PD ISO/TR 24119:2015

BSI Standards Publication

Safety of machinery — Evaluation of fault masking serial connection of interlocking devices associated with guards with potential free contacts

bsi.

...making excellence a habit.™

National foreword

This Published Document is the UK implementation of ISO/TR 24119:2015.

The UK participation in its preparation was entrusted to Technical Committee MCE/3, Safeguarding of machinery.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2015

ISBN 978 0 580 86043 0
ICS 13.110

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 November 2015.

Amendments/corrigenda issued since publication

Date	Text affected

PD ISO/TR 24119:2015

TECHNICAL REPORT

ISO/TR 24119

First edition
2015-11-15

Safety of machinery — Evaluation of fault masking serial connection of interlocking devices associated with guards with potential free contacts

Sécurité des machines — Évaluation du masquage de fautes dans les connexions en série des dispositifs d'interverrouillage associés aux contacts sans potentiel

Reference number
ISO/TR 24119:2015(E)

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/TC 199, *Safety of machinery*.

Safety of machinery — Evaluation of fault masking serial connection of interlocking devices associated with guards with potential free contacts

1 Scope

This Technical Report illustrates and explains principles of fault masking in applications where multiple interlocking devices with potential free contacts (B1 to Bn) are connected in series to one logic unit (K) which does the diagnostics (see Figures 1 to 7). It further provides a guide how to estimate the probability of fault masking and the maximum DC for the involved interlocking devices. This Technical Report only covers interlocking devices in which both channels are physical serial connections.

This Technical Report does not replace the use of any standards for the safety of machinery.

The goals of this Technical Report are the following:

— guidance for users for estimation of the maximum DC values;

— design guidance for SRP/CS.

NOTE 1 Interlocking devices with integrated self-monitoring are not included in the scope of this Technical Report.

NOTE 2 Limitation is also given by the diagnostic means implemented in the logic unit.

NOTE 3 This Technical Report is not restricted to mechanical actuated position sensors.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 12100, *Safety of machinery — General principles for design — Risk assessment and risk reduction*

ISO 13849-1:2006, *Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design*

ISO 14119:2013, *Safety of machinery — Interlocking devices associated with guards — Principles for design and selection*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 12100, ISO 13849-1, ISO 14119 and the following apply.

3.1
fault masking
unintended resetting of faults or preventing the detection of faults in the SRP/CS by operation of parts of the SRP/CS which do not have faults

3.2
series connected devices
devices with potential free contacts (B1 to Bn) are connected in series to one logic unit (K) which does the diagnostics

3.3
signal evaluation of redundant channels with same polarity
technique where the logic unit of the safety function evaluates redundant signals which have the same supply voltage

3.4
signal evaluation of redundant channels with inverse polarity
technique where the logic unit of the safety function evaluates redundant signals in which the second channel has the ground polarity

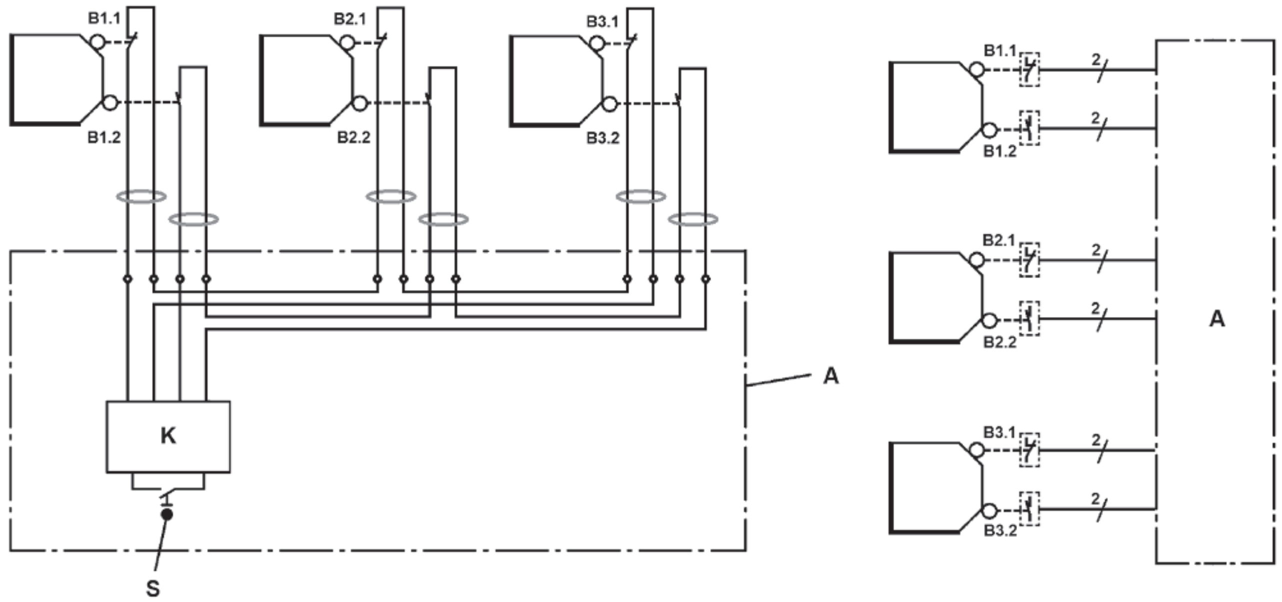
Note 1 to entry: See IEC 60204-1:2005, 9.4.3.1, method a).

3.5
signal evaluation of redundant channels with dynamic signals
technique where the logic unit of the safety function evaluates redundant dynamic signals

Note 1 to entry: Dynamic signals can be generated with test pulses, frequency modulation, etc.

3.6
star cabling
cabling structure where every interlocking device is wired with a single cable to the electric cabinet or enclosure

Note 1 to entry: Figure 1 shows a star cabling.



Key

A electrical cabinet

B1.1, B1.2,
B2.1, B2.2, interlocking devices with potential free contacts
B3.1, B3.2

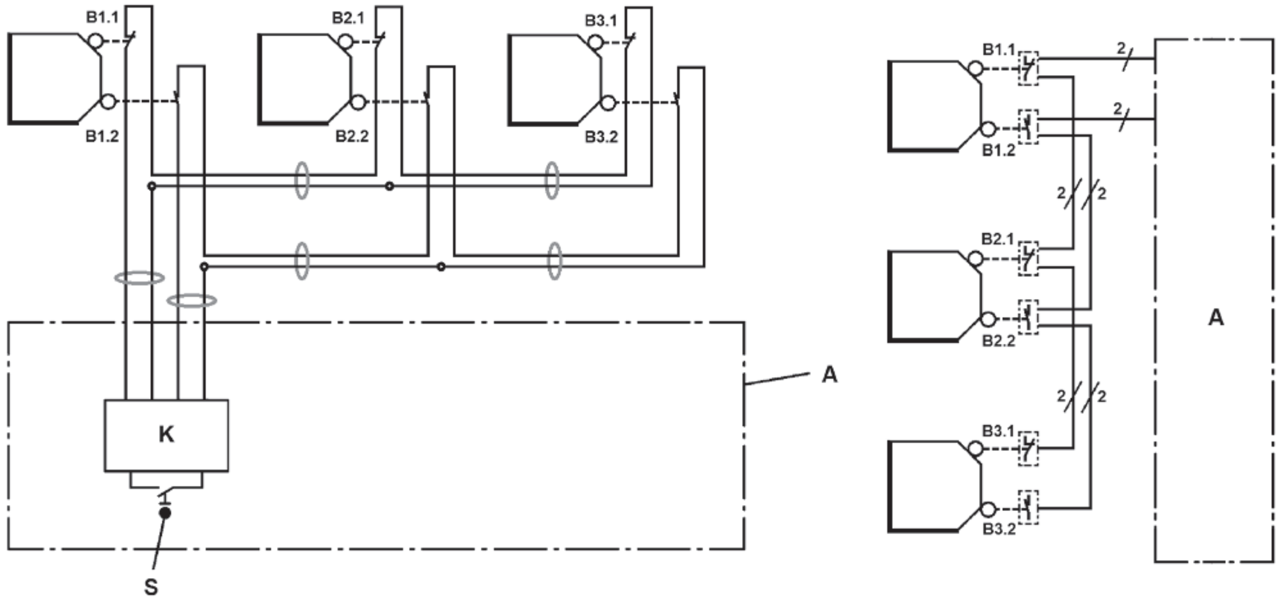
K logic unit

S manual reset function reset device

Figure 1 — Star cabling

3.7
branch cabling
trunk cabling
cabling structure where a single cable from the electric cabinet is wired to the first interlocking device and from this interlocking device to the next, and so on, until the last interlocking devices and the resulting signals are wired the same way back to the electric cabinet

Note 1 to entry: Figure 2 shows a branch (trunk) cabling.



Key

A electrical cabinet

B1.1, B1.2, B2.1, B2.2, B3.1, B3.2 interlocking devices with potential free contacts

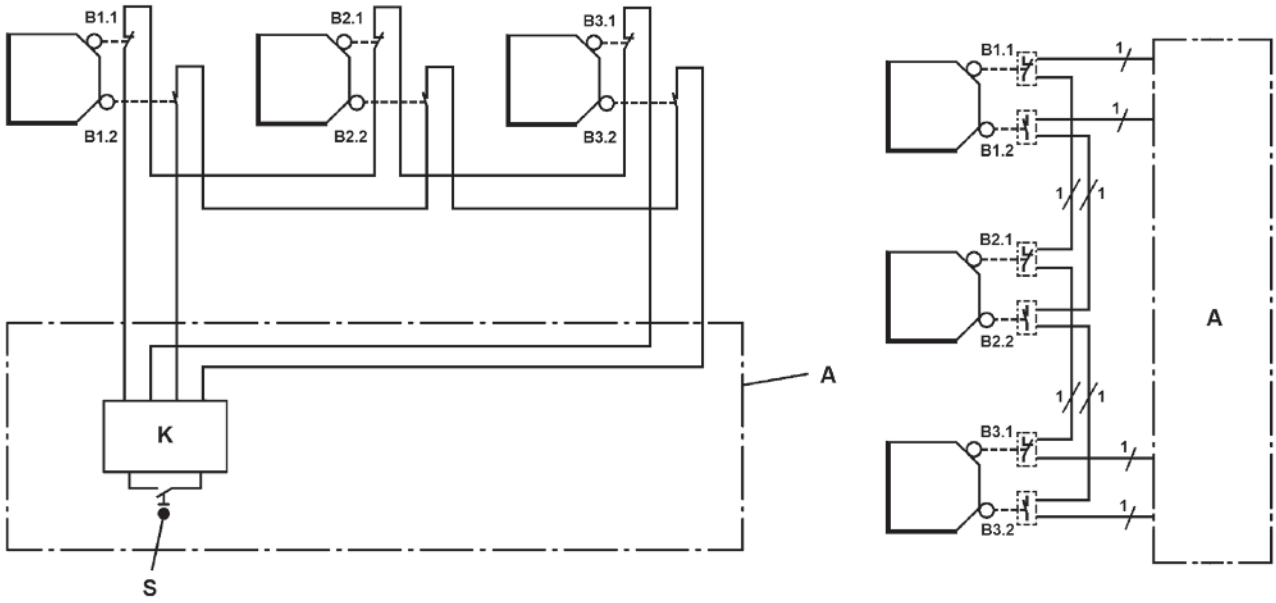
K logic unit

S manual reset function reset device

Figure 2 — Branch (trunk) cabling

3.8
loop cabling
cabling structure where a single cable from the electric cabinet is wired to the first interlocking device and from this interlocking devices to the next, and so on, until the last interlocking device while the signals return to the electric cabinet in a separate cable

Note 1 to entry: Figure 3 shows a loop cabling.



Key

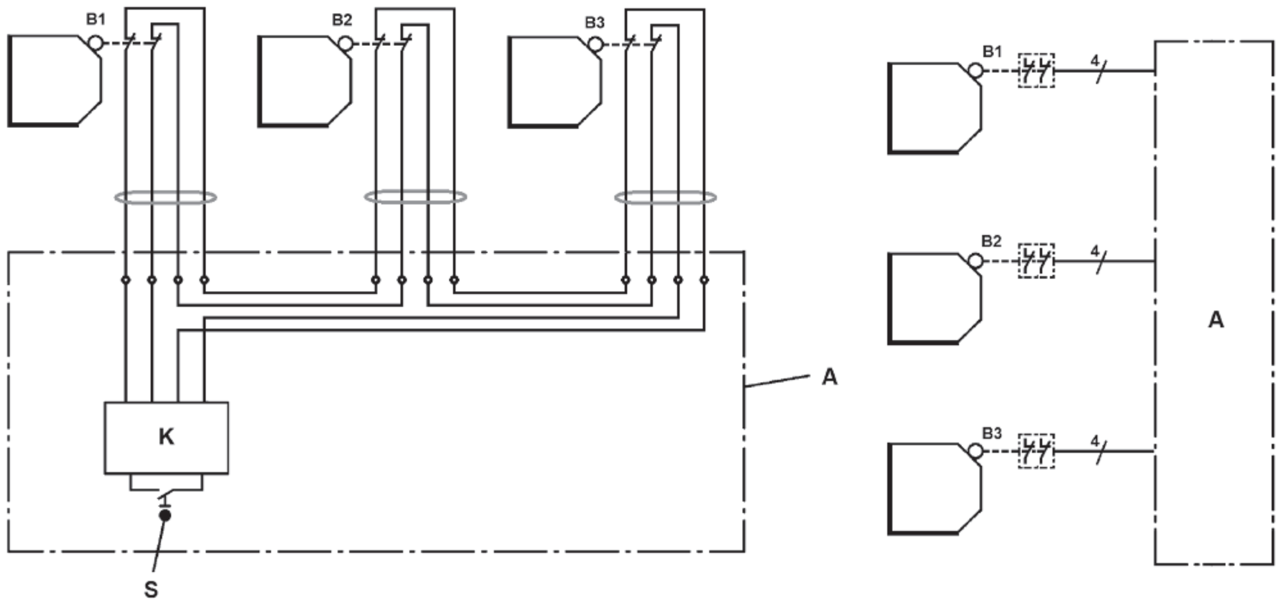
A	electrical cabinet
B1.1, B1.2, B2.1, B2.2, B3.1, B3.2	interlocking devices with potential free contacts
K	logic unit
S	manual reset function reset device

Figure 3 — Loop cabling

3.9
single arrangement

application of two different contacts of a single interlocking device in the redundant channels of an interlocking circuit for a single guard interlocking

Note 1 to entry: Figure 4 shows a single arrangement.



Key

A	electrical cabinet
B1, B2, B3	interlocking devices with potential free contacts
K	logic unit
S	manual reset function reset device

Figure 4 — Single arrangement

3.10
redundant arrangement
application of single contacts of two (redundant) interlocking devices in the redundant channels of an interlocking circuit for a single guard interlocking

Note 1 to entry: Figures 1 to 3 show redundant arrangements.

3.11
protected cabling
cabling which is permanently connected (fixed) and protected against external damage, e.g. by cable ducting, armoring, or within an electrical enclosure according to IEC 60204-1

4 Fault masking

4.1 General

A common approach in the design of safety related circuits is to series connect devices with potential free contacts, e.g. multiple interlocking devices connected to a single safety logic controller which performs the diagnostics for the overall safety function. Although in such applications a single fault will, in most cases, not lead to the loss of the safety function and will be detected, in practice, problems sometimes occur.

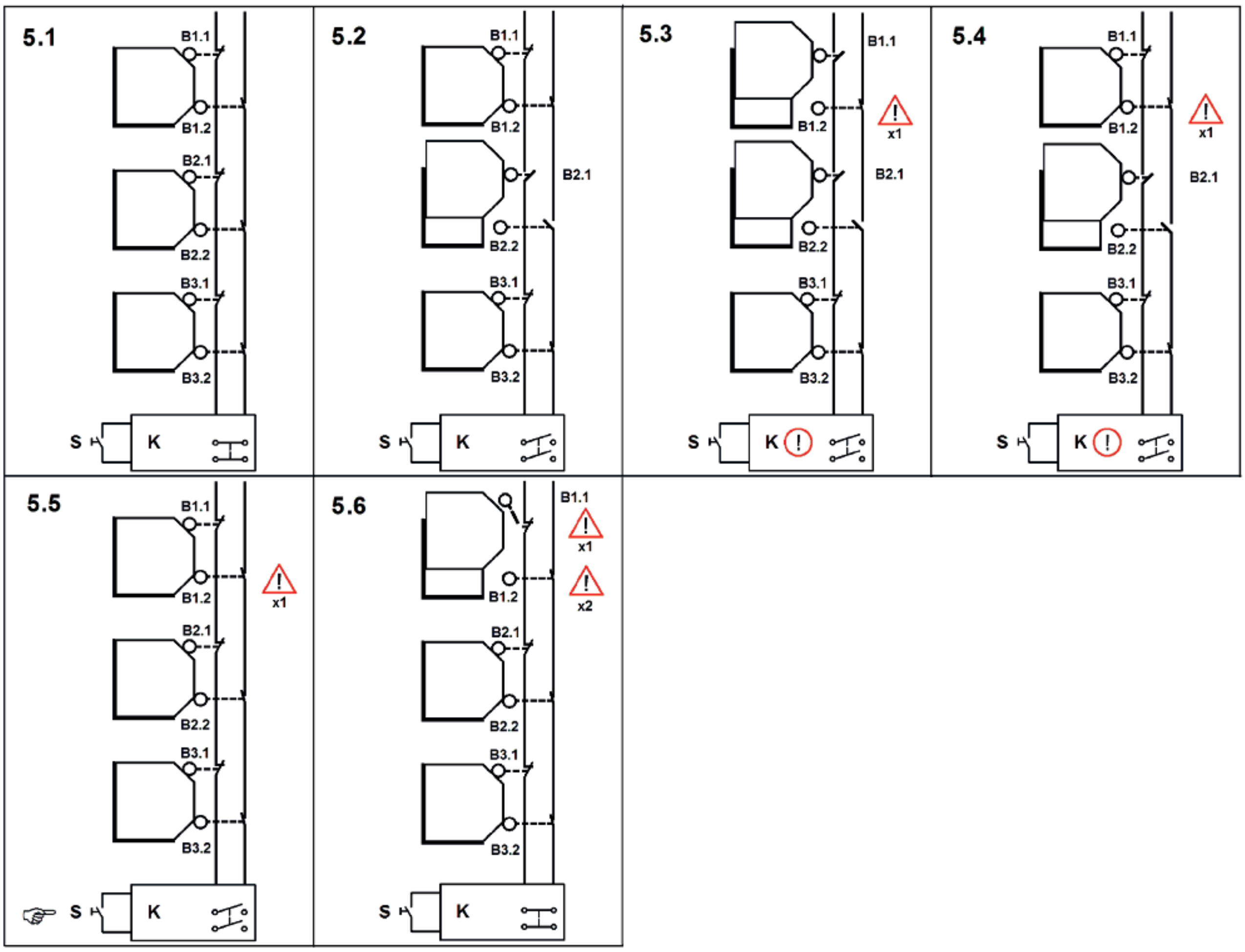
It is foreseeable that more than one movable guard will be open at the same time or in a sequence, e.g. due to subsequent fault finding procedure or as part of the regular operation of the machine.

Due to the serial connection of the contacts, faults in the wiring or contacts detected by the logic unit may be masked by the operation of one of the other (non-faulty) in series connected devices. As a result, the operation of the machine is possible while a single fault is present in the SRP/CS. This can, in consequence, allow the accumulation of faults leading to an unsafe system.

Figures 5 to 7 show examples for fault masking in situations with movable guards with series connected interlocking devices.

4.2 Direct fault masking

Figure 5 shows a situation where two movable guards actuated in a specific sequence can lead to fault masking.



Key

B1, B2, B3 interlocking devices with potential free contacts

K logic unit

S manual reset function reset device

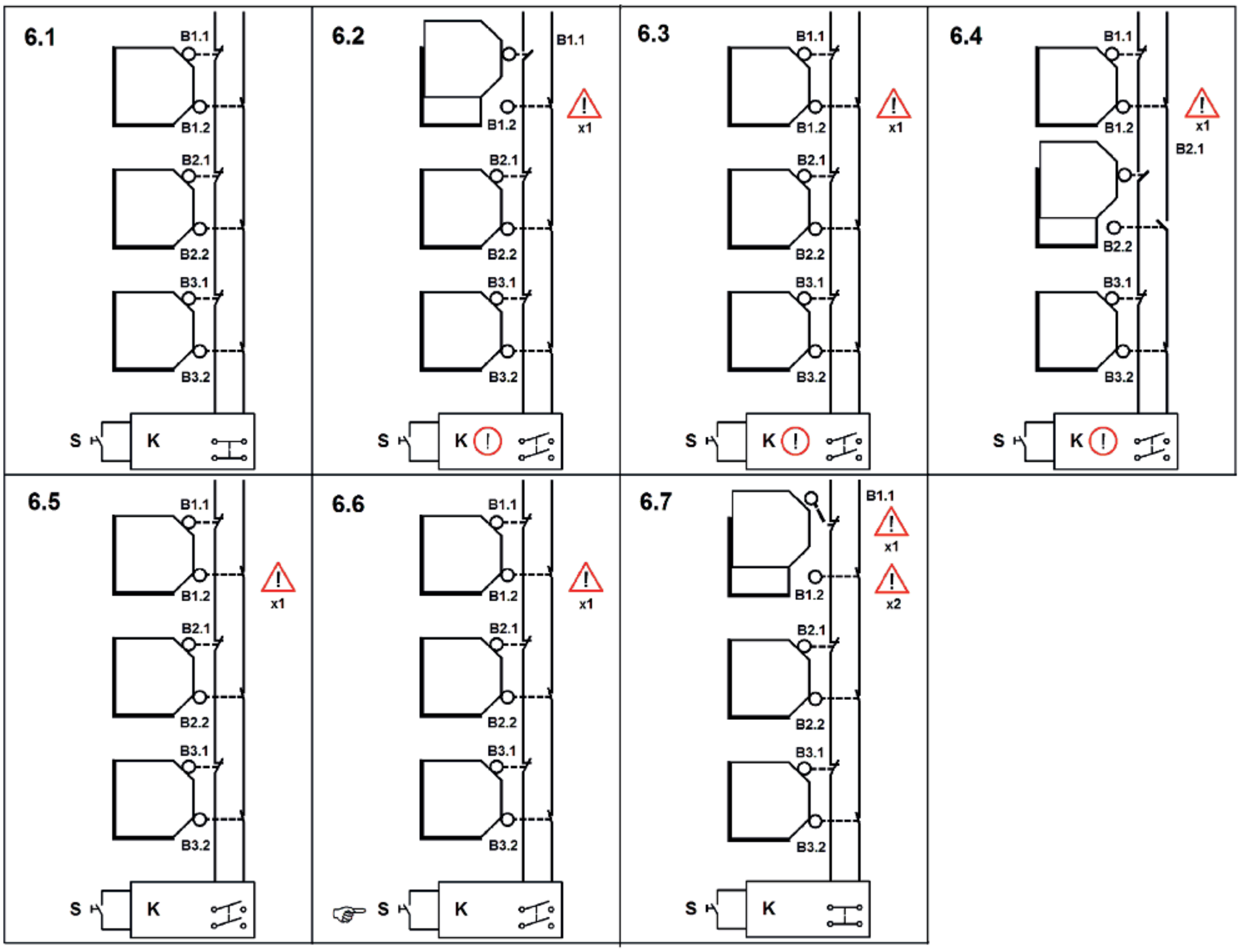
x1 initial fault – contact fails to open

x2 second fault – broken switch lever

Figure 5 — Direct fault masking

4.3 Unintended reset of the fault

Figure 6 shows a situation where a fault in one interlocking device is initially detected but then is reset unintentionally by operation of one of the other interlocking devices.



Key

B1, B2, B3 interlocking devices with potential free contacts

K logic unit

S manual reset function reset device

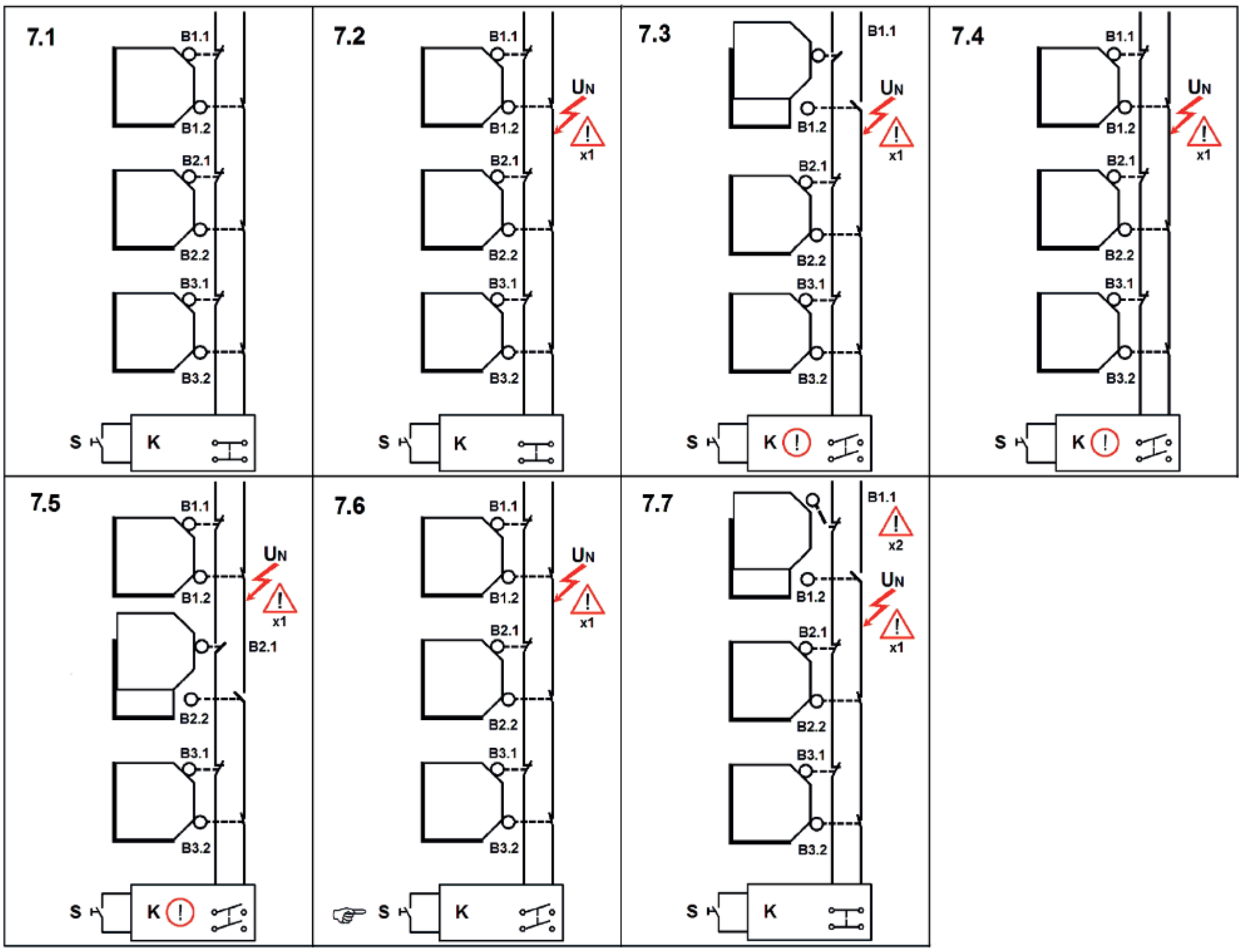
x1 initial fault – contact fails to open

x2 second fault – broken switch lever

Figure 6 — Unintended reset of the fault

4.4 Cable fault with unintended reset

Figure 7 shows a situation where a fault in the cabling is initially detected but then is reset unintentionally by operation of one of the other interlocking devices.



Key

B1, B2, B3	interlocking devices with potential free contacts
K	logic unit
S	manual reset function reset device
x1	initial fault – short circuit to Un
x2	second fault – broken switch lever
Un	nominal voltage of the channel

Figure 7 — Cable fault with unintended reset

5 Methodology for evaluation of DC for series connected interlocking devices

Step 1: Determine DC (see ISO 13849-1:2006, Annex E) of every single position switch which is a part of the safety function(s).

Step 2: Improve the resistance to fault masking if required by enhancing the design or changing the diagnostic method (refer to Clauses 6 and 7 and ISO 13849-2:2012, Annex D).

— Improve diagnostic coverage using a different diagnostic measure (see ISO 13849-1:2006, Annex E).

— Improve cabling in order to reduce fault possibilities or to allow fault exclusion.

— Select other type of interlocking device in order to allow fault exclusion.

Step 3: Limit the DC of the position switch to the maximum achievable DC by applying one of the methods given in Clause 6.

Step 4: Improve DC if required according to Clause 7.

6 Limitation of DC by effects of series connected devices

6.1 General

According to ISO 14119:2013, 8.6, with respect to serial wiring of contacts (without additional diagnostics), the effect of possible fault masking should be carefully taken into consideration.

Possible fault masking may lead to a fault accumulation, therefore, the maximum achievable DC should be estimated using one of the methods described in 6.2 and 6.3. The maximum achievable PL is limited to PL d and the maximum DC is limited to medium.

NOTE The probability of occurrence of faults due to random and systematic failures cannot be fully known. Therefore, any degradation of the diagnostics function will result in an increased probability of dangerous failures. This is not acceptable for higher levels of risk therefore PL and DC is limited.

6.2 Simplified method for the determination of the maximum achievable DC

Table 1 provides a simplified approach for the determination of the maximum achievable DC taking into account the probability of masking. If the maximum achievable DC resulting from the application of this table does not meet the required level the more detailed approach given in 6.3 may be more suitable.

Table 1 — Maximum achievable DC (simplified)

Number of frequently used movable guards[a][b]	Number of additional movable guards[c]	Maximum achievable DC[d]
0	2 to 4	Medium
	5 to 30	Low
	>30	None
1	1	Medium
	2 to 4	Low
	≥5	None
>1	≥0	None

[a] If the frequency is higher than once per hour.

[b] If the number of operators capable of opening separate guards exceeds one then the number of frequently used movable guards is increased by one.

[c] The number of additional movable guards may be reduced by one if one of the following conditions are met

— when the minimum distance between any of the guards is more than 5 m or

— when none of the additional movable guards is directly reachable.

[d] In any case, if it is foreseeable that fault masking will occur (e.g. multiple movable guards will be open at the same time as part of normal operation or service), then the DC is limited to none.

6.3 Regular method for the determination of the maximum achievable DC

6.3.1 Estimation of the fault masking probability

The probability of fault masking is dependent on several parameters that should be considered including:

— number of series connected devices;

— actuation frequency of each movable guard;

— distance between the movable guards;

— accessibility of the movable guards;

— number of operators.

To estimate the fault masking probability the following Table 2 applies and shows the fault masking probability level (FM).

Table 2 — Fault masking probability

Number of frequently used movable guards[a][b]	Number of additional movable guards[c]	Fault masking probability level (FM)[d]
0	2 to 4	1
	5 to 30	2
	>30	3
1	1	1
	2 to 4	2
	≥5	3
>1	≥0	3

a If the frequency is higher than once per hour.

b If the number of operators who are capable of opening separate guards exceeds one, then the number of frequently used movable guards is increased by one.

c The number of additional movable guards may be reduced by one if one of the following conditions are met

— when the minimum distance between any of the guards is more than 5 m or

— when none of the additional movable guards is directly reachable.

d In any case, if it is foreseeable that fault masking will occur (e.g. multiple movable guards will be open at the same time as part of normal operation or service), then the fault masking probability level (FM) is 3.

6.3.2 Determination of the maximum achievable DC

The maximum achievable DC depends on the fault masking probability level (FM) and the type of cabling used in combination with the switch arrangement and the diagnostic capabilities of the overall system to detect faults. Tables 3 to 5 show the maximum reachable DC depending on those parameters. In any case, if it is foreseeable that fault masking will occur (e.g. multiple movable guards will be open at the same time as part of normal operation or service) then the DC is limited to none.

Different types of switches are not taken into account in Tables 3 to 5 because they can be evaluated using their $MTTF_d$ value and the DC according to ISO 13849-1 and limiting DC to the range given in the Tables 3 to 5.

Table 3 — Maximum achievable DC for unprotected multicore cable without positive (+U) voltage wire

Unprotected multicore cable without positive (+U) voltage wire					
position switch arrangement	cabling	Signal evaluation of redundant channels with	Maximum achievable DC		
			FM = 3	FM = 2	FM = 1
single arrangement	Branch/ Star	same polarity (+U / +U)	none	low	medium
		inverse polarity (+U / GND)	none	low	medium
		dynamic signals	none	low	medium
	Loop	same polarity (+U / +U)	none	low	medium
		inverse polarity (+U / GND)	none	low	medium
		dynamic signals	medium	medium	medium
redundant arrangement	Branch/ Star	same polarity (+U / +U)	none	low	medium
		inverse polarity (+U / GND)	none	low	medium
		dynamic signals	none	low	medium
	Loop	same polarity (+U / +U)	medium	medium	medium
		inverse polarity (+U / GND)	none	low	medium
		dynamic signals	medium	medium	medium

Table 4 — Maximum achievable DC for unprotected multicore cable with positive (+U) voltage wire

Unprotected multicore cable with positive (+U) voltage wire					
position switch arrangement	cabling	Signal evaluation of redundant channels with	Maximum achievable DC		
			FM = 3	FM = 2	FM = 1
single arrangement	Branch/ Star	same polarity (+U / +U)	none	low	medium
		inverse polarity (+U / GND)	none	low	medium
		dynamic signals	low	medium	Medium
	Loop	same polarity (+U / +U)	none	low	medium
		inverse polarity (+U / GND)	none	low	medium
		dynamic signals	medium	medium	medium

Table 4 *(continued)*

Unprotected multicore cable with positive (+U) voltage wire					
position switch arrangement	cabling	Signal evaluation of redundant channels with	Maximum achievable DC		
			FM = 3	FM = 2	FM = 1
redundant arrangement	Branch/ Star	same polarity (+U / +U)	none	low	medium
		inverse polarity (+U / GND)	none	low	medium
		dynamic signals	low	medium	medium
	Loop	same polarity (+U / +U)	none	low	medium
		inverse polarity (+U / GND)	none	low	medium
		dynamic signals	medium	medium	medium

Table 5 — Maximum achievable DC for protected multicore cable with or without positive (+U) voltage wire

Protected multicore cable with or without positive (+U) voltage wire					
position switch arrangement	cabling	Signal evaluation of redundant channels with	Maximum achievable DC		
			FM = 3	FM = 2	FM = 1
single arrangement	Branch/ Star	same polarity (+U / +U)	medium	medium	medium
		inverse polarity (+U / GND)	none	low	medium
		dynamic signals	medium	medium	medium
	Loop	same polarity (+U / +U)	medium	medium	medium
		inverse polarity (+U / GND)	none	low	medium
		dynamic signals	medium	medium	medium
redundant arrangement	Branch/ Star	same polarity (+U / +U)	medium	medium	medium
		inverse polarity (+U / GND)	none	low	medium
		dynamic signals	medium	medium	medium
	Loop	same polarity (+U / +U)	medium	medium	medium
		inverse polarity (+U / GND)	none	low	medium
		dynamic signals	medium	medium	medium

6.4 Interlocking devices with potential free contacts and other potential free contacts of devices with different functionality connected in series

Fault masking can occur even if the other contacts are non-safety related, e.g. the operation of series connected devices containing a non-safety related limit switch within a safety related circuit.

In such cases, the probability of fault masking cannot be estimated with the methods of this Technical Report and therefore the DC should be considered as none.

7 Avoiding fault masking

To avoid fault masking of interlocking devices with potential free contacts, the following methods can be applied:

— use additional contacts individually connected to a monitoring device in combination with appropriate diagnostic procedures to avoid fault masking;

— avoid connecting in series of interlocking devices and use individual safety inputs for each interlocking device;

— use interlocking devices with internal diagnostics and monitored outputs.

Other methods can be possible.

Annex A
(informative)

Examples of the application of the evaluation methods described in 6.2 and 6.3

A.1 Application in an integrated manufacturing system

Figure A.1 shows an integrated manufacturing system with a perimeter guard. This guard also includes several interlocked movable guards (doors A, B, C, D, F) and a material entry exit area safeguarded with an (AOPD) active optoelectronic protective device (E).

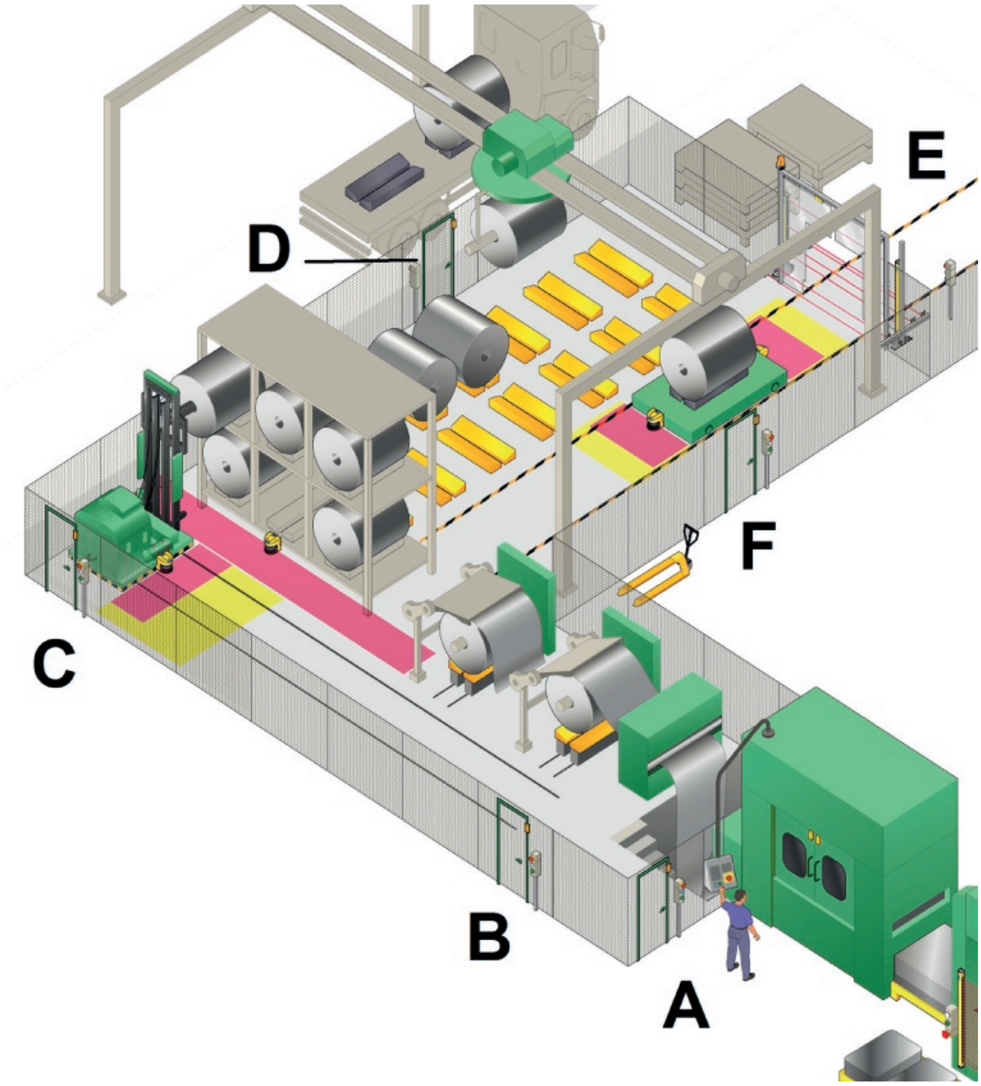


Figure A.1 — Integrated manufacturing system with several interlocked movable guards

A.2 Application Example 1

The following is assumed (see Figure A.1):

— the interlocking devices have dual potential free contacts (1 sensor with 2 NC contacts);

— the contacts will open when the movable guard is opened;

— the contacts are connected in series to a logic unit which evaluates both channels;

— the interlocking devices are cabled in a loop to the main cabinet;

— the cabling is not protected against external damage;

— the interlocked movable guard at "A" will be opened regularly (10x/day) due to functional reasons (loading the trailing edge of a new coil);

— the other movable guards (B, C, D, F) will be opened seldom (10x/year);

— only one operator is required to operate the system and therefore no other persons may directly interact with the IMS.

If the method explained in 6.3 is applied to determine the maximum achievable DC, then:

According to Table 2, the following applies:

— Number of frequently used movable guards = 1

No increasing due to Table 2, footnote b;

— Number of additional (others, not frequently used guards) = 4

No decreasing due to Table 2, footnote c, since B is considered as easily reachable.

The resulting fault masking probability level is = 2.

According to Table 3, the following applies:

— For a signal evaluation which uses static signals with same or inverse polarity, the maximum achievable DC is "low" and therefore the achievable PL of the interlocking function depends on the $MTTF_d$ values (derived from $B10_d$ values) of the incorporated position sensors but limited to PL d according to ISO 13849-1;

— For a signal evaluation which uses dynamic signals, the maximum achievable DC is "medium" and therefore the achievable PL of the interlocking function depends on the $MTTF_d$ values (derived from $B10_d$ values) of the incorporated position sensors. This may even reach PL e according to ISO 13849-1 but is limited to PL d (see 6.1).

Otherwise, if the method explained in 6.2 is applied to determine the maximum achievable DC, then:

According to Table 1 the following applies:

— Number of frequently used movable guards = 1

No increasing due to Table 1, footnote b;

— Number of additional (others, not frequently used guards) = 4

No decreasing due to Table 1, footnote c, since B is considered as easily reachable.

The resulting maximum achievable DC is limited to "low", despite how the interlocking devices are cabled and their signals evaluated.

If it is foreseeable that the operator will use other movable guards to leave the safeguarded area than he will use to access, the DC is "none" according Table 1, footnote d, if the method according 6.3 is used, the number of frequently operated movable guards is obviously >1.

A.3 Application Example 2

The following is assumed (see Figure A.2):

— the interlocking devices have dual potential free contacts (1 sensor with 2 NC contacts);

— the contacts will open when the movable guard is opened;

— the contacts are connected in series to a logic unit which evaluates both channels;

— the interlocking devices are cabled in a loop to the main cabinet;

— the cabling is not protected against external damage;

— the interlocked movable guard at "A" will be opened regularly (10x/day) due to functional reasons (loading the trailing edge of a new coil);

— the other movable guards (C, D, F) will be opened seldom (10x/year);

— more than one operator is required to operate the system.

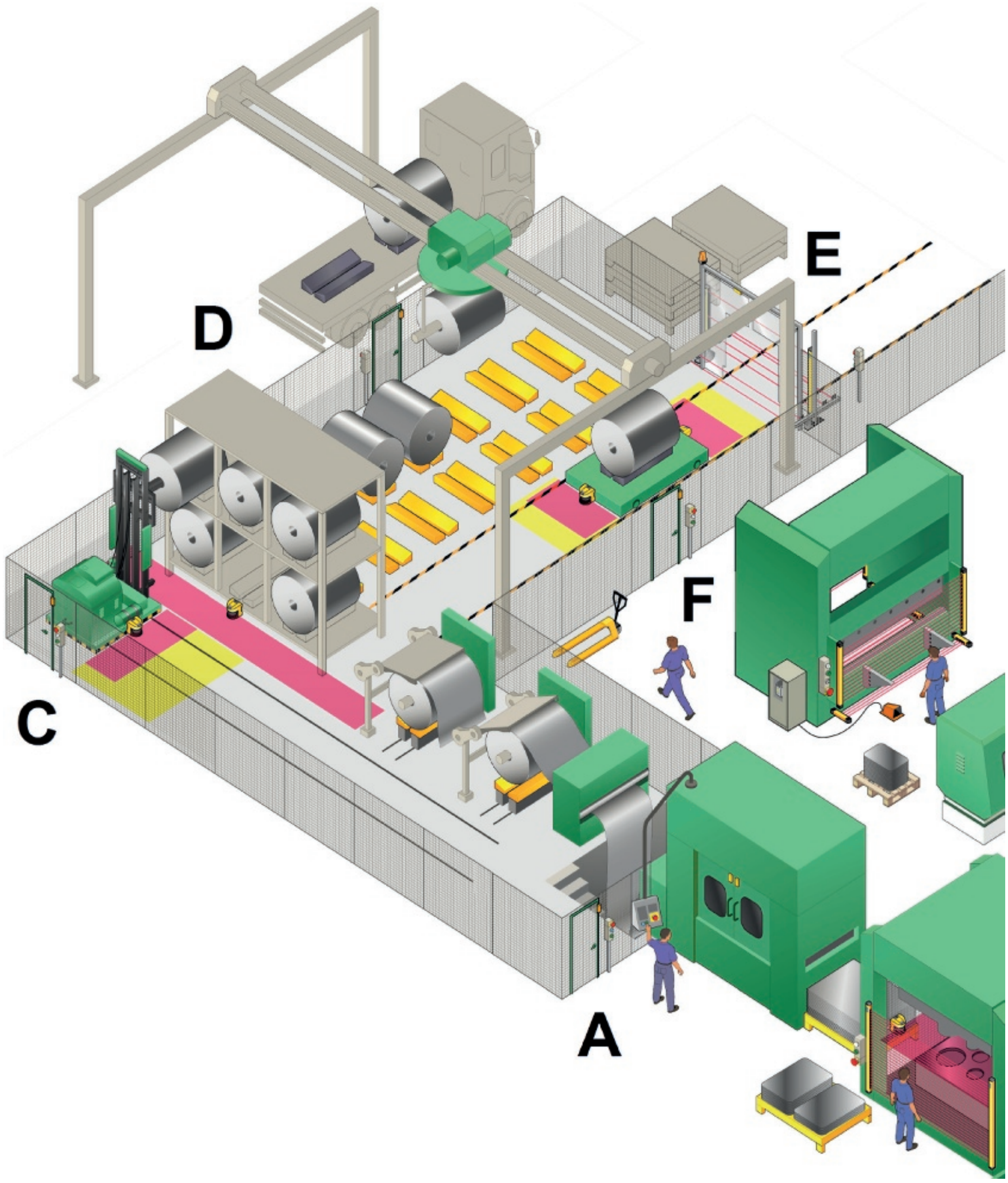


Figure A.2 — Integrated manufacturing system with several operators

If the method explained in 6.3 is applied to determine the maximum achievable DC, then:

According to Table 2 the following applies:

— Number of frequently used movable guards = 1, but due to Table 2, footnote b, it will be considered = 2 (movable guard F is easy to reach by other operators);

— Number of additional (others, not frequently used guards) = 4, but due to Table 2, footnote c, it will be considered = 3 (since C and D can be considered as not easily reachable). This is not relevant since the number of frequently used movable guards is >1.

The resulting fault masking probability level is = 3.

According to Table 3 the following applies:

— For a signal evaluation which uses static signals with same or inverse polarity, the maximum achievable DC is “none” and therefore the achievable PL of the interlocking function depends on the $MTTF_d$ values (derived from $B10_d$ values) of the incorporated position sensors but limited to PL c according to ISO 13849-1;

— For a signal evaluation which uses dynamic signals, the maximum achievable DC is “medium” and therefore the achievable PL of the interlocking function depends on the $MTTF_d$ values (derived from $B10_d$ values) of the incorporated position sensors. This may even reach PL e according to ISO 13849-1 but is limited to PL d (see 6.1).

Otherwise, if the method explained in 6.2 is applied to determine the maximum achievable DC, then:

According to Table 1 the following applies:

— Number of frequently used movable guards = 2

  Increasing due to Table 1, footnote b;

— Number of additional (others, not frequently used guards) = 3

  Decreasing due to Table 1, footnote c, but nevertheless irrelevant.

The resulting maximum achievable DC is limited to “none”, despite how the interlocking devices are cabled and their signals evaluated and the PL is limited to PL c.

A.4 Application Example 3

Figure A.3 shows an industrial robot system with a perimeter guard according to ISO 10218-2. This guard includes two interlocked movable guards (doors B and D) a material entry exit area (C) and a loading station (A) both safeguarded with an (AOPD) active optoelectronic protective device.

The following is assumed (see Figure A.3):

— the interlocking devices have dual potential free contacts (1 sensor with 2 NC contacts);

— the contacts will open when the movable guard is opened;

— the contacts are connected in series to a logic unit which evaluates both channels;

— the interlocking devices are cabled in a loop to the main cabinet;

— the cabling is not protected against external damage;

— the interlocked movable guards at “B” and “D” will be opened seldom (10x/year);

— the safeguarding devices at A and C are not considered;

— more than one operator is required to operate the system.

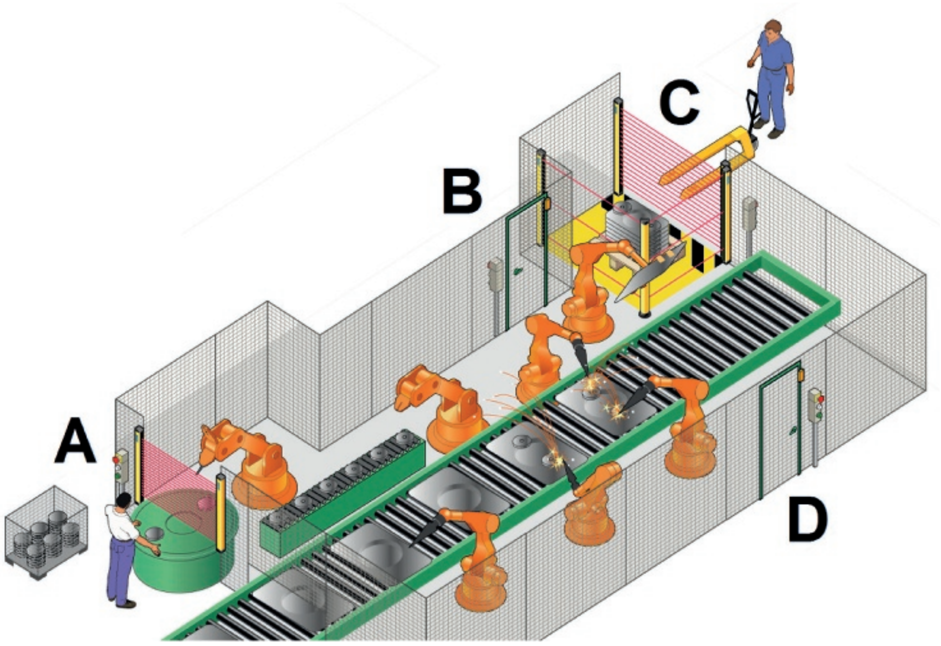


Figure A.3 — Industrial robot system with several operators

If the method explained in 6.3 is applied to determine the maximum achievable DC, then:

According to Table 2 the following applies:

— Number of frequently used movable guards = 0, but due to Table 2, footnote b, it will be considered = 1 (both movable guards are easy to reach by other operators);

— Number of additional (others, not frequently used guards) = 1.

The resulting fault masking probability level is = 1.

According to Table 3 the following applies:

— For any kind of signal evaluation the maximum achievable DC is “medium” and therefore the achievable PL of the interlocking function depends on the $MTTF_d$ values (derived from $B10_d$ values) of the incorporated position sensors. This may even reach PL e according to ISO 13849-1 but is limited to PL d (see 6.1);

— The requirements for category 4 are not fulfilled.

Otherwise, if the method explained in 6.2 is applied to determine the maximum achievable DC, then:

According to Table 1 the following applies:

— Number of frequently used movable guards = 1

  Increasing due to Table 1, footnote b;

— Number of additional (others, not frequently used guards) = 1.

The resulting maximum achievable DC is limited to “medium”, despite how the interlocking devices are cabled and their signals evaluated. The achievable PL of the interlocking function depends on the $MTTF_d$ values (derived from $B10_d$ values) of the incorporated position sensors. This may even reach PL e according to ISO 13849-1 but is limited to PL d (see 6.1). The requirements for category 4 are not fulfilled.

Bibliography

[1] ISO 13849-2:2012, *Safety of machinery — Safety-related parts of control systems — Part 2: Validation*

[2] ISO 10218-2, *Robots and robotic devices — Safety requirements for industrial robots — Part 2: Robot systems and integration*

[3] IEC 60204-1:2005, *Safety of Machinery — Electrical equipment of machines — Part 1: General requirements*

