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)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

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

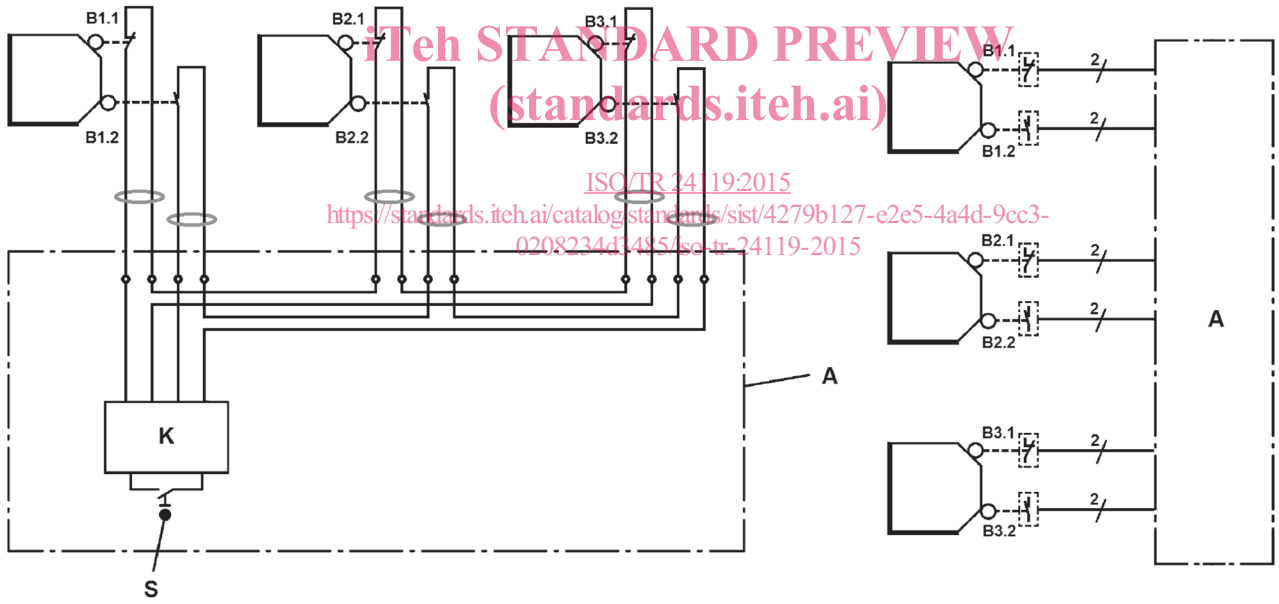
Note 1 to entry: See IEC 60204-1:2005, 9.4.3.1, method a).

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.



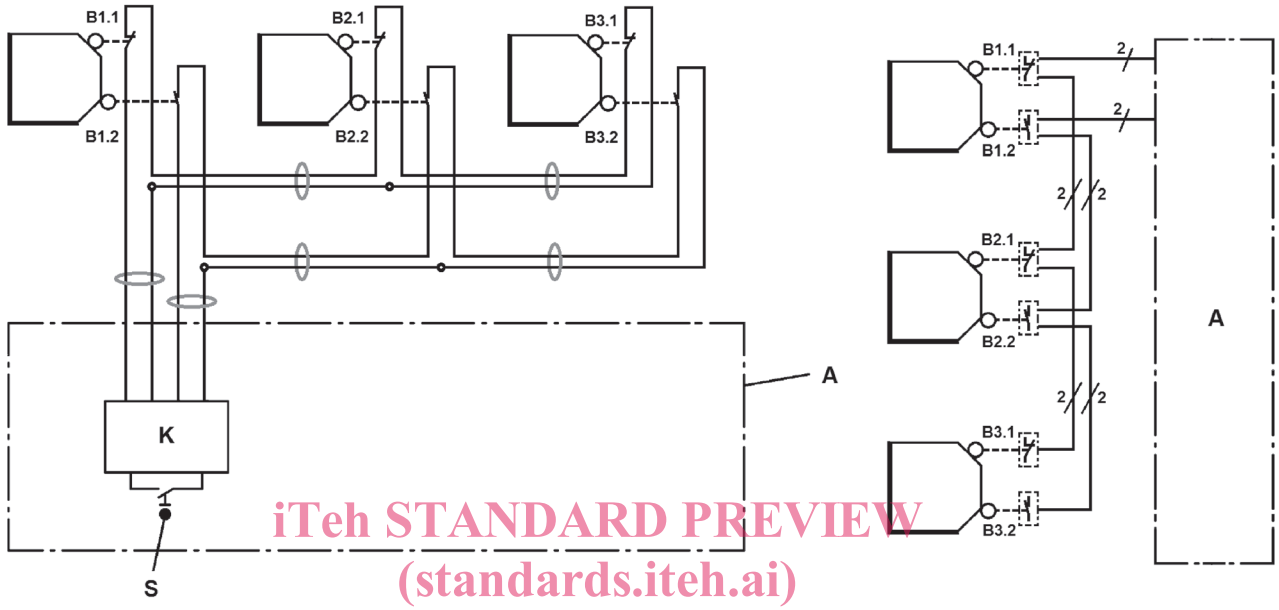
Key

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



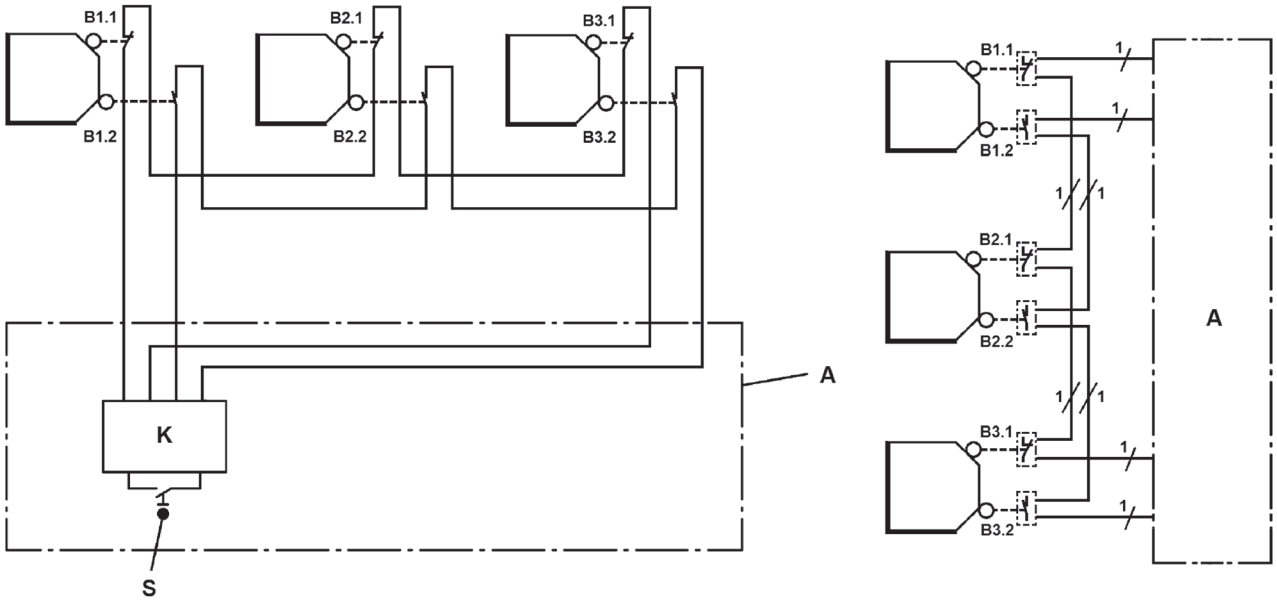
Key

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.



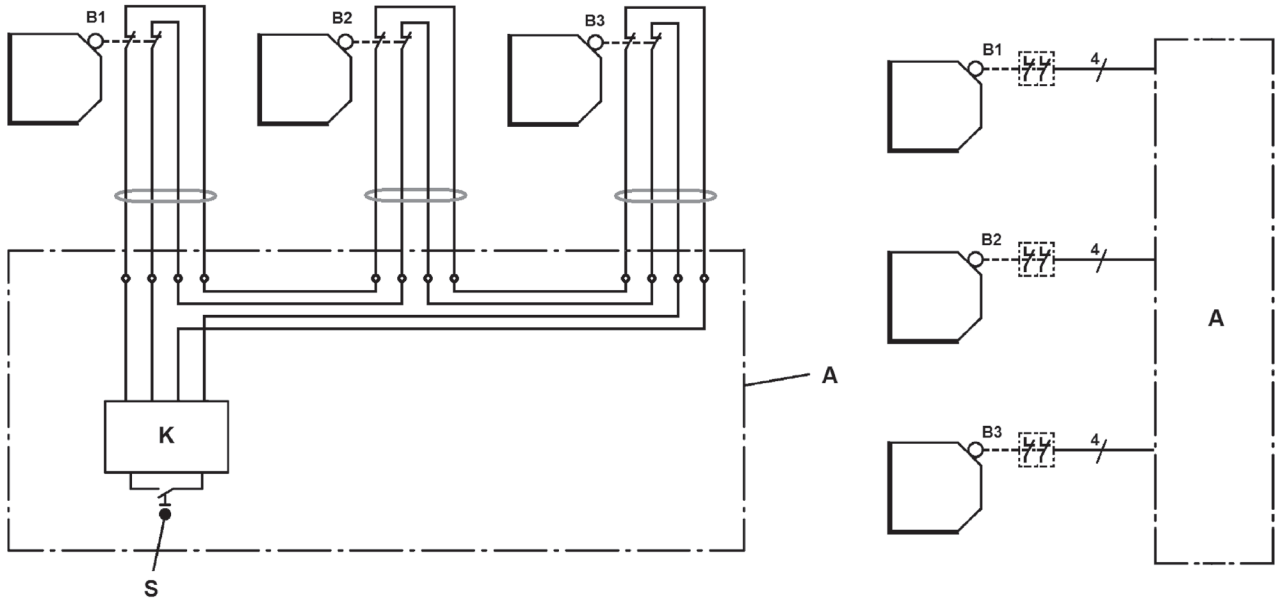
Key

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.

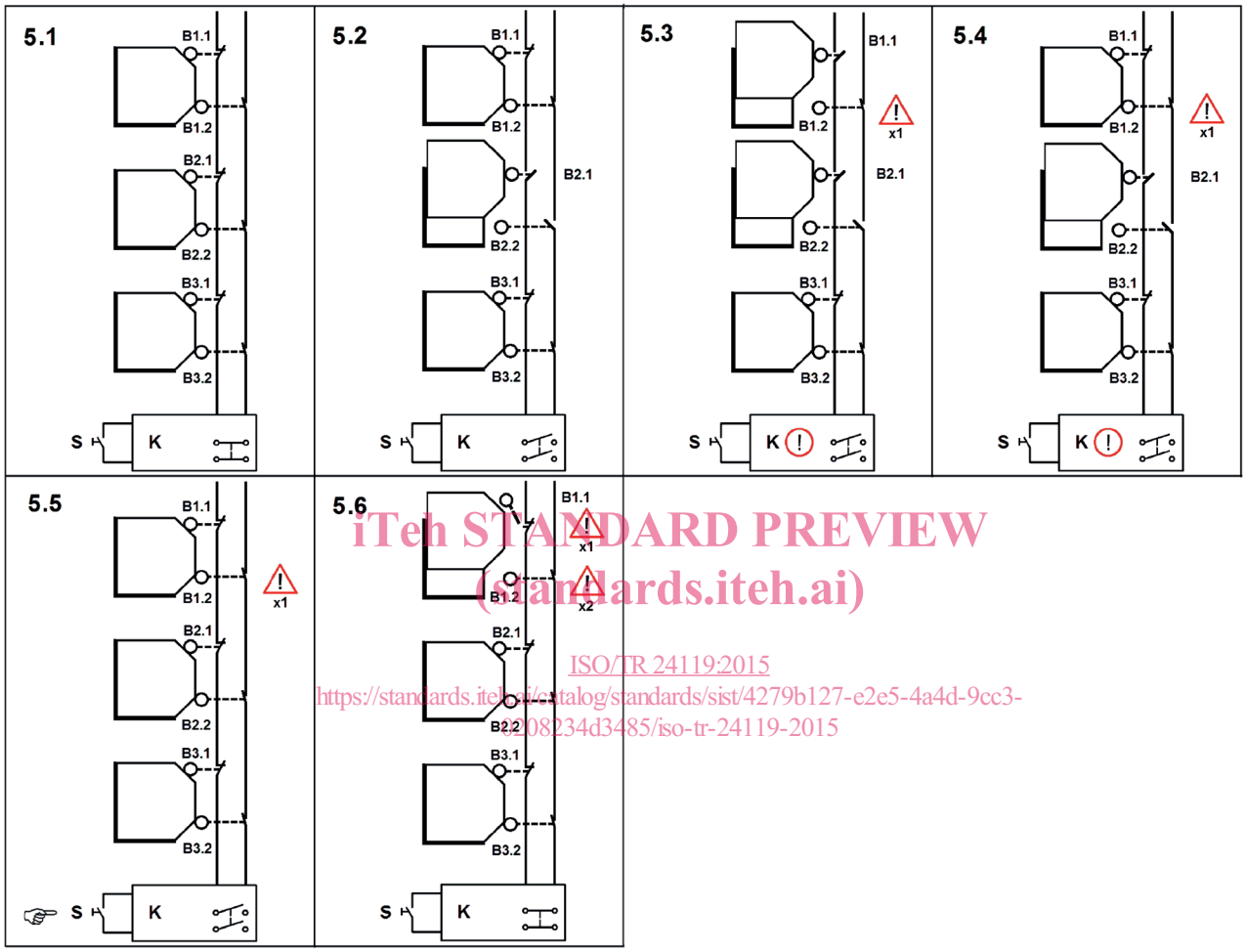
It is foreseeable that more than one movable guard will be open at the same time or in a sequence, e.g. due to subsequent fault finding procedure or as part of the regular operation of the machine.

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.



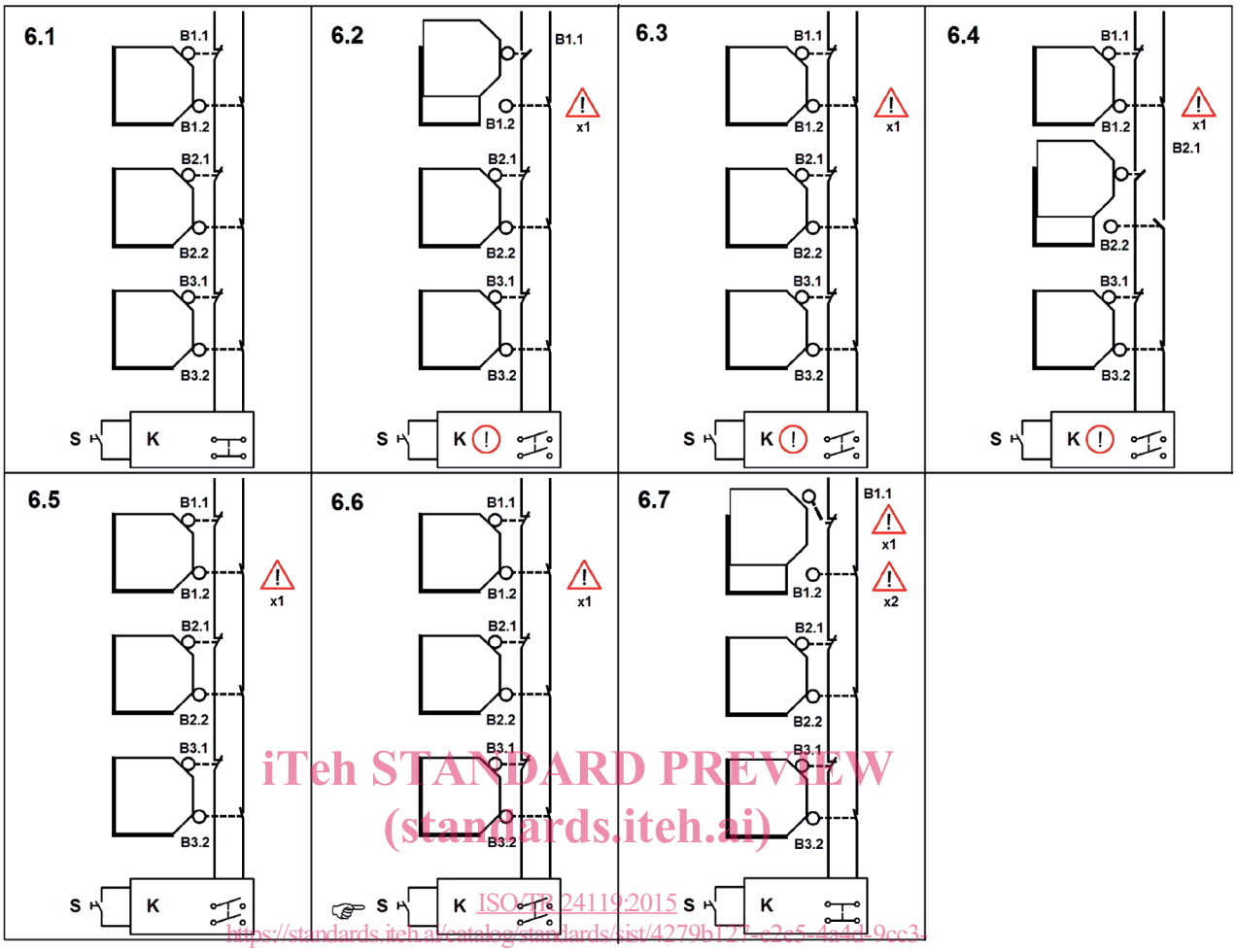
Key

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.