Journal of KONBiN 2023
Volume 53, Issue 3
DOI 10.5604/01.3001.0053.9063

Leszek KASPRZYCZAK ORCID 0000-0003-2413-7610, leszek.kasprzyczak@polsl.pl
Silesian University of Technology (Politechnika Śląska), Poland

COMMON ERRORS IN MACHINE SAFETY-RELATED CONTROL SYSTEMS AND METHODS OF THEIR ELIMINATION

Często występujące błędy w układach sterowania związanych z bezpieczeństwem maszyn oraz metody ich eliminacji

Abstract: *The article focuses on the description of non-conformities occurring in safety-related control systems of machines collected by the author during safety audits of machines and production lines. The aim of the article is to familiarise machine designers with safety requirements and ways of eliminating common mistakes made during design, while at the same time indicating to investors buying machines which requirements to take into account when placing an order.*
Keywords: safety-related control systems, machine safety, safety requirements, machinery directive, improvement of machine safety,

Streszczenie: *W artykule skupiono się na opisie niezgodności występujących w związanych z bezpieczeństwem systemach sterowania maszyn zebranych przez autora podczas audytów bezpieczeństwa maszyn i linii produkcyjnych. Celem artykułu jest zapoznanie projektantów maszyn z wymaganiami bezpieczeństwa i sposobami eliminowania często popełnianych błędów podczas projektowania, a jednocześnie wskazanie inwestorom kupującym maszyny, jakie wymagania należy wziąć pod uwagę przy składaniu zamówienia.*
Słowa kluczowe: związany z bezpieczeństwem układ sterowania, bezpieczeństwo maszyn, wymagania bezpieczeństwa, dyrektywa maszynowa, poprawa bezpieczeństwa maszyn

Received: September 18, 2023 / Revised: September 26, 2023 / Accepted: September 28, 2023

1. Introduction

Legal and normative requirements are available to the general public, but nevertheless pose a challenge to machine manufacturers, as their content is often poorly understood by designers and the large number of requirements in the standards pose a problem to master. Although it is possible to use a Notified Body in machinery safety for certification, it is not common because according to the Machinery Directive (Article 12), there are three procedures for assessing the conformity of machinery. The most commonly chosen procedure is the internal checks on the manufacture of machinery. Only potentially hazardous machinery referred to in Annex IV can be subjected to Notified Bodies unless they are manufactured according to detailed C-type standards. Thus, in practice, it is possible to omit Notified Bodies from the conformity assessment which leads to neglecting many safety requirements. Therefore, the article presents common non-conformities occurring in safety-related machine control systems with ways of eliminating them, as many errors can be avoided at the design and procurement specification stages.

According to Annex B of EN ISO 12100 titled *'Safety of machinery. General principles for design. Risk assessment and risk reduction'* [1] hazards are divided into:

- mechanical (e.g. loss of stability, fall from a height due to incorrect permanent means of access to machinery, crushing, impact and cutting caused by moving machine actuators, gravity fall or whipping of flexible fluidic hoses),
- electrical (direct contact with live parts, indirect contact to exposed conductive parts),
- thermal (contact with hot or very cold surfaces),
- caused by noise and mechanical vibrations (exceeding permissible levels),
- caused by radiation (laser, ultraviolet, electromagnetic field),
- caused by hazardous substances (produced in the production process or used for production and maintenance),
- combinations of hazards, e.g. from unexpected start-up resulting in mechanical injury or exposure to electrical shocks during maintenance work,
- caused by failure to comply with ergonomic principles, e.g. in the area of excessive effort, inadequate lighting, incorrect location and identification of controls.

Some of the above-mentioned hazards are controlled by safety-related control systems, which significantly minimise the risks [2–3]. A safety-related control system should be characterised by adequate reliability and certainty of operation depending on the level of risk it reduces. Namely, depending on the level of the risk, which consists, among other things, of the severity of the injury (slight or serious injuries - including death), the control system must perform its functions with a lower or higher level of reliability, which translates into its costs [4]. An example of an analysis of a real production line is the low-emission composite fuel production line described in the paper [5].

The essential requirements for control systems are contained in Section 1.2 of Annex I of the current Machinery Directive 2006/42/EC. The essential requirements for control systems are contained in Section 1.2 of Annex III of the Machinery Regulation 2023/1230, which will be in force from 2027. It is noteworthy that the new Machinery Regulation 2023/1230, passed by the European Parliament and the Council in 2023, has started to cover cybersecurity issues of safety-related control systems, as malicious deactivation of safety systems can result in accidents during operation [6–7].

The recommendations are described in more detail later in the article. Where possible, the concepts are illustrated with example drawings.

2. Nonconformities related to incorrect location and identification of control elements

Nonconformities related to incorrect location and identification of controls have an impact on safety and ergonomics. Requirements and recommendations in this respect for electrical, hydraulic and pneumatic systems are given in EN 60204-1 [8], EN ISO 4413 [9] and EN ISO 4414 [10]. It is also worth supplementing the requirements contained in the three-part EN 894 standard [11].

The requirements in this matter will be fulfilled if the following questions, among others, are answered in the affirmative:

– whether the controls are labelled/marked (e.g. Fig. 1 and 2),

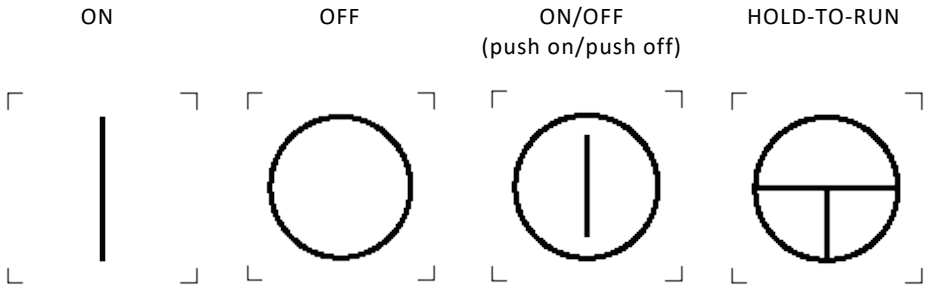

Fig. 1. Symbols of controls used in power circuits according to EN 60204-1 [8]

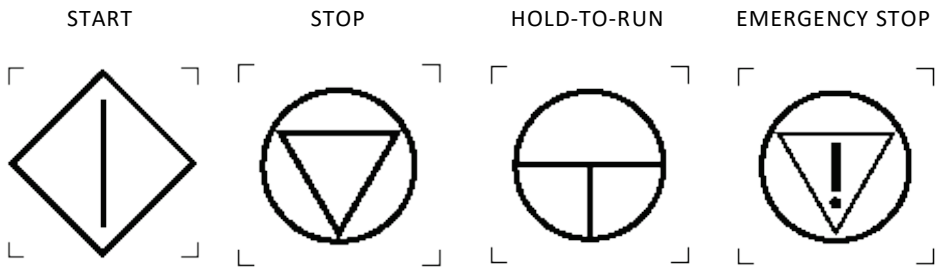

Fig. 2. Symbols of controls used in machine control circuits according to EN 60204-1 [8]

- whether the control elements are at a height above 0.6 m (clearly visible, not susceptible to accidental actuation, e.g. by a knee or a hip),
- whether the main switch-disconnector is between 0.6 and 1.9 m from the operating level,
- that the colours of the pushbuttons comply with the recommendations of EN 60204-1
- that the operator interface on the HMI is available in a language understood by the operator,
- that the emergency stop buttons comply with EN ISO 13850 [12], e.g. red 'mushroom' on a yellow background,
- that the emergency stop devices are located between 0.6 and 1.7 m high,
- whether emergency stop devices are present on each operator control panel (unless this is not valid),
- whether the E-stop buttons have marked spans of control (where there is more than one 'mushroom' next to each other stopping different parts of the machinery),
- whether the resetting devices cannot be reached from inside the danger zone,
- whether the danger zones are visible from the resetting area, preventing an operator from starting the machine when another operator is inside the machine,
- if the machine operates in several modes requiring different protective measures and/or procedures, there is a mode selector switch that can be locked in each position (e.g. with a key). The mode selector switch may be replaced by another selection method, such as an access code that restricts the use of certain functions to certain groups of operators,
- whether the two-hand-control device (THCD) meets the requirements of EN ISO 13851 [13] in terms of the arrangement of buttons, their colours, height from the operating level and their covers.

3. Nonconformances in the safety-related control systems

The safety functions are implemented using the safety-related parts of control systems SRP/CS discussed in the 2-part standard EN ISO 13849 [14] [15] or SCS (Safety-related Control Systems) according to EN 62061, which has a new edition [16].

1.1. Earthing control circuits

The starting point for further considerations is the proper power supply and earthing of the SCS and SRP/CS parts. In EN ISO 13849-2, Table D.1 on basic safety principles (and therefore applicable to all categories B to 4) states the principle of the correct protective bonding, namely: '*one side of the control circuit, one terminal of the operating coil of each electromagnetic operated device or one terminal of another electrical device are connected to the protective bonding circuit (see also EN 60204-1, 9.4.3.1)'*. Thus, according to EN 60204-1, the output of a transformer or DC power supply with ground potential should be earthed (Fig. 3), which is often neglected by manufacturers. The reason for this requirement is that in the absence of earthing and symmetrical voltage division at the transformer output and the occurrence of isolation faults on the switched conductors (1), it will not be possible to switch off the contactor/valve coil (and stop the machine).

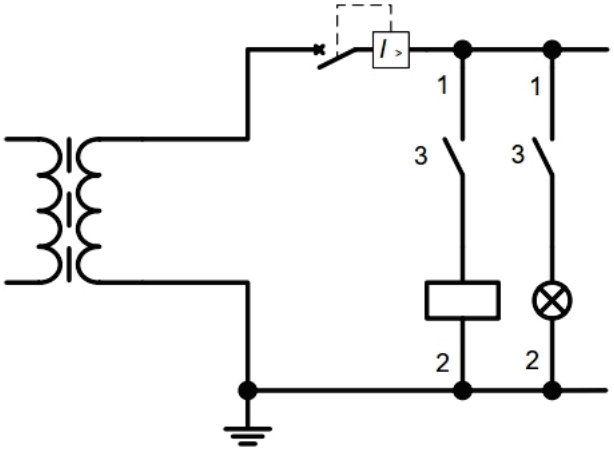

Fig. 3. Required earthing [8] according to EN ISO 13849-2; 1 – Switched conductors, 2 – common conductors, 3 – control switches

The method can also be used for DC voltage control circuits

1.2. Suppression of transients

Another common mistake made by manufacturers is not to use suppression devices (Fig. 4) on the coils of contactors, relays and valves. Meanwhile, the basic safety principles state that *a suppression device (RC, diode, varistor) must be used in parallel with the load but not parallel with the contacts*. So, this is a rule without which the requirements for any safety category cannot be met.

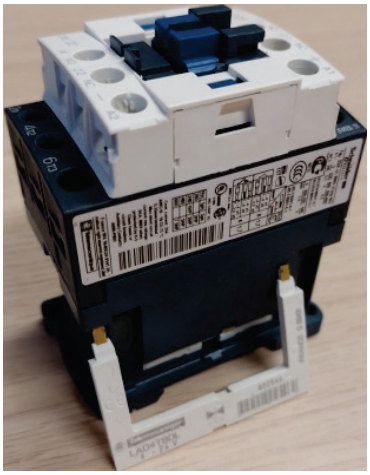

Fig. 4. Bidirectional diode (Transient Voltage Suppressor) prepared for connection to the contactor coil

1.3. Diagnostic Coverage

The significant mistake is the lack of appropriate devices to provide the required level of diagnostics (according to Table E.1 of EN ISO 13849-1), which is required for categories 2, 3 and 4. The connection of feedback signals from actuators to a standard PLC is not forbidden, but unauthorised access and the possibility of making unauthorised changes to the controller's programme are noteworthy, which can remove the diagnostic coverage of the safety function under consideration.

Also encountered mistake is the inadequate level of safety achieved for control systems. For example, the EN ISO 10218 standard for robotic workstations requires the provision of the PLr=d level at category 3, which implies the use of redundancy. According to EN ISO 13849-1, PL means Performance Level which is a discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions.

In contrast, a mistake made by integrators is to use sensors with the PL=d level of category 2, with a single channel.

1.4. Achieved Performance Level (PL)

A similar situation exists with interlocking gates/guards. Manufacturers of safety devices supply the market with dual-channel electromechanical interlocks that meet the PLd/e level in the electrical part but stipulate that a single mechanical activator (tongue) does not provide dual-channel operation, reducing the level achieved to PL=c. In this case, it is necessary to add a robust mechanical guide (Fig. 5), by which damage to the mechanical activator can be excluded and, as a result, a higher safety level of the interlocking function can be achieved (depending on the electrical part).

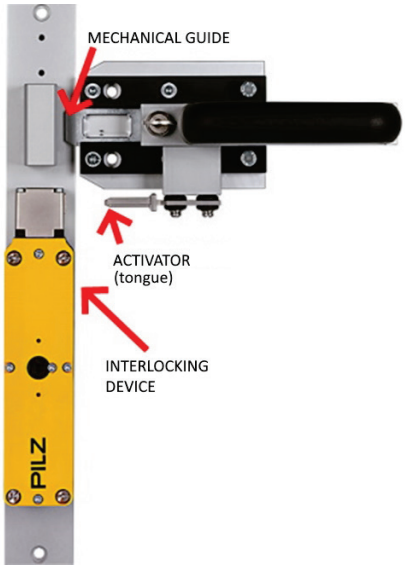

Fig. 5. Interlocking device with guard locking with additional guide excluding damage to the mechanical activator [17]

1.5. Fault masking and impact on Diagnostic Coverage

A production line, e.g. a robotic cell, may have several entrances secured with interlocking guards. A common mistake is to connect electromechanical locks in series, which decreases the level of the diagnostic coverage. If any interlock in one channel is damaged, the damage may be masked by opening and closing other doors (Fig. 6). However, when using interlocks with integrated diagnostics, a high PL level can be achieved, e.g. PL=d/e for a series connection. Nevertheless, it is necessary to analyse the manufacturer's documentation in order to meet the appropriate requirements for correct wiring.

If the operator has a problem with starting the machine, i.e. the control system does not allow the machine to restart, the operator will look for a simple solution and, for

example, will open and close individual doors, thinking that this will help. This way the fault will be masked. If the second channel is damaged as well, opening the door will not stop the machine. Diagnostic Coverage will deteriorate significantly.

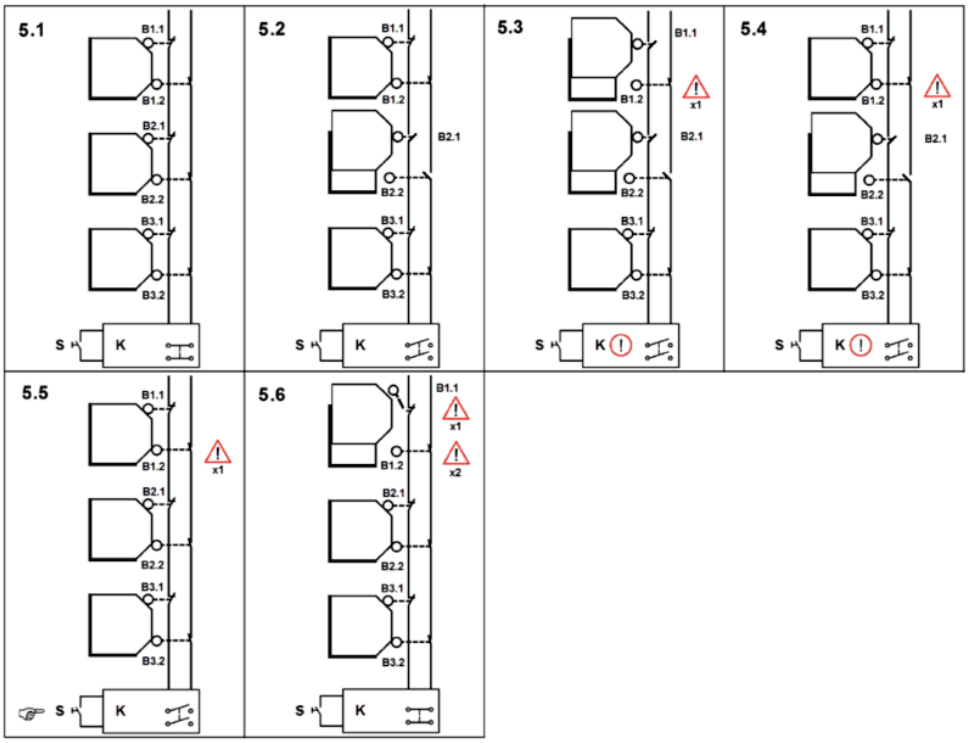

Fig. 6. Fault masking [18]; B1, B2, B3 interlocking devices with potential free contacts; K logic unit; S manual reset; x1 initial fault – contact fails to open; x2 second fault – broken switch lever

Technical report ISO/TR 24119 [18] provides methods for estimating achievable Diagnostic Coverage depending on potential fault masking. The report presents the simplified and regular methods. Table 1 provides the simplified approach to the determination of the maximum achievable Diagnostic Coverage. If the maximum achievable Diagnostic Coverage resulting from the application of this table does not meet the required level, the more detailed approach given in the regular method may be more suitable; however, it will not be discussed in this paper.

The topic of Diagnostic Coverage is very extensive, and to understand it well, it is necessary to familiarize yourself with the requirements of many standards and technical reports, including EN ISO 13849, EN IEC 62061, EN 61508, EN ISO 14119 and ISO/TR 29119. At the same time, Diagnostic Coverage values are crucial for categories 2, 3 and 4.

Often, the lack of diagnostic coverage or its too low-value results in failure to meet safety requirements [19].

Table 1

Maximum achievable Diagnostic Coverage for the simplified method [18]

Number of frequently used movable guards[a, b]	Number of additional movable guards[c]	Maximum achievable Diagnostic Coverage [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.

4. Summary

The content of this article presents the author's selective insights from machinery safety assessments carried out. The aim of the paper is to provide both manufacturers and users of machinery with practical advice in this area.

Despite the fact that the safety standards related to control systems were published many years ago and are still updated, machinery manufacturers are still struggling to understand and implement their requirements correctly. Statistics on serious and fatal accidents in Europe show that efforts are still required to make machinery safer and to check the correct implementation of safety functions in the control systems.

In addition, there are new challenges related to the increasing autonomy of machines, e.g. RIA (robotic-intelligent-autonomous) systems, cybersecurity and artificial intelligence, which will result in the implementation of new legal and normative regulations in this area.

5. References

1. EN ISO 12100:2010, Safety of machinery. General principles for design. Risk assessment and risk reduction.
2. M. Dźwiarek, "An analysis of Accident Caused by Improper Functioning of Machine Control Systems", International Journal of Occupational Safety and Ergonomics vol. 10, no. 2, 2004, 129–136.
3. M. Dźwiarek, Assessment of software and hardware safety of programmable control systems of machinery. In: Safety and Reliability for Managing Risk. C. Guedes Soares & E. Zio (ed.) © Taylor & Francis Group, London, 2006, ISBN 978-0-415-42315-2, 2325-2330.
4. M. Dźwiarek, "Performance Level validation of the machinery control system", Journal of KONBiN, (33) 2015, 29-40.
5. A. Kozłowski et. al., "The role and importance of risk assessment in machinery design and control systems on the example of a model research line designed for the production of low-emission composite fuel", Journal of KONBiN, Volume 53, Iss. 1, 2023, DOI 10.5604/01.3001.0016.3234, 25-46.
6. G. Macher, A. Höller, H. Sporer, E. Armengaud, C. Kreiner: A comprehensive safety, security, and serviceability assessment method. In: Koornneef, F., Gulijk, C. (eds.) SAFECOMP 2015. LNCS, vol. 9337, Springer, Cham (2015). DOI:10.1007/978-3-319-24255-2_30, 410–424.
7. M. Śliwiński, E. Piesik, J. Piesik, "Integrated functional safety and cybersecurity analysis", IFAC PapersOnLine, Vol. 51, Issue 24, 2018 https://doi.org/10.1016/j.ifacol.2018.09.572, 1263–1270.
8. EN 60204-1:2018 Safety of machinery - Electrical equipment of machines - Part 1: General requirements.
9. EN ISO 4413:2010 Hydraulic fluid power. General rules and safety requirements for systems and their components.
10. EN ISO 4414:2010 Pneumatic fluid power. General rules and safety requirements for systems and their components.
11. EN 894 Safety of machinery. Ergonomics requirements for design of displays and control actuators (3 parts).
12. EN ISO 13850:2015 Safety of machinery. Emergency stop function. Principles for design.
13. EN ISO 13851:2019 Safety of machinery. Two-hand control devices. Principles for design and selection.
14. EN ISO 13849-1:2015 Safety of machinery. Safety-related parts of control systems - General principles for design.

15. EN ISO 13849-2:2012 Safety of machinery. Safety-related parts of control systems – Validation.
16. EN IEC 62061:2021 Safety of machinery. Functional safety of safety-related control systems.
17. https://www.pilz.com/pl-PL/products/sensor-technology/safety-switches/psenbolt-safety-bolt (available 18.09.2023).
18. ISO/TR 24119:2015 Safety of machinery. Evaluation of fault masking serial connection of interlocking devices associated with guards with potential free contacts.
19. M. Dźwiarek, "Prevention of defeating interlocking devices associated with guards", Journal of KONBiN, Volume 49, Issue 3, 2019, DOI 10.2478/jok-2019-0067, 451-460.