PROBLEMY MECHATRONIKI
UZBROJENIE, LOTNICTWO, INŻYNIERIA BEZPIECZEŃSTWA

ISSN 2081-5891
E-ISSN 2720-5266

13, 4 (50), 2022, 137-146

PROBLEMS OF MECHATRONICS
ARMAMENT, AVIATION, SAFETY ENGINEERING

IT Protection of Safety-Related Machine Control Systems in Industry 4.0

Marek DŹWIAREK

Central Institute for Labour Protection − National Research Institute,
16 Czerniakowska Str., 00-701 Warsaw, Poland
Author's e-mail address and ORCID:
madzw@ciop.pl; https://orcid.org/0000-0001-5817-9515

Received: August 15, 2022 / Revised: September 10, 2022 / Accepted: December 6, 2022 / Published: December 30, 2022.

DOI 10.5604/01.3001.0016.1465

Abstract. The overall objective of the research was to develop the consideration of threats of unauthorized interference in information systems in the risk assessment process carried out by designers of machine control systems. For this purpose, an analysis of typical structures related to the security of control systems was carried out in terms of the possibility and consequences of the loss of security functions as a result of unwanted interference. Recommendations for proceeding "step by step" in the subsequent stages of the risk analysis were determined.
Keywords: Industry 4.0, cyber security, safety of machinery

1. INTRODUCTION

In modern machinery, control systems play an increasingly important role in ensuring the safety of their operators. However, when developing such systems, it is important to be aware of the possibility of any defects and failures that could cause a hazard to the machine operators. In [1] are the results of an accident analysis caused by the malfunction of machine control systems. In those accidents caused by improper operation of the control system, serious accidents were much more common (41%) than among accidents not related to the control system (7%). This indicates how important are the issues related to machine control systems. Therefore, one of the important problems encountered while using modern machine control systems is to ensure that these systems provide security functions [2].

The implementation of manufacturing systems using the Internet of Things (IoT) in Industry 4.0 allowed significant flexibility in production, with a focus on the needs of customers. At the same time, this has resulted in the rise of new threats associated with unauthorized interference with informatics (IT) systems. This is particularly relevant in the case of critical infrastructure, where unauthorised interference can even lead to an industrial disaster with significant consequences for people and the environment. Therefore, in the case of critical infrastructure, work on security against unauthorised interference has been carried out for many years [3, 4]. This work has focused primarily on the functional safety of industrial processes.

In [5], the authors state that cyber security is gaining importance in the lifecycle risk analysis of technical systems, e.g., cyber-physical systems (CPS) in the context of the increasing dependence on networked systems and processes. In industrial environments, functional safety assessment is a standard procedure, such as the use of IEC 61508 and its derivatives, while cyber security in safety-related fields has only been introduced in the last few years. Cyber security assessment is a rapidly evolving discipline, but so far there have been few approaches to combining standard procedures in safety and security.

It can therefore be concluded that work on aspects of IT protection in industrial control systems is being carried out in many centres. They mainly concern such areas as large process industry installations, vehicle control systems or critical infrastructure. However, there are no reports on the principles of considering IT protection in the design of machine control systems. Such systems tend to be much simpler in design than complex high-risk systems, and so the methodology developed for complex high-risk systems is excessive in relation to the complexity of machine control systems. It is therefore necessary to develop methods for considering IT protection appropriate for the complexity of the machine control systems.

2. RESEARCH OBJECTIVES AND METHODOLOGY

Current technologies enable remote monitoring and/or improved machine operation by adjusting the parameters without having to be on site. The mere possibility of adjusting machine parameters to increase its efficiency creates, however, the possibility of making adjustments by the people who may put employees and other people at risk. For example, speed or force can be adjusted to a dangerous level, temperature may be reduced below the "kill step" level, and error codes or messages may be deleted or falsified. Those safety-related IT attacks involving direct or remote access to and manipulation of safety-related control systems for deliberate misuse can affect machine safety.

The aim of the study was to develop a method that takes into account the risks associated with unauthorized interference (cyber-attacks) in machine control systems during the risk analysis process carried out by the designers of these systems.

The problem of data protection in computer-based machine control systems is currently completely ignored by their designers, due to the lack of an accessible methodology for risk assessment in this respect. Developing such a methodology should significantly improve the process of designing protection appropriate to the level of risk. This will make it possible to overcome the barriers to the digitalisation of technological processes and the systems that support them, which are threats to those fully automated production processes associated with the possibility of cyber-attacks.

In order to develop a method of taking into account the risks of unauthorized interference with the control systems, an analysis of the main structures of the machine control systems has been carried out in terms of the potential unauthorized interference and the types of such interference. The potential consequences of unauthorised interference and the associated risks were analysed. On this basis, a method has been developed that provides step-by-step recommendations for the following phases of the risk analysis:

- determination of the limits of the machinery,
- hazard identification,
- risk estimation,
- residual risk information.

3. RESULTS

Risk assessment is a process that provides the most relevant information necessary to make decisions about safety assurance methods. It is an iterative process that should be performed at different stages in the life cycle of a machine.

The risk assessment performed by the developers allows us to gather detailed information about the construction and operation of the machine, and to identify information important for the user.

The basic principles of risk assessment are set out in EN ISO 12100:2011 [6]. These principles do not take into account the possibility of unwanted interference in the increasingly common IT systems of Industry 4.0. The interrelation of cyber security aspects with risk assessment according to [6] is addressed in ISO/TR 22100-4:2018 [7]. Although intentional misuse does not fall within the scope of the standard [6] and the risk assessment process, it is reasonable for machine manufacturers to also consider such risks.

The potential impact of cyber-attacks on machine safety is shown in Figure 1. It shows that, when assessing the risks associated with the operation of machinery, one should also take into account the possibility of the adverse effects of potential attacks on the integrity of the information system, in particular those control systems performing safety functions. Since the result of such an attack could be the loss of safety functions, preventing cyber-attacks should be part of the methodology for preventing dangerous faults.

The PN EN – ISO 13849-1:2016 standard [8] is most commonly used to determine the resistance of the safety-related machine control system. This standard classifies the control system's fault tolerance to five levels of PL safety performance, from "a" to "e". These levels are probabilistic indicators of the probability of a dangerous fault occurring per hour over the expected lifetime of the machine. The standard also divides systems into five categories: B, 1, 2, 3 and 4, depending on their structure and behaviour under fault conditions. This division is not dependent on the technology used, but only on the resistance of the devices to faults and their behaviour in the defect state. The basic principles of IT protection are actually formulated in IEC TS 62443-1-1:2009 [9]. This document introduces the security classifications to 3 Security Levels (SL). The SL provide a reference framework for decisions on the application of remedies and equipment with different levels of security. It is recommended to use at least three levels of security: SL1 - low, SL2 - medium and SL3 - high.

3.1 Analysis of control system structures in terms of cyber security

3.1.1. Category B

Category B is the main category of fault tolerance. Equipment manufactured in accordance with the standards in question and according to the intended working environment are eligible for this category. A foult of equipment in this category may result in a loss of the safety function. Category B requirements implement serial structure systems. They provide the PLa or PLb safety level. They are usually electromechanical systems but can also be electronic programmable systems.

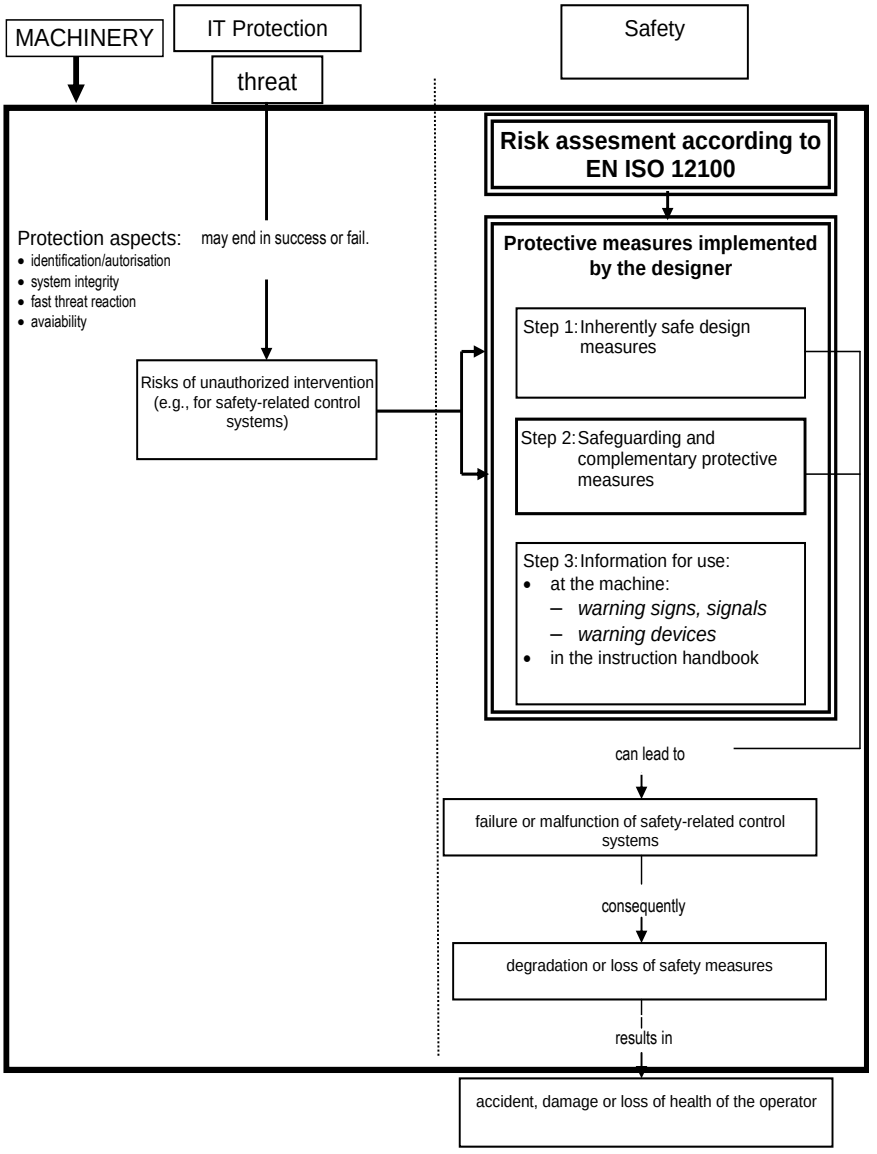

Fig. 1. Impact of cyber security on machine safety

They are used where the potential severity of the damage is minor, usually a reversible injury, and the frequency of recalling the safety function is low. This means that Category B systems provide low-level risk reduction. Possible unwanted interference with the system is only possible if it is a programmable electronic system.

Such interference may result in the loss of the safety function. Due to the low level of reduced risk, the potential damage to such interference will be low. In this case, it is enough to apply preventive solutions to achieve an SL-T 1 security level.

3.1.2. Category 1

Category 1 systems also have a single-channel structure in which a single fault can cause a loss of safety functions. Category 1 systems require the use of well-tried components. This reduces the risk by increasing system reliability. It is assumed that programmable electronic circuits do not allow high MTTF values to be obtained, and therefore cannot be used in Category 1 systems. This means that unwanted interference is not possible and therefore protection is not required.

3.1.3. Category 2

In categories 2, 3 and 4, the increase in fault resistance is achieved by expanding the system structure. In category 2, this is performed by periodic tests of the safety function. In such systems, a single fault can cause the loss of the safety function between tests. Category 2 systems are used when the severity of the potential damage is low, usually reversible. The demand rate of the safety function may be high and the possibility of avoiding harm low. This means that these systems are used to reduce the average risk, which corresponds to the level of safety performance of PLa - c. This means that it will be sufficient to provide security at the SL-T 1 level (for PLa and PLb) or the SL-T 2 level (for PLc).

3.1.3. Category 3

In categories 3 and 4, fault resistance is achieved by continuously ensuring that a single defect does not cause a loss of the safety function. In Category 3 equipment, defects should be detected when reasonable. These systems have a two-channel structure. In these systems, diversification (one programmable channel, the other electro-mechanical) is a common solution. Such systems are used when potential injuries are severe (usually irreversible). The frequency of demand of the safety function can be high. These systems provide PLb and PLc levels of safety, while for systems with high MTTF and medium diagnostic coverage also provide PLd. In those cases, where a category 3 system reduces the risk corresponding to a PLb or PLc level in systems where channel diversification is applied, protection against unwanted interference at the SL-T 2 level will be sufficient, and in the case of a risk reduction at the PLd level it should be SL-T 3.

3.1.5. Category 4

Category 4 systems are also dual-channel. For this category, defects should be detected. If this is not possible, resistance to the accumulation of defects shall also be specified. Due to the high-risk reduction implemented at the PLe level, high MTTF values and high DC diagnostic coverage are required for them. In these systems, unwanted interference can lead to an immediate serious accident caused by the loss of safety functions. Therefore, protection at the highest level, SLT 3, should be used.

3.2 Method of incorporating cyber-attack threats into the risk analysis process

3.2.1. General principles

The previous chapter proposes principles to formulate the requirements for IT security measures depending on the risk level and system category. These principles should be applied at all stages of the risk assessment in accordance with [6]. The risk assessment of any machine should therefore be carried out before considering the risks associated with IT protection. Then the resulting per se safe solutions should be analysed, followed by an analysis of the design, protective and risk mitigating measures associated with the machine IT vulnerability. The resulting IT risks can then be reduced by the combined efforts of component suppliers, machine manufacturer, integrator and machine user.

3.2.2. Determination of the limits of the machinery

The risk assessment starts with the determination of the limits of the machinery. limits related to cyber security aspects fall under the category of other limits. The most effective method of eliminating the risks of unauthorised interference in IT systems is to use solutions that, in their very design, do not allow external access to the control system. However, the use of Industry 4.0 and especially IoT capabilities in machines does not allow the machine to be completely separated from external systems. Vulnerability to IT-related attacks depends largely on whether the device needs to be connected to an external IT system, and how often this happens. The machine control system developer should therefore ask the following questions:

1) Does the control system have to be able to connect to an external network?
2) Does it have to be connected permanently (continuously)?
3) Is the connection monitored?
4) Is the connection configurable (e.g., authorized access only)?
5) Can the connection be restricted to "read only" mode?

3.2.3. Hazard identification

The next step is to systematically identify the hazards that can reasonably be foreseen during all phases of the machine's life cycle. Only when hazards are identified can appropriate steps be taken to eliminate the hazards or reduce the risks. Hazard identification is performed in relation to the functioning of the machine. Potential cyber-attacks have no impact on machine-related hazards that are closely related to the machine design. Therefore, IT security issues do not need to be taken into account when identifying a hazard.

3.2.4. Risk assessment

For safety-related control systems, the risk assessment should be carried out in accordance with the standard [8]. The following aspects should be taken into account in this process:
S1 – severity of injury – the potential cyber-attack has no impact,
F1 – frequency or duration of exposure – not dependent on cyber-attacks,
P1 – possibility of avoiding the hazard or limiting harm is independent of a cyber-attack.

We can therefore see that cyber-attacks do not affect the risk assessment parameters.

3.2.5. Selection of protective measures

The results of the risk assessment should form the basis for the selection of the risk reduction measures. According to IEC TR 63069:2019 [9], cyber security aspects should be taken into account as a source of potentially dangerous defects. This means that the vulnerability of a system sensitive to cyber-attacks will be higher than that of a resilient system. The requirements for the resilience of an IT system to attacks can be determined from the analyses in section 3.1

3.2.6. User information

The machine user should be informed of all aspects of the machine operation, in particular the residual risk and the necessary additional security measures. This information should be given in the "User Information". Effective IT security solutions require the collaboration of various parties, including machine manufacturers and users. The instruction manual should contain all the information necessary to maintain the intended SL level for each safety function. Information on the required training and retraining of personnel to comply with IT security procedures should also be provided.

4. CONCLUSIONS

The side effect of technological progress in the development of IT systems is the evolution of unwanted interference in these systems. This also applies to any machine control systems that are connected to Industry 4.0 and IoT systems used in companies. Such interferences currently aim to disrupt production processes in order to achieve material benefits. However, they can also lead to the deactivation of the safety functions provided by machine control systems and, consequently, to accidents. It is therefore increasingly important to take appropriate measures to limit the possibilities of such events. The developed methods should allow the counteracting of cyber-attacks adequately to the level of threat.

FUNDING

A publication based on the results of the 5th phase of the multi-annual programme "Improvement of safety and working conditions", financed in the years 2020-2022 for scientific research and development works from the funds of the Polish National Centre for Research and Development (project no. IIPB18, Method of risk analysis conducted by machine designers taking into account aspects of cyber security). Programme coordinator: Central Institute for Labour Protection — National Research Institute, Warsaw, Poland.

REFERENCES

[1] Dźwiarek, Marek. 2004. "An analysis of Accident Caused by Improper Functioning of Machine Control Systems". *International Journal of Occupational Safety and Ergonomics* 10 (2) : 129–136.

[2] Dźwiarek, Marek. 2006. 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.). London: Taylor & Francis Group.

[3] Ota, Yuitaka, Tomomi Aoyama, Davaadorjet Nyambayar, and Ichiro Koshijima. 2018. "Cyber incident exercise for safety protection in critical infrastructure". *Int. J. of Safety and Security Eng*. 8 (2) : 246–257.

[4] Barnert, Tomasz, Kazimierz T. Kosmowski, and Marcin Śliwiński. 2010. Integrated functional safety and security analysis of the process control and protection systems with regard to uncertainty issue. In *Proceedings of the 10th International Conference on Probabilistic Safety Assessment and Management, PSAM 2010*; Seattle, WA; United States.

[5] Lichte, Daniel, and Kai-Ditrich Wolf. 2019. Bayesian Network Based Analysis of Cyber Security Impact on Safety. In *Proceedings of the 29th European Safety and Reliability Conference (ESREL)*.
[6] PN-EN ISO 12100:2011. *Bezpieczeństwo maszyn. Ogólne zasady projektowania. Ocena ryzyka i zmniejszanie ryzyka*.
[7] ISO/TR 22100-4:2018. *Safety of machinery - Relationship with ISO 12100 - Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects*.
[8] PN-EN 138491-1:2016-02. *Bezpieczeństwo maszyn - Elementy systemów sterowania związane z bezpieczeństwem - Część 1: Ogólne zasady projektowania*.
[9] IEC TS 62443-1-1:2009. *Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models*.
[10] IEC TR 63069:2019. *Industrial-process measurement, control and automation - Framework for functional safety and security.*

Ochrona informatyczna związanych z bezpieczeństwem systemów sterowania maszynami w Przemyśle 4.0

Marek DŹWIAREK

Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy
ul. Czerniakowska 16, 00-701 Warszawa

Streszczenie. Celem badań było opracowanie uwzględniania zagrożeń nieuprawniona interwencją w systemy informatyczne w procesie oceny ryzyka prowadzonego przez projektantów systemów sterowania maszynami. W tym celu przeprowadzono analizę typowych struktur związanych z bezpieczeństwem systemów sterowania w aspekcie możliwości i skutków utraty funkcji bezpieczeństwa w wyniku niepożądanych ingerencji. Określono zalecenia postępowania „krok po kroku" w kolejnych etapach analizy ryzyka.
Słowa kluczowe: Przemysł 4.0, Cyber bezpieczeństwo, bezpieczeństwo maszyn.