hazard occurs;
g) the maximum response time of each function.

The following aspects are extracted from the *safety integrity requirements specification* (IEC 61508 [7]):

a) a target failure measure (PL or SIL) and an upper limit of *PFH* value for each safety function;
b) the mission time (T_M);
c) the extremes of all environmental conditions (including electromagnetic ones) that are likely to be encountered during storage, transport, testing, installation, operation, and maintenance;
d) limits and constraints for the realization of the safety functions, to minimize the possibility of *common cause failures* (*CCF*).

The following aspects are extracted from the *safety system architecture specification* (IEC 61508 [7]):

a) requirements for the subsystems and their parts;
b) requirements for the integration of subsystems and parts to meet the safety requirement specification;
c) logic and mechanical performance that enables response time requirements to be met;
d) accuracy and stability requirements for measurements and controls;
e) interfaces between the safety-related part of the control system and any other system;
f) interfaces with operators;
g) all modes of behavior, including the failure behavior and the required response (for example, alarms, automatic shut-down);
h) the significance of all hardware/software interactions and constraints;
i) any limits and constraints for the safety-related part of the control system and its subsystems (for example, time constraints or the required diagnostic test interval of the hardware necessary to achieve the target failure measure).

3.1 Accounting the architectural constraints

The *PFH* of each safety function, due to random hardware failures, can be estimated by taking into account:

a) the architecture of that safety function (including *HFT* values);
b) the estimated failure rate of *safe failures* (λ_S, where *S* stands for *safe*);
c) the estimated failure rate of *dangerous failures* which are *detected* by diagnostic tests (λ_{DD}, where *DD* stands for *dangerous detected*);
d) the estimated failure rate of *dangerous failures* which are *undetected* by diagnostic tests (λ_{DU}, where *DU* stands for *dangerous undetected*);
e) the susceptibility of the safety function to *common cause failure*s (β, for *DU* failures, and β_D, for *DD* failures);
f) the *diagnostic coverage* (*DC*) of the *diagnostic tests* (so that $\lambda_{DD} = DC \cdot \lambda_D$ and $\lambda_{DU} = (1 - DC) \cdot \lambda_D$, where $\lambda_D = \lambda_{DD} + \lambda_{DU}$) and the associated *diagnostic test interval* ($\tau_{test} = 1/\mu_{test}$);
g) the *proof test interval* (τ);
h) the *mean repair time* ($MRT = \tau_{rep} = 1/\mu_{rep}$);
i) the probability of *dangerous failure* of any data communication process.

Component failure rate data can be obtained from a recognized source (for example, data published from a certain number of industry sources) or be estimated based upon site-specific failure data, if available. If this is not the case, then generic data can be used.

A constant failure rate is assumed for each component, to permit an algebraic treatment of the mathematics involved. This only applies provided that the useful lifetime of components is not exceeded, since beyond the useful lifetime the probability of failure significantly increases with time. The useful lifetime depends highly on the operating conditions (temperature in particular).

The highest SIL that can be claimed for a safety function is limited by its architecture.

IEC 61508 [7] gives two routes (Route 1H and Route 2H) that may be used to derive a SIL. Both routes take into account the architecture in terms of the *hardware fault tolerance* and the *safe failure fraction* of the subsystems used in the realization of that safety function. The *safe failure fraction* (*SFF*) is defined as the ratio between those failures that are safe (i.e. that lead to a safe state, whose rate is λ_S) or are managed by the diagnostic part of the safety function (whose rate is λ_{DD}) and all failures (including the dangerous undetected ones, whose rate is λ_{DU}):

$$SFF = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_{DD} + \sum \lambda_{DU}} \tag{1}$$

To estimate the *SFF* of a subsystem, an analysis (for example, *fault tree analysis* or *failure mode and effects analysis*) has to be performed to determine all relevant faults and their corresponding failure modes. The rate of each failure mode is determined based on the rate of the associated faults.

Route 2H can be followed if component reliability data is obtained through feedback from end-users and there is sufficient confidence in such data, otherwise Route 1H is preferred.

According to Route 1H in IEC 61508 [7], Table 3 and Table 4 specify the highest SIL that can be claimed for a *safety function*, which uses a given *subsystem*, in terms of the *HFT* and *SFF* of that subsystem.

Table 3: Maximum allowable SIL for a safety function carried out by a *type* A safety-related element or subsystem (according to IEC 61508 [7] and IEC 61800-5-2 [8])

Safe failure fraction	**Hardware fault tolerance (*HFT*)**		
	0	**1**	**2**
***SFF* < 60%**	SIL 1	SIL 2	SIL 3
60% ≤ *SFF* < 90%	SIL 2	SIL 3	SIL 3
90% ≤ *SFF* < 99%	SIL 3	SIL 3	SIL 3
99% ≤ *SFF*	SIL 3	SIL 3	SIL 3

Table 4: Maximum allowable SIL for a safety function carried out by a *type* B safety-related element or subsystem (according to IEC 61508 [7] and IEC 61800-5-2 [8])

Safe failure fraction	**Hardware fault tolerance (*HFT*)**		
	0	**1**	**2**
***SFF* < 60%**	Not allowed	SIL 1	SIL 2
60% ≤ *SFF* < 90%	SIL 1	SIL 2	SIL 3
90% ≤ *SFF* < 99%	SIL 2	SIL 3	SIL 3
99% ≤ *SFF*	SIL 3	SIL 3	SIL 3

When using Table 3 or 4, in determining the *HFT*:

a) no account shall be taken of other measures (such as diagnostics) that may control the effects of faults;
b) where one fault directly leads to the occurrence of subsequent faults, these are considered as a single fault;
c) certain faults may be excluded, provided that the likelihood of them occurring is very low.

A *subsystem* can be regarded as *type* A if the following criteria are satisfied:

a) the failure modes of all its components are well defined; and
b) the behavior of the *subsystem* under fault conditions can be completely determined; and
c) there is sufficient dependable failure data from field experience to show that the claimed failure rates for *DD* and *DU* failures are met.

A *subsystem* can be regarded as *type* B if one or more of the criteria for type A is not satisfied by at least one of its components (complex hardware or sub-systems containing software are regarded as type B).

If Route 2H is selected, Table 5 (which resumes clause 7.4.4.3 in IEC 61508 [7], part 2) provides the minimum *HFT* that a *subsystem* implementing a *safety function* with a specified SIL shall possess. In this case, the reliability data uncertainties shall be taken into account and the system shall be improved until there is a confidence greater than 90% that the target failure measure is achieved. Moreover, all type B elements shall have a minimum diagnostic coverage of not less than 60%.

Table 5: Minimum *HFT* for a safety-related element or subsystem with specified SIL (high demand or continuous mode of operation, according to IEC 61508 [7])

Safety integrity level	**Minimum hardware fault tolerance (*HFT*)**
SIL 3	2(*)
SIL 3	1(*)
SIL 2	1(*)
SIL 1	0

(*) For type A elements and situations where an *HFT* greater than 0 is required, if, by following the *HFT* requirements, additional failures, leading to a decrease in the overall safety, would be introduced, then a safer alternative architecture with reduced *HFT* may be implemented.

4 Results: *PFH* determination

The *safety-rated monitored stop* is triggered when the redundant sensors detect a human being inside the collaborative workplace (safeguarding and presence detection in the non-collaborative part of the workplace are controlled by a different safety function). Other redundant sensors monitor the standstill position. The safety function, which is active in continuous mode of operation, is implemented together with other non-safety-related functionality of the control system, using only a few exclusive components. A reliability model can be split into three parts, such as in fig. 9:

- the internal *Supply Unit* (also called *S-module*, fig. 10, with $PFH=PFH_S$),
- the *Safety-related part of control system* (also called *C-module*, fig. 11, with $PFH=PFH_C$), and
- the *Robot power module and joint motors* (also called *P-module*, fig. 12, with $PFH=PFH_P$).

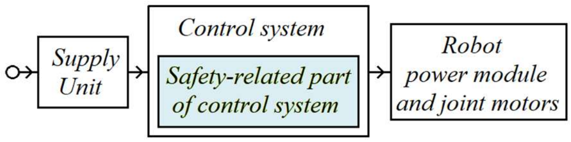


Fig. 9: Reliability block diagram

The likelihood of failures affecting more than one subsystem in the same proof test interval is low, hence neglecting higher order cut sets is possible and the function *PFH* can be calculated as follows:

$$PFH \approx PFH_S + PFH_C + PFH_P \tag{2}$$

According to the operating philosophy in IEC 61508 [7], when *DD* failures are detected in a single channel, that channel is immediately brought to a safe state. Hence, *DD* failures of non-redundant channels can be disregarded when determining the *PFH* of those channels. Instead, *DU* failures, which are revealed only in a proof test, play a fundamental role. Since *DU* failures remain undetected (and thus unrepaired), there can be at most one *DU* failure in each proof test interval $(0, \tau)$ for a single channel. If $N(0, \tau)$ is the number of failures in the interval $(0, \tau)$, then the expected number of failures that are able to lead that channel to a hazardous event is:

$$E[N(0,\tau)] = 0\cdot\Pr[N(0,\tau)=0]+1\cdot\Pr[N(0,\tau)=1] = \\ = \Pr[N(0,\tau)=1] = 1-e^{-\lambda_{DU}\tau}$$

and the *PFH* of that channel is [7, 9]:

$$PFH = \frac{E[N(0,\tau)]}{\tau} = \frac{\left(1-e^{-\lambda_{DU}\tau}\right)}{\tau} \approx \lambda_{DU} \tag{3}$$

For what concerns the mean downtime of a channel:

- if a *DU* failure occurs, the mean downtime is given by the sum of the mean downtime in the proof test interval ($\tau/2$) and the mean repair time (*MRT*) [7, 9], while
- if a *DD* failure occurs, the mean downtime is called *mean time to restore MTTR* and it is given by the sum of the mean time to reveal the failure ($\tau_{test}/2$) and the mean repair time (*MRT*) [7, 9].

Then it is possible to define the channel-equivalent mean downtime as [7, 9]:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{\tau}{2}+MRT\right)+\frac{\lambda_{DD}}{\lambda_D}MTTR \tag{4}$$

When redundant channels are considered, it is possible to adopt the β-model to take into account the effect of *CCF*s. Failures are partitioned into *CCF*s, with failure rate ${\lambda_D}^{(CCF)} = \beta\lambda_{DU} + \beta_D\lambda_{DD}$, and failures that affect an individual channel only, with failure rate:

$${\lambda_D}^{(i)} = (1-\beta)\lambda_{DU} + (1-\beta_D)\lambda_{DD} \tag{5}$$

The contribution of *CCF*s to the determination of *PFH* is determined by taking into account only *DU CCF*s, since when a *DD CCF* is detected, that channel is brought to a safe state to be restored. Hence:

$$PFH^{(CCF)} = \beta\lambda_{DU} \tag{6}$$

The contribution to *PFH* of failures that affect individual channels of a redundant architecture is shown, according to the architectures considered in § 2.1.1 and § 2.1.2, only for a 1-*out*-*of*-2 (1*oo*2) architecture (a two channel, redundant architecture in which at least one channel has to operate to perform the safety function). Since there are two channels, a *DD* or a *DU* failure can occur in one of the channels, with a channel-equivalent mean downtime t_{CE} and a global rate of $2{\lambda_D}^{(i)}$ (double that of a single channel). If the next failure is a *DD* failure, it is certainly detected and the function is restored within the *MTTR*, with a negligible likelihood of a request of the safety function leading to a hazardous event in this very short time interval. Thus, only a *DU* failure remains as the main contribution to *PFH*, with the probability of occurrence of such a second failure, within the time interval t_{CE}, equal to:

$$\Pr_{DU} = \left(1-e^{-(1-\beta)\lambda_{DU}t_{CE}}\right) \approx (1-\beta)\lambda_{DU}t_{CE}$$

Therefore, the contribution to *PFH* of individual failures is:

$$PFH^{(i)} = 2{\lambda_D}^{(i)}\cdot\Pr_{DU2}$$

and, adding the contribution of CCFs, one finally has:

$$PFH^{(1oo2)} = PFH^{(i)} + PFH^{(CCF)} = \\ = 2{\lambda_D}^{(i)}(1-\beta)\lambda_{DU}t_{CE} + \beta\lambda_{DU} \tag{7}$$

4.1 *PFH* determination of the *S-module*

The internal *Supply Unit* (*S-module*) is a single channel unit (fig. 10), composed of an internal power supply (PS) block (used to provide the robot motors with stabilized line voltages and the robot printed boards with suitable d.c. voltages) and a voltage monitor (VM) block (used to provide continuous supervision of the power supply circuit).

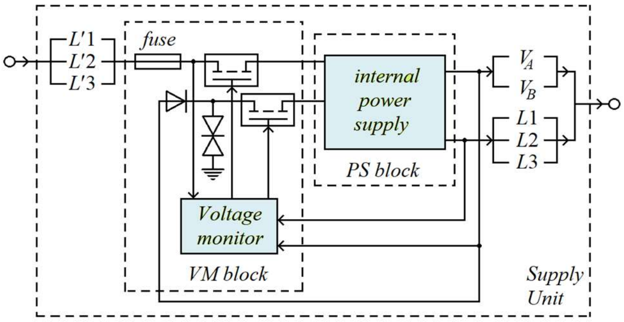


Fig. 10: Detail of the box "Supply Unit" (*S-module*) in fig. 9

The realization of the module is a type B subsystem with a *hardware fault tolerance* of 0 (single channel). According to tab. 4, for SIL 2 and *HFT*=0, the *SFF* must be at least 90%. A FMEA can determine whether the failure of an element is safe or dangerous for the block. Yet, for complex components, IEC 61508 [7], Part 6, Annex C, allows us to accept a simplified method, assuming a 50% portion of safe failures and a 50% portion of dangerous failures.

The diagnostic coverage *DC* can be roughly estimated by using the tables of IEC 61508 [7], Part 2, Annex A, (see tab. 6).

Table 6: Maximum diagnostic coverage of the *S-module*, achievable according to IEC 61508 [7], Part 2, Annex A

Diagnostic measure	DC level	Method adopted
IEC 61508-2, Table A.9, Voltage control (secondary) with safety shut-off or switch-over to second power unit	High (99%)	The voltage monitor powers down the robot system
IEC 61508-2, Table A.3, Hardware with automatic check	High (99%)	The voltage monitor has a self-diagnostic

According to tab. 6, it is possible to assume *DC*=99% for the PS block, and *DC*=99% for the VM block, which performs self-diagnostics.

The failure rates of the PS and VM blocks, based on realistic example values [8], are contained in tab. 7 (where 1 *fit* = 10^{-9} h^{-1}).

Table 7: Failure rates of the PS and VM blocks

Internal power supply (PS block)
$\lambda_{PS} = 250\ fit$
$\lambda_{PS\text{-}S} = \lambda_{PS\text{-}D} = 50\%\ \lambda_{PS} = 125\ fit$
$\lambda_{PS\text{-}DD} = DC\cdot\lambda_{PS\text{-}D} = 99\%\ \lambda_{PS\text{-}D} = 123{,}75\ fit$
$\lambda_{PS\text{-}DU} = (1–DC)\ \lambda_{PS\text{-}D} = 1\%\ \lambda_{PS\text{-}D} = 1{,}25\ fit$
Voltage monitor (VM block)
$\lambda_{VM} = 250\ fit$
$\lambda_{VM\text{-}S} = \lambda_{VM\text{-}D} = 50\%\ \lambda_{VM} = 125\ fit$
$\lambda_{VM\text{-}DD} = DC\cdot\lambda_{VM\text{-}D} = 99\%\ \lambda_{VM\text{-}D} = 123{,}75\ fit$
$\lambda_{VM\text{-}DU} = (1–DC)\ \lambda_{VM\text{-}D} = 1\%\ \lambda_{VM\text{-}D} = 1{,}25\ fit$

The *safe failure fraction*, according to (1), is:

$$SFF_S = \frac{\lambda_{PS\cdot S} + \lambda_{PS\cdot DD} + \lambda_{VM\cdot S} + \lambda_{VM\cdot DD}}{\lambda_{PS} + \lambda_{VM}} = 99{,}5\%$$

that is compliant with the previously identified constraint, obtained from tab. 4. The *CCF* factor is estimated by using IEC 61508 [7], Part 6, Annex D, as $\beta = 2\%$.

Safe failures have no influence on the *PFH* value and the system is switched off and repaired after detection of a failure. Therefore, the PFH_S can be determined as (where $\lambda_S = \min\{\lambda_{PS\cdot DU}, \lambda_{VM\cdot DU}\}$):

$$PFH_S = \lambda_{PS\cdot DU} + \lambda_{VM\cdot DU} - \beta \cdot \lambda_S = 2{,}475\ fit$$

4.2 *PFH* determination of the *C-module*

The *Safety-related part of control system* (*C-module*) is implemented with two channels (fig. 11), to achieve a *hardware fault tolerance* of 1. The module is a type B subsystem. According to tab. 4, for SIL 2 and *HFT*=1, the *SFF* must be at least 60%.

The *DC* can be estimated by using the tables of IEC 61508 [7], Part 2, Annex A, (see tab. 8).

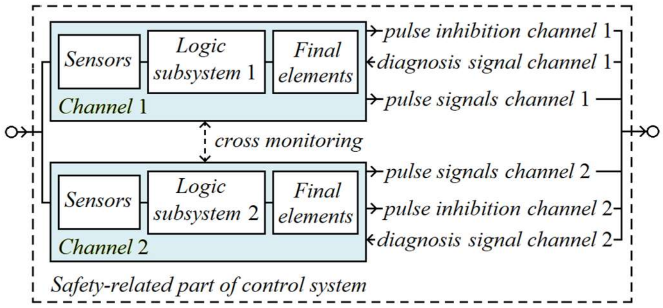


Fig. 11: Detail of the box "Safety-related part of control system" (*C-module*) in fig. 9

Table 8: Maximum diagnostic coverage of the *C-module*, achievable according to IEC 61508 [7], Part 2, Annex A

Diagnostic measure	DC level	Method adopted
IEC 61508-2, Table A.3, Failure detection by on-line monitoring	Medium (90%)	Cyclic test checks redundant channels
IEC 61508-2, Table A.3, Monitored redundancy	High (99%)	Cyclic test checks redundant channels
IEC 61508-2, Table A.4, self-test by software (walking bit) (one channel)	Medium (90%)	Self-test of the microprocessor
IEC 61508-2, Table A.6, RAM test "galpat"	High (99%)	Done by the microprocessor
IEC 61508-2, Table A.8, Inspection using test patterns	High (99%)	Done by RAM-test
IEC 61508-2, Table A.14, Cross monitoring of multiple actuators	High (99%)	Cyclic test monitors actuators

According to tab. 8, it is possible to assume *DC*=90% for both channels. The failure rates are contained in tab. 9 (1 *fit* = 10^{-9} h^{-1}).

Table 9: Failure rates of the Channel 1 and Channel 2 blocks

Channel 1 and Channel 2 blocks
$\lambda_C = 450$ *fit*
$\lambda_{C\text{-}S} = \lambda_{C\text{-}D} = 50\%\ \lambda_C = 225$ *fit*
$\lambda_{C\text{-}DD} = DC \cdot \lambda_{C\text{-}D} = 90\%\ \lambda_{C\text{-}D} = 202{,}5$ *fit*
$\lambda_{C\text{-}DU} = (1\text{–}DC)\ \lambda_{C\text{-}D} = 10\%\ \lambda_{C\text{-}D} = 22{,}5$ *fit*

The *safe failure fraction* $SFF_C = 95\%$ is compliant with the constraint obtained from tab. 4.
The *CCF* factor is estimated by using IEC 61508 [7], Part 6, Annex D, as $\beta = 2\%$. Safe failures have no influence on the *PFH* value and blocks are switched off and repaired after detection of a failure. Therefore, the PFH_C can be determined, according to (7), as:

$$PFH_C = 2\lambda_{C \cdot D}{}^{(i)}(1-\beta)\lambda_{C \cdot DU} t_{CE} + \beta\lambda_{C \cdot DU}$$

where $\lambda_D{}^{(i)} = (1-\beta)\lambda_{C \cdot DU} + (1-\beta_D)\lambda_{C \cdot DD}$. The results of the PFH_C value calculation, for $\tau = 8760$ h, $MRT = 8$ h, $\beta_D = 0{,}5\beta$ and different values of the τ_{test} parameter, are reported on tab. 10.

Table 10: PFH_C for different values of the τ_{test} parameter

τ_{test}	PFH_C
8 h	0,454 *fit*
24 h (1 day)	0,454 *fit*
168 h (7 days)	0,455 *fit*
720 h (1 month = 30 days)	0,458 *fit*
2160 h (3 months = 90 days)	0,464 *fit*
8760 h (1 year = 365 days)	0,493 *fit*

4.3 *PFH* determination of the *P-module*

The *Robot power module and joint motors* (*P-module*) is a single channel unit (fig. 12). Its realization is a type B subsystem with a *hardware fault tolerance* of 0. According to tab. 4, for SIL 2 and *HFT*=0, the *SFF* must be at least 90%.
The *DC* can be estimated by using the tables of IEC 61508 [7], Part 2, Annex A, (see tab. 11).

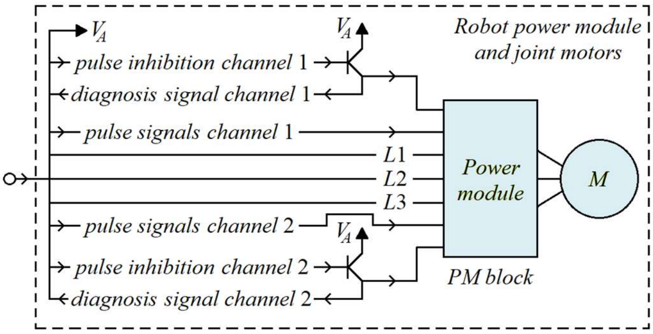


Fig. 12: Detail of the box "Robot power module and joint motors" (*P-module*) in fig. 9

Table 11: Maximum diagnostic coverage of the *P-module*, achievable according to IEC 61508 [7], Part 2, Annex A

Diagnostic measure	**DC level**	**Method adopted**
IEC 61508-2, Tables A.2, A.3, A.14, Failure detection by on-line monitoring	Medium (90%)	Cyclic test checks redundant channels
IEC 61508-2, Table A.14, Cross monitoring of multiple actuators	High (99%)	Cyclic test monitors actuators

According to tab. 11, it is possible to assume *DC*=90%. The failure rates are contained in tab. 12 (1 *fit* = 10^{-9} h^{-1}).

Table 12: Failure rates of the *P-module*

Power module (PM block)
$\lambda_{PM} = 520$ *fit*
$\lambda_{PM\text{-}S} = \lambda_{PM\text{-}D} = 50\%\ \lambda_{PM} = 260$ *fit*
$\lambda_{PM\text{-}DD} = DC \cdot \lambda_{PM\text{-}D} = 90\%\ \lambda_{PM\text{-}D} = 234$ *fit*
$\lambda_{PM\text{-}DU} = (1\text{–}DC)\ \lambda_{PM\text{-}D} = 10\%\ \lambda_{PM\text{-}D} = 26$ *fit*
Joint motors (M block)
$\lambda_M = 70$ *fit*
$\lambda_{M\text{-}S} = \lambda_{M\text{-}D} = 50\%\ \lambda_M = 35$ *fit*
$\lambda_{M\text{-}DD} = DC \cdot \lambda_{M\text{-}D} = 90\%\ \lambda_{M\text{-}D} = 31{,}5$ *fit*
$\lambda_{M\text{-}DU} = (1\text{–}DC)\ \lambda_{M\text{-}D} = 10\%\ \lambda_{M\text{-}D} = 3{,}5$ *fit*

The *safe failure fraction* $SFF_P = 95\%$ is compliant with the constraint obtained from tab. 4.
The *CCF* factor is estimated by using IEC 61508 [7], Part 6, Annex D, as $\beta = 2\%$.
The PFH_P can be determined as:

$$PFH_P = \lambda_{PM \cdot DU} + \lambda_{M \cdot DU} - \beta \cdot \lambda_P = 29{,}43\, fit$$

where $\lambda_P = \min\{\lambda_{PM \cdot DU}, \lambda_{M \cdot DU}\}$.

4.4 Overall function *PFH* determination

The results of the *PFH* value of the overall function (2), for different values of the τ_{test} parameter, compliant with SIL 2 or higher, are shown in tab. 13.

Table 13: *PFH* for different values of the τ_{test} parameter

τ_{test}	*PFH*
8 h	32,36 *fit*
24 h (1 day)	32,36 *fit*
168 h (7 days)	32,36 *fit*
720 h (1 month = 30 days)	32,36 *fit*
2160 h (3 months = 90 days)	32,37 *fit*
8760 h (1 year = 365 days)	32,40 *fit*

5 Discussion

Usually, reliability and availability of industrial robots are faced from the point of view of productivity and accomplishment of tasks [10–12, 18]. Collaborative applications need planning of tasks [14], risk assessment [17], and a safe layout design [15, 16]. However, an example of a method to conduct a functional safety analysis of a specific safety function for collaborative applications (namely the *safety-rated monitored stop*), as shown in § 4, is still not available in the literature. The method proposed, resumed in §§ 3 and 4, follows the suggestions contained in the standard IEC 61508 [7]. Future developments are possible by considering other collaborative operation types, other kinds of actuators (pneumatic, hydraulic) and/or specific applications.

6 Conclusion

The possibility of carrying out tasks in a collaborative way allows us to improve the performance characteristics and the efficiency with which the robot cell completes the assigned work. If the task is well designed, the capabilities of the operator complement those of the robot, making the robot cell more versatile and adaptive. However, since during a collaborative act the robot and the operator share the same workspace, there is still a non-negligible risk of impact. The risk can be reduced with an intrinsically safe design or with the use of safety functions, in accordance with the applicable standards [1–3].
These standards require that the safety functions implemented must comply with the performance requirements illustrated in § 2.1.1, which translate into specific architectural constraints, as shown in § 2.1.2.
A method to conduct a functional safety analysis of a typical safety function for collaborative applications (namely the *safety-rated monitored stop*), based on IEC 61508 [7], has been proposed in §§ 3 and 4. In § 4, the application of the method is depicted as an example, which shows how a safety reliability model can be used by system designers and integrators to certify the achievement of the required safety objectives for the chosen safety function.

References:

[1] ISO 10218-1: Robots and robotic devices – Safety requirements for industrial robots – Part 1: Robots, 2011.
[2] ISO 10218-2: Robots and robotic devices – Safety requirements for industrial robots – Part 2: Robot systems and integration, 2011.
[3] ISO/TS 15066: Robots and robotic devices – Collaborative robots, 2016.
[4] IEC 60204-1: Safety of machinery – Electrical equipment of machines – Part 1: General requirements, 2016.
[5] ISO 13849-1: Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design, 2015.
[6] IEC 62061: Safety of machinery – Functional safety of safety-related control systems, 2021
[7] IEC 61508: Functional safety of electrical/ electronic/programmable electronic safety–related systems (Parts 1–7), 2010.
[8] IEC 61800-5-2: Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional, 2016.
[9] M. Rausand, *Reliability of safety-critical systems – Theory and applications*, John Wiley & Sons, Inc., 2014.
[10] B. S. Dhillon, *Robot system reliability and safety: A modern approach*. CRC Press, Taylor & Francis Group, 2015.
[11] A. Kumar, S. P. Sharma, D. Kumar, Robot reliability using Petri nets and fuzzy lambda–tau (λ–τ) methodology, *3rd Int. Conf. on Reliability and Safety Eng.*, 2007.
[12] A. F. Fudzin, M. A. A. Majid, Reliability and availability analysis for robot subsystem in automotive assembly plant: a case study, *IOP Conf. Ser.: Mater. Sci. Eng.* 100, 2015.
[13] V. Villani, F. Pini, F. Leali, C. Secchi, Survey on human–robot collaboration in industrial settings: Safety, intuitive interfaces and applications, *Mechatronics*, Vol. 55, November 2018, pp. 248–266.
[14] A. Djuric, R. Urbanic, J. Rickli, A Framework for Collaborative Robot (CoBot) Integration in Advanced Manufacturing Systems, *SAE Int. J. Mater. Manf.* 9(2), 2016, pp. 457–464.
[15] V. Gopinath, F. Oreb, K. Johansen, Safe assembly cell layout through risk assessment – An application with hand guided industrial robot, *Procedia CIRP* 63, 2017, pp. 430–435.
[16] P. Wadekar, V. Gopinath, K. Johansen, Safe layout design and evaluation of a human-robot collaborative application cell through risk assessment – A computer aided approach, *Procedia Manufacturing* 25, 2018, pp. 602–611.
[17] L. Poot, K. Johansen, V. Gopinath, Supporting risk assessment of human-robot collaborative production layouts: a proposed design automation framework, *Procedia Manufactu-ring* 25, 2018, pp. 543–548.
[18] A. Kampa. The Review of Reliability Factors Related to Industrial Robots, *Robot Autom. Eng. J.* 3(5), 2018, pp. 145–149.
[19] C. S. Franklin, E. G. Dominguez, J. D. Fryman, M. L. Lewandowski, Collaborative robotics: New era of human–robot cooperation in the workplace, *Journal of Safety Research* 74, 2020, pp. 153–160.