Jan PRZYBYLSKI
Institute for Sustainable Technologies – National Research Institute, Radom
jan.przybylski@itee.radom.pl

CONCEPT OF A MACHINE SAFETY SYSTEM FOR A MODULAR PVD TEST STAND

Key words

Safety system, machine safety, risk assessment, safety controller, PA-PVD technology device.

Abstract

The article presents the concept of a machine safety system for a modular PVD test stand. The specificity of the device means that nearly all kinds of hazards can be observed in it. The ones that are analysed in this paper are mechanical (machine) hazards according to the 2006/42/WE Directive on Machinery. The author discusses the methods of risk assessment, the rules of safe machine stopping, and safety functions. The required level of safety of the machine is set and the hardware and functional structure of the designed machine safety system are described.

Introduction

Industrial devices and technological lines can be the source of hazards for both technical personnel operating them and for other people as well [1]. Table 1 delineates the most common hazards, the ways to minimize the risks and deal with their consequences. The hazards described in the paper can all, to a lesser or greater extent, occur in the test stand. The device has a modular structure. It is typically applied for the configuration according to the requirements of

a tested process or apparatus. Therefore, the occurrence of all hazards from Table 1 are characteristic for the stand. The article presents work on the creation of a safety system for hazards arising from the presence of moving parts in the stand.

Table 1 . Analysis of risks and the methods for their reduction and minimization of their effects

Hazard	Risk reduction	
	Design and construction stage	Operations stage
Mechanical (machine) hazards	– casings, housings, partitions – curtains – safety systems – marking of hazard zones	– health and safety training – protective equipment and clothing – periodic inspections
Risk of electric shock	– The use of insulating housings – PE systems – Graded protection against short circuit and overload – Differential switch – Difficult access to live parts – Construction of devices in accordance with the Low Voltage Directive – Marking of hazard areas	– Health and safety training – Personal protective equipment and the use of appropriate tools – The requirement to have appropriate authorization allowing the repair and maintenance of the device
Fire hazard	– The use of non–inflammable materials – Smoke and fire detectors – Automatic fire extinguishing systems	– Health and safety and fire training – Periodic testing of fire equipment (fire extinguishers, blankets, etc.) – Periodic inspection of rooms in terms of fire hazards
Risk of explosion	– Construction of equipment in accordance with the ATEX Directive – Systems for the detection of the presence and level of maximum allowable concentration of explosive gases – The use of anti-explosion cabinets – Adequate ventilation of rooms	– Health and safety training – Periodic inspections of safety systems and diagnostics
Chemical contamination	– Proper storage of chemicals – Detection of contamination – Fume hoods – Ventilation systems	– Health and safety training – Personal protective equipment and clothing – periodic medical examinations
Ionizing radiation	– Casings and partitions reducing radiation – Permanent monitoring of radiation levels in the workplace – Appropriate marking of hazard zones	– Health and safety training – Personal equipment for the measurement of the dose of the absorbed ionizing radiation (dosimeter) – Periodic medical examinations

1. Aspects of machine safety in the PVD stand

The test stand for PVD processes [2] is built based on a specialized vacuum chamber in which both PVD processes using magnetron and arc sputtering and glow discharge processes can be carried out. An important stage of the technological process is the batch loading and unloading stage, which takes place in a working chamber in a specialized rotating rack. This solution requires user safety to be guaranteed. This issue must be resolved in accordance with the 2006/42/EC Directive on Machinery [3, 4]. The methodology for estimating and eliminating risk in accordance with this directive, and defined by the PN-EN ISO 13849-1 standard, is shown in the diagram in Figure 1. The algorithm needs to be used for all types of hazards.

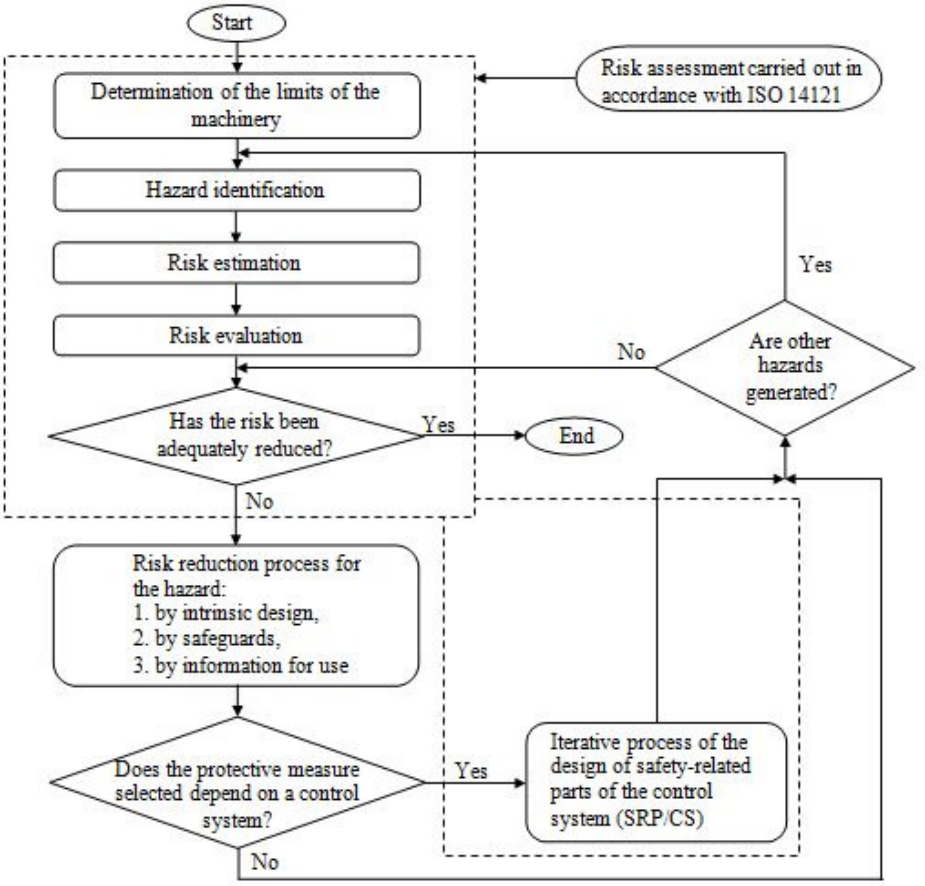

Fig. 1. Procedure for risk assessment and elimination according to the Directive on Machinery [5]

The issues of detailed risk assessment are covered by the PN-EN ISO 13849-1 [5] standard, which replaced the PN-EN 954-1 standard, which expired on 31 December 2009. The previous standard was based on the estimated risk and was divided into categories of safety B, 1, 2, 3, and 4. In the PN-EN ISO 13849-1 standard, the parameter for the assessment of safety circuits is the function defining the system's resilience to the loss of the safety function (Performance Level – PL), which includes reliability parameters. This standard mainly focuses on aspects related to mechanical and hydraulic hazards. The method of risk assessment according to this standard is shown in Figure 2, where PLs are marked with the letters from "a" to "e," where "a" reflects the lowest risk and "e" reflects the highest.

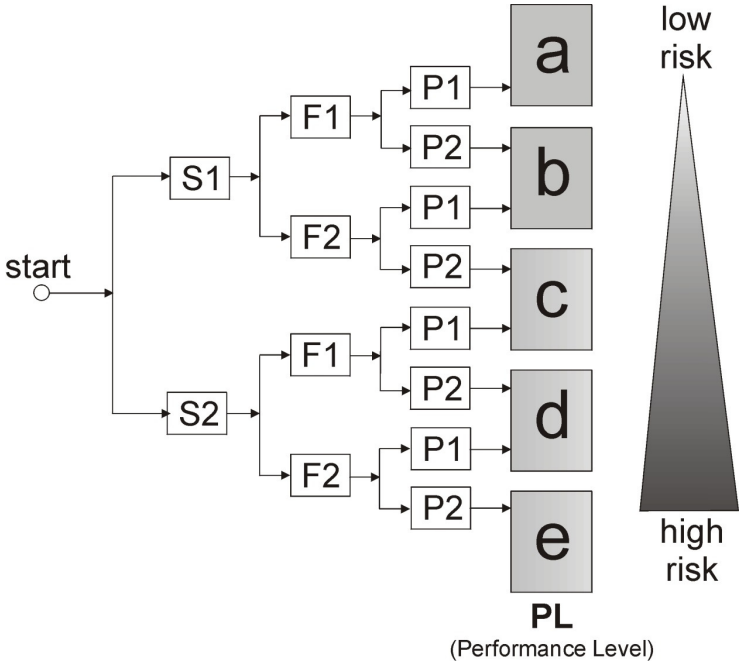

Fig. 2. Risk estimation according to the PN-EN ISO 13849-1 standard [5]:
S – severity of injury
S1 – light (reversible), S2 – severe (irreversible / death)
F – time and/or frequency of exposure to danger
F1 – rare / average, F2 – often / permanent
P – possibility to prevent hazards or limit their consequences
P1 – possible under certain conditions, P2 – almost impossible

The EN/IEC 62061 standard [6], which fully replaced the IEC 61508 standard, concerns machine safety depending on programmable control systems. This standard is mainly concentrated on electric and electronic programmable

safety systems and applies Safety Integrity Levels (SILs). Most current standards concerning the aspects of safety refer to the EN ISO 13849-1 standard, which in industry is far more often used as a standard norm. Good knowledge of issues covered by both the standards enables better and optimal performance of safety functions, since these matters can be accurately addressed in one of these standards. The method of risk estimation according to the EN/IEC 62061 standard is delineated in Table 2, where individual SILs are represented by numbers 1 through 3. The higher values in the table stand for the higher level of risk, and no SILs are defined for safe devices.

Table 2. Risk estimation method according to the EN/IEC 62061 standard [6]

Frequency (and occurrence time) **F**		Probability of hazard occurrence **O**		Possibility to avoid hazards **P**	
=<1h	**5**	frequent	**5**	impossible	**5**
>1h =<day	**5**	probable	**4**		
>1day =<2weeks	**4**	possible	**3**	possible	**3**
>2weeks =<1year	**3**	rare	**2**		
>1year	**2**	irrelevant	**1**	probable	**1**

Effect	Severity **S**	Class **C = F + O + P**				
		3-4	5-7	8-10	11-13	14-15
Death, eye or arm loss	**4**	**SIL 2**	**SIL 2**	**SIL 2**	**SIL 3**	**SIL 3**
Disability, finger loss	**3**			**SIL 1**	**SIL 2**	**SIL 3**
Reversible, treatment	**2**				**SIL 1**	**SIL 2**
Reversible, first-aid	**1**					**SIL 1**

Both standards specifying PL and SIL levels and are correlated and define the limits of acceptable Probability of Dangerous Failure per Hour (PFH_d). The figure dependencies can be found in Figure 3. Both methods of risk assessment [7, 8] can be used to determine the requirements to be met by the designed safety system.

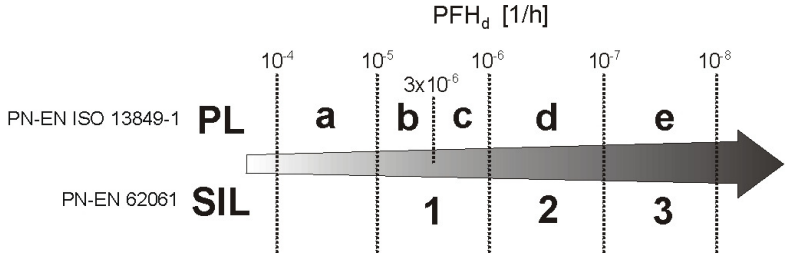

Fig. 3. Correlation between PL and SIL levels

An important element in the system ensuring the safe operation of machines is an aspect directly related to the stopping of machines to which the PN-EN 60204-1 [9] is devoted. It specifies three categories of machine stop, described as Category 0, 1 and 2 Category 0 is a solution often used in older machines, where the stop function is uncontrolled, and this process consists in an immediate disconnection of the machine from power. In the case of large rotating masses, this process can take some time, and the machine operator may not be provided with enough safety. It is by far safer to stop the machine according to Category 1 in which the stopping process is completely controlled when the power is on, and the power is disconnected only when the machine is switched off, which allows a shorter time for the machine to stop through, e.g., the braking process.

Stopping the machine in both these categories leads to a complete stop and the disconnection of power from all the drives, but there are situations that require continuous, but limited operation of the drive. Such a situation is embraced in Category 2 of machine stop, performed by reducing the speed or power.

2. Performance of safety functions by dedicated control systems

Safety functions should be performed based on one of the three defined architecture variants, dependent of the safety category, as defined in the PN-EN 13849-1 standard, which in turn depend on the Performance Level (PL), Diagnostic Coverage (DC), and the Mean Time to Dangerous Failure MTTFd. The basic option is the solution for safety Category B or 1, based on a single-channel structure constituting an input serial connection (I), from which the signal is transmitted to the logic element (L), and the signal generated by the output element (O) performs the safety function, as shown in Figure 4.

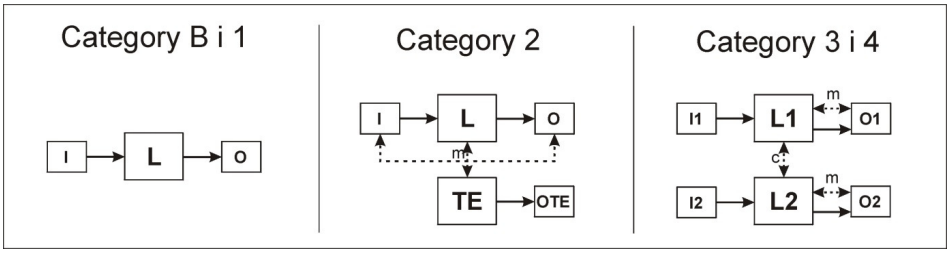

Fig. 4. Variants of the hardware architecture for safety functions in accordance with the PN-EN ISO 13849-1 standard [5]:
I (I1, I2) – input (sensor), L (L1, L2) – logics (performance of a function),
O (O1, O2) – output, TE – test modules, OTE –TE output,
m – monitoring, c – cross monitoring

The variant for Category 2 is more developed. In this solution, there is one input circuit and two output circuits; the first performs in the same way as in the case of the first solution, whereas the second is based on the diagnostic element (monitoring). This solution significantly increases the safety level, because the monitoring element (TE) checks the correctness of the operation of both the input and the basic output circuits, and the logic element, and if irregularities are detected, through its output circuit (OTE), which performs a "safe stop" function and notifies the operator about the situation. The third variant of the solution concerns Categories 3 and 4 and consists in the determination of two independent safety circuits, which additionally are mutually monitored.

3. Determination of the required performance level (PLr) for a PVD stand

In the developed test stand for PVD processes, a turntable located in the working chamber containing a special stand supporting parts whose surface layers undergo processing are placed constitutes the main hazard for its user. The determination of the required performance level (PLr) is discussed in detail in Annex A to the PN-EN ISO 13849-1, and it is performed according to the algorithm shown in Figure 1 in which three basic aspects connected with the hazards arising from the operation of the device (machine) need to be assessed.

When analysing the operation of the turntable, it can be assumed that it can cause reversible body damage, and the operator can frequently be exposed to danger stemming from the need to load and unload the parts during each technological process. Therefore, proper health and safety functions should eliminate the danger of the hazard occurrence. Based on this assessment, in the test stand, at least the PLr = b level needs to be achieved, which corresponds to SIL Level 1.

4. Concept of a safety system for a drive of a turntable of a PVD stand

Safety standards do not directly say how a system should be designed, but they give quantitative safety parameters that must be met, thereby providing the designer of the system with the possibility to consider different alternative variants in order to get the information necessary to achieve a desired level of safety for the developed system. This approach is consistent with the economic approach to system design, including the following: fewer losses in production, the production of higher quality products, the reduction of maintenance costs, the ability to schedule maintenance, lower costs of risk, and compliance with regulations [10].

The PVD test stand is a modular device whose configuration can be easily modified, enabling flexible adaptation to the requirements arising from the need to test new hardware solutions or innovative materials engineering technologies,

which can also make it necessary to introduce any possible changes to their safety systems. This, due to the application of a safety controller, is easy to perform. In its basic version, the safety system concerns two drives that enable the creation of a system for the movement of parts on which surface layers are deposited in a working chamber. In the initial phase of the technological process, in order to arrange parts on a specialized rack, the start-stop operation of these drives is necessary when the chamber door is open. A similar situation occurs in the final phase of the technological process, in which the parts are removed from the rotating rack.

In order to ensure safe conduct of the two phases of the technological process, a safety system was developed. Its structure was determined based on the analysis of commercial solutions by companies specializing in the development of solutions for the safety of machinery [11] and producing electric safety systems [12]. The structure of the system is presented in Figure 5. In the structure, a programmable safety controller, the use of which allows further expansion and modernization of the stand with simultaneous modification of the safety system, is used.

The developed safety system is based on four input elements connected to the safety controller. One of them is the sensor detecting if the working chamber door is closed, and one is a safety switch placed directly by the chamber door. Both elements constitute the basis of the system.

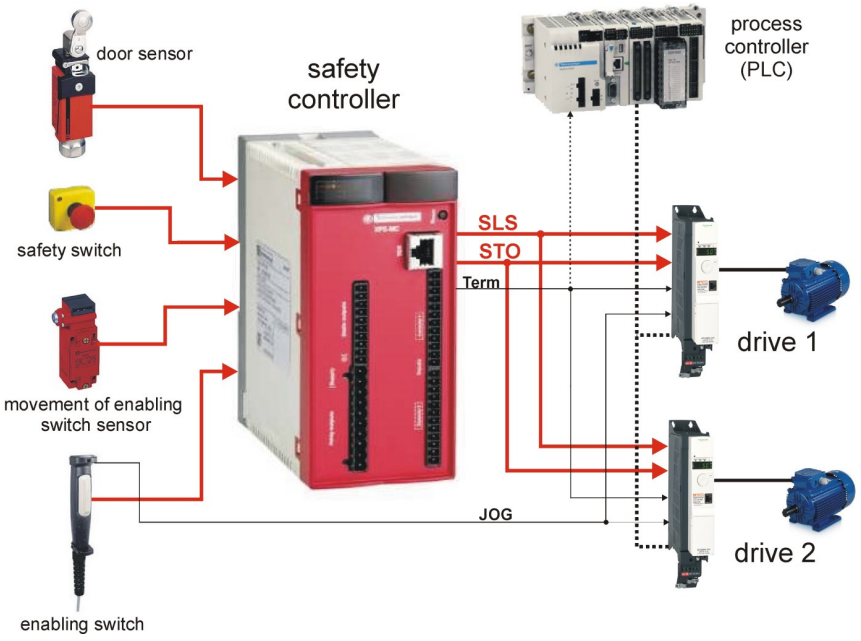

Fig. 5. Concept of a safety system for a PVD stand

To ensure safe operation of drives of the turntable, the safety system was equipped with two additional elements, the first of which is an enabling switch with an additional button allowing the operator to start the drives in a controlled manner. The second additional element is a sensor detecting the move of the enabling switch from the stand-by position.

Opening the door of the working chamber makes the drives quickly switch into the stop mode according to Category 2 specified by the PN-EN 61800-5-2:2007E standard [13], which enables the drives to work at safe speed. This is achieved by transferring the signals from the controller onto the SLS inputs (Safe Limited Speed), which helps the operator to verify the accuracy of the arrangement of parts in a specialized rack in the working chamber. Pressing the safety button initiates the transmission of the STO signal (Safe Torque Off) onto the inputs of motor controllers, which forces a complete stop of both drives. The transition to this mode also takes place when the door of the chamber is open and the enabling switch is removed from the stand-by position, which additionally results in a change in the drive control system from the network control (control via PLC using CANopen) to the local control using direct digital signals from motor controllers by transmission onto proper TERM signal inputs.

This solution enables full and safe control of the drives only by the operator who has the enabling switch in his hand. Holding this switch with proper force and in a correct position (not pressed) of the safety switch enables the STO signal to be turned off and the additional auxiliary button for the JOG signal to be switched on, which guarantees safe operation of the drives at a limited speed specified in the configuration of the drive controller. Closing the door of the chamber and not pressing the safety button will bring back regular control, based on a local CANopen network.

Summary

In many devices which are still used for PVD technologies, the aspects of the reduction of hazards emerging from the presence of dangerous moving parts has not yet been fully resolved. The current Directive on Machinery requires the designers and developers of devices to ensure maximum safety for their service. The developed safety system for a test stand enables the minimization of the risks arising from the presence of moving parts. This system can be applied for other types of devices. The solution and the analysis of the estimation and assessment of mechanical hazards can be used to build safety systems for other devices and technological lines containing dangerous moving parts. After determining the safety level based on the calculations, taking into account the structure and qualitative parameters of the components used, the safety system will form a basis that will further be expanded with new elements allowing the minimizing of other risks that can occur in this stand.

Scientific work executed within the Strategic Project "Innovative Systems of Technical Support for Sustainable Development of Economy" within Innovative Economy Operational Programme.

References

1. Abrahamsen E.B., Asche F., Milazzo M. F.: An evaluation of the effects on safety of using safety standards in major hazard industries. Safety Science, 59 (2013) pp. 173–178.
2. Przybylski J., Majcher A.: Modułowe stanowisko badawcze dla procesów PVD pozwalające na wdrażanie nowatorskich technologii. Problemy Eksploatacji 3, pp. 197–204 (2011).
3. Dyrektywa 2006/42/WE z dn. 17 maja 2006 r. (PL) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:157:0024:0086:pl:PDF
4. Directive 2006/42/EC of The European Parliament and of The Council of 17 may 2006 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:157:0024:0086:en:PDF
5. PN-EN ISO 13849-1:2008/AC:2009 Bezpieczeństwo maszyn – Elementy systemów sterowania związane z bezpieczeństwem – Część 1: Ogólne zasady projektowania.
6. PN-EN 62061:2008/A1:2013_06E Bezpieczeństwo maszyn – Bezpieczeństwo funkcjonalne elektrycznych, elektronicznych i elektronicznych programowalnych systemów sterowania związanych z bezpieczeństwem.
7. Hietikko M., Malm T., Alanen J.: Risk estimation studies in the context of a machinery control function. Reliability Engineering and System Safety, 96 (2011) pp. 767–774.
8. Smith D.J., Simpson K.G.L.: Safety Critical Systems Handbook. A Straightforward Guide to Functional Safety: IEC 61508 (2010 Edition and Related Standards Including: Process IEC 61511, Machinery IEC62061 and ISO 13849. Third Edition – 2011. Published by Elsevier.
9. PN-EN 60204-1:2010P Bezpieczeństwo maszyn – Wyposażenie elektryczne maszyn – Część 1: Wymagania ogólne.
10. Goble W. M.: Control systems safety evaluation and reliability. 3rd ed. – 2010. International Society of Automation. NC27709.
11. Pilz. The new Safety Compendium http://www.pilz.com/imperia/md/content/documentation/offen/produkt_bergreifend/promotional_literature/Safety_Compendium_UK_Version_12-12.pdf?redirected=true.

12. Schneider-electric. Machine Safety Guide http://download.schneider-electric.com/files?p_File_Id=27569309&p_File_Name=dia4ed1100102en%28web%29.pdf.
13. PN-EN 61800-5-2:2007E Elektryczne układy napędowe mocy o regulowanej prędkości – Część 5-2: Wymagania dotyczące bezpieczeństwa – Funkcjonalne.

Koncepcja systemu bezpieczeństwa maszynowego modułowego stanowiska badawczego PVD

Słowa kluczowe

System bezpieczeństwa, bezpieczeństwo maszynowe, ocena ryzyka, kontroler bezpieczeństwa, urządzenia technologiczne PA-PVD.

Streszczenie

W artykule omówiono koncepcję systemu bezpieczeństwa maszynowego stanowiska badawczego technologii PVD. Specyfika tego urządzenia powoduje, że występują w nim praktycznie wszystkie możliwe typy zagrożeń. Analizie poddano zagrożenia mechaniczne (maszynowe) zgodnie z wytycznymi dyrektywy 2006/42/WE. Przedstawiono metody szacowania ryzyka, zasady bezpiecznego zatrzymania maszyny oraz metody realizacji funkcji bezpieczeństwa. Wyznaczono wymagany poziom bezpieczeństwa urządzenia oraz opisano strukturę sprzętową i funkcjonalną opracowanego dla niego systemu bezpieczeństwa maszynowego.