PRACTICAL EXAMPLES OF THE DETERMINATION OF PERIODICAL INSPECTION FREQUENCY IN MACHINERY SAFETY SYSTEMS

Marek DŹWIAREK[*]

[*]Central Institute for Labour Protection – National Research Institute, ul. Czerniakowska 16, 00-701 Warsaw, Poland

madzw@ciop.pl

Abstract: The paper deals with the problem of choosing an appropriate inspection interval for monitoring of safety related control systems in machinery. According to international standards the safety related systems are categorized according to their Safety Integrity Levels or Performance Levels, depending on their reliability parameters. Extremely simple, approximate models have been proposed in order to provide practitioners without reliability training with useful tools for the determination of inspection policies. The method(s) based on the required availability of the system. The paper presents some practical examples of systems of categories B, 1 and 3, respectively. The frequencies of periodical inspection are calculated for: system monitoring closure of the door, behind which a dangerous element moves slowly, system of monitoring the access door on the automated production line and system, in which a light curtain is employed to monitor the access to the dangerous zone of an automatic assembly machine.

Kay words: Safety of Machinery, Safety Related Parts of Control System, Functional Safety, Periodical Inspection

1. INTRODUCTION

In the course of electronic technology development it can be observed that machine control systems despite their operational functions perform also more and more safety functions. More and more complex electronic systems, for example vision systems (Grabowski et al., (2011)), are applied as protective systems for machinery. General roles for application of such systems are well known and it is described, for example by Dźwiarek (2010). But the most important problem is ensuring proper functioning of the system on demand. The analyses of accidents happened in the course of machine operation presented in Dźwiarek (2004) showed that 36% of them were caused by improper functioning of the machine control systems. Additionally, in the group of accidents caused by improper functioning of machine control systems serious accidents happened much more frequently (41%) as compared to the group of accidents with no relation to the control system (7%). Most common cause of such accidents consisted in the lack of safety functions (58%). Most often, functions like monitoring of guard position or presence in the dangerous zone were missing. Other group of accidents comprises those caused by failure of a safety-related element of the control system due to insufficient resistance to fault (26% of all accidents). Other reported causes, i.e., mistakes in definitions of safety functions (4%), errors in control system software (6%) too low resistance to environmental effects (climatic agents, power supply distortion – 6%) affected much lower number of the accidents happened. Those results proved that machine control systems are very important in view of the safety of machine operators. Therefore, designers of the safety related control systems should apply the structures that improve their resistance to fault, which most frequently means the application of reliable elements and redundant architecture of the systems. But, in preventing the accidents due to improper operation of the control system periodical inspection of its functioning is also of crucial importance. Therefore, the control system designer should specify how often the system should undergo the periodical inspection. Unfortunately, in the binding standards, there are no suggestions on how to determine the frequency of periodical inspection of the control system. The aforementioned problem has been discussed many times at meetings of the working group VG11 "Safety components" of the European Co-ordination of Notified Bodies for Machinery and Safety Components (Machinery Directive 2006/42/WE), however, no satisfactory solution has been found yet, thus the Recommendation for Use could not be developed. The research aimed at formulation of the rules for determination of periodical inspection frequency of safety related parts of control systems in machinery, as simple as possible so as to ensure that their possible defect would be detected early enough. The results of these studies have been presented in Dżwiarek and Hryniewicz (2011). The paper shows sample practical applications of those methods.

2. SAFETY FUNCTIONS PERFORMED BY THE MACHINERY CONTROL SYSTEM

Most often, a machinery control system performs both the safety functions and those irrelevant to safety. A safety function is a function, a failure of which can increase risk(s). Generally, the safety function can be implemented for the reduction of risk associated with the following three groups of hazards (Dźwiarek, 2007):

- resulting from improper machine operation,
- resulting from the application of technological processes the physical parameters of which differ significantly from standard environmental conditions,
- mechanical hazards.

The following safety functions are most common:

- safety-related stop function initiated by a safeguard,
- manual reset function,

- start/restart function,
- local control function,
- muting function,
- monitoring of parameterization of the safety-related input values,
- response time,
- monitoring of safety-related parameters such as speed, temperature or pressure,
- reaction to fluctuations, loss and restoration of power sources.

Since failure of those functions can increase the risk, therefore the designers of safety related control systems should apply the structures that improve their resistance to fault. Basic rules for improving the machinery control system resistance to fault were formulated in the following standards (Dźwiarek 2006, Dźwiarek 2007):

- IEC 62061:2005 „Safety of machinery - functional safety of safety-related electrical, electronic and programmable electronic control systems",
- ISO 13849-1:2006 „Safety of machinery. Safety-related parts of control systems - Part 1: General principles for design", where, depending on their behaviour under fault conditions the devices were classified into 5 categories.

In standard IEC 62061:2005 the functional safety methodology formulated in IEC 61508:2001 "Functional safety of electrical/ electronic/ programmable electronic safety-related systems" was adapted so as to be applicable to machinery control systems. For each safety-related control system performing the defined safety-related function the probabilistic criteria for assessing their resistance to fault (named the Safety Integrity Level) are defined in IEC 62061.

Standard ISO 13849-1 formulates a simplified method for the assessment of machinery control systems. The following parameters are characteristic of each system: *Structure (Category), Mean time to failure (MTTF), Diagnostic coverage (DC) and Common cause failure factor (CCF)*. Those parameters are divided into the following qualitative groups: high, medium, low. The expected safety performance level is determined from a graph into which the assessed parameters and the system architecture (single channel, redundancy, monitoring, etc.) have been included. It allows for assessment of the designed system in a relatively simple way. The performance level (PL) represents the system resistance to faults. The relationship between the performance level (PL) and SIL is given in Tab. 1.

Tab. 1. Relationship between the Performance Level and SIL (ISO 13849-1)

Performance level (PL)	Probability of a dangerous failure per hour *(PFH_D)*	Safety integrity level (SIL)
a	[10^{-5}, 10^{-4})	No correspondence
b	[$3x10^{-6}$, 10^{-5})	1
c	[10^{-6}, $3x10^{-6}$)	1
d	[10^{-7}, 10^{-6})	2
e	[10^{-8}, 10^{-7})	3

According to both the aforementioned standards the designer of machinery control system should determine, taking into account the results of risk assessment, the required SIL or PL for each safety function performed by the control system. The required SIL or PL should be achieved by applying the design solutions appropriate for the considered control system. The required SIL or PL should be also maintained during the whole life time of machinery. The long-term results of using a machine usually involve consistent degradation of its sub-assemblies, due to both material deterioration and mechanical wear. The aforementioned phenomena can lead to decrease of the achieved SIL or PL. It means that all safety functions should be periodically inspected for identification of any changes in their parameters, which can reduce the ability of control system to perform its functions.

3. SIMPLIFIED ALGORITHMS FOR THE DETERMINATION OF INSPECTION INTERVALS FOR THE SAFETY RELATED CONTROL SYSTEMS

The determination issues of periodical inspection frequency of safety related systems were analyzed mainly in view of the critical infrastructure in processing industry (Taghipour et al., (2010). That resulted mainly from both the hazard levels arising there as well as high costs of stopping the process to make the inspection including its performance costs. As a result, very complicated procedures were developed for the determination of periodical inspection frequency of such systems. The procedures are far too much complicated and expensive to be applied to periodical inspection of safety devices in machinery. Mainly, due to their mathematical complexity. Therefore, the simplified procedures presented by Dźwiarek and Hryniewicz (2011) and Dźwiarek and Hryniewicz (2012) are much more suitable in such cases.

Let us consider the simplest case when the inspection allows for immediate checking if a system is ready to perform its safety function or not. The assumption that the "probability of a dangerous failure per hour" remains constant over the whole life cycle of the machine accepted in standards ISO 13849-1 and IEC 62061 means that also the availability of the system should remain unchanged in every year of its exploitation. The availability of the system, when its time to failure is represented by the exponential distribution, is given by the following simple formula:

$$A(T) = \frac{1}{PFH_D T}(1 - e^{-PFH_D T}) \qquad (1)$$

If $PFH_D T$<<1, then the following approximation can be applied:

$$A(T) \approx 1 - \tfrac{1}{2} PFH_D T + \tfrac{1}{6}(PFH_D T)^2 \qquad (2)$$

Taking into consideration the values of PFH_D given in Tab. 1 we can determine the required availability of the system per year A_r (see Tab. 2).

Tab. 2. Required availability of the system per year for particular values of SIL and PL (Dźwiarek and Hryniewicz, 2011)

Performance level (PL)	A_r	Safety integrity level (SIL)
a	0.957	No correspondence
b	0.987	1
c	0.997	1
d	0.99956	2
e	0.999956	3

In should be noted, that for the purposes of risk assessment from among the variety of possible faults one should select the dangerous ones; i.e., those causing the safety function loss, to be considered in the process. For example, in a redundant system a failure of one channel may not necessary result in safety function loss for the whole system, since it the function is performed by the second channel. Therefore, the periodical inspections aim at detecting the faults that however do not cause the safety function loss but still result in reducing the values of SIL or PL.

According to Hryniewicz (2008), if we set the required value of the availability A_r we can find the inspection interval T_0 by solving the equation $A(T_0)=A_r$. Thus, that value can be found from the expression:

$$A_r = 1 - \tfrac{1}{2}\lambda T + \tfrac{1}{6}(\lambda T)^6 \tag{3}$$

where λ stands for the probability of any failure, not only the dangerous one.

Hence, the required inspection interval should be calculated from the following equation:

$$T_0 = \frac{3-6\sqrt{0.25-\frac{2}{3}(1-A_r)}}{2\lambda} \approx \frac{2(1-A_r)}{\lambda} \tag{4}$$

When the safety related control system has a parallel structure with two channels represented by the exponentially distributed random variables characterized by the failure rates λ_1 and λ_2, respectively, we can use the procedure proposed in international standard ISO 13849-1, Annex D that allows one to approximate this system using an equivalent one having two identical channels characterized by the failure rate calculated from the following equation:

$$MTTF_m = \tfrac{2}{3}(MTTF_1 + MTTF_2 - \tfrac{1}{MTTF_1+MTTF_2}) \tag{5}$$

Then, we can use:

$$T_0 = \tfrac{1}{\lambda}\sqrt{2(1-A_r)} \tag{6}$$

in calculation of the inspection interval.

When the inspection and repair times cannot be neglected, Hryniewicz (2008) proposed the following formula for calculation of the optimal values of inspection intervals:

$$T_0 = \sqrt{\tfrac{2\mu_0}{\lambda}} \tag{7}$$

were μ_0 means the time required for inspection and repair.

4. CASE STUDIES

The method presented above for determination of periodical inspection frequency of safety-related control systems in machinery was put into practice in systems of different complexity and different requirements for their fault resistance. Usually, periodical inspections of machines are carried out during their idle times and the duration of such inspection is negligible as compared to the machine working time. There are, however, cases in which the inspection time cannot be neglected, therefore both the cases have been considered.

4.1. A system of category B

The simplest systems of category B according ISO 13849-1 are applied in the case when risk from the hazard being reduced is very small. A typical case consists in monitoring the closure of the door, behind which a dangerous element moves slowly. In such a case the risk assessment carried out following the A1 graph shown in standard ISO 13849-1 leads to the required performance level PL_r of b and $3x10^{-6} \leq PFH_{Dr} < 10^{-5}$.

A proximity switch is usually applied to monitor the door closure state. A sample system of that type is shown in Fig.1. When the guard opens the power supply to motor M is cut off by relay Q1, controlled by proximity switch C1. C1 is a classical proximity switch of $MTTF_D$ equal to 30 years. According to the manufacturer's declaration the electrical switching capacity of Q1 is $B_{10}Q1$= 10 000.

Since in the considered case the access door to the dangerous zone is to be opened every hour and the fraction of dangerous failure is 50% we can determine:

$$\begin{aligned} MTTFQ1 &= 10000/0.1*8*365 = 34 years \\ MTTF_D Q1 &= 2*MTTFQ1 = 68 years \end{aligned} \tag{8}$$

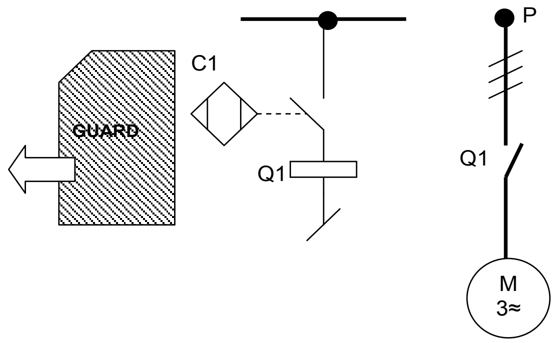

Fig. 1. Sample control system of category B

Finally, for the safety function we have:

$$\begin{aligned} MTTF_D &= \tfrac{1}{\frac{1}{30}+\frac{1}{68}} = 20 years \\ PFH_D &= \tfrac{1}{24*365*20} = 5.71*10^{-6} \\ \lambda &= 2*PFH_D 1.14*10^{-5} \end{aligned} \tag{8}$$

In the case of systems of category B with no embedded mechanisms of fault detection, in which a single fault causes the loss of safety function, it is necessary to make periodical inspections. In that case the inspection consists in actuation of safety functions and verifying that the dangerous motion has been stopped. Therefore, the inspection is simple and of short duration.

In that case we apply formula (6). According to Table 2 we have:

$$T_0 = \frac{2(1-0,987)}{1.14*10^{-5}} = 2280h \approx 3month \tag{9}$$

4.2. A system of category 1

If the access door is situated by the automated production line it is opened very rarely, while the hazards created are much greater. In such a case the protection level ensured by a system of cat B is not high enough. The results of risk assessment lead to the required performance level PL_r of *c* and $10^{-6} \leq PFH_{Dr} < 3x10^{-6}$.

It can be achieved by means of using a device monitoring the door closing that satisfies the requirements of category 1 according ISO 13849-1. In such a case one should employ a limit switch manufactured in accordance with standard IEC 60947-5-1. Annex K. Also to stop the motor a contactor should be applied that satisfies the requirements specified for “well-tried elements” in Tab. D3 given in standard ISO 13849-2. For conrtoling the dangrous movement directional control valve 1V1 have been used.

In the manufacturer’s declaration of the limit switch it is B_{10} *K1* = 10^6, while in that of the contactor the durability is B_{10} *Q1* = 1.3x10^6 and f B_{10} *1V1* = 40x10^6.

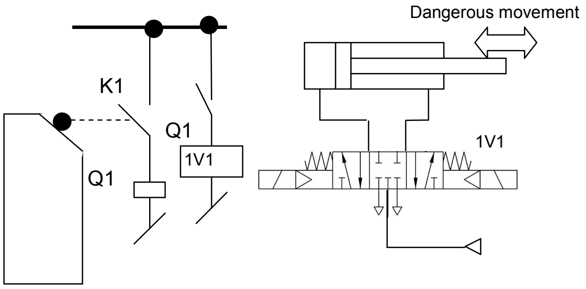

Fig. 2. Sample control system of category 1

Let us assume that the production line works twenty-four hours a day and the access to the dangerous zone should be provided once a week, and the valves 1V1 are activated every 2 minutes:

$$MTTF1V1 = 40*10^6 / 0.1(30*24*365) = 1530 years$$
$$MTTFK1 = 10^6 / 0.1*52 = 192300 years \qquad (10)$$
$$MTTFQ1 = 1,3*10^6 / 0.1*52 = 250000 years$$

and for the safety function, taking into consideration the fact that only half of faults are dangerous we have:

$$MTTF = \frac{1}{\frac{1}{1530}+\frac{1}{192300}+\frac{1}{250000}} 1510 years$$
$$MTTF_D = 2*MTTF = 3020 years \qquad (11)$$

According to standard ISO 13849-1 the maximal value of $MTTF_D$ for the system of category 1 is 100 years and:

$$\lambda = PFH_D = 1.14*10^{-6} \qquad (12)$$

To carry out the inspection of automated production line it is necessary to stop it over the whole length. Stopping the whole production line and then restarting it is rather time-consuming and creates the need for engaging a special supervising crew, which may take a few hours. Upon the application of formula (7) we have:

$$\mu_0 = 4h$$
$$T_0 = \sqrt{\frac{2\mu_0}{\lambda}} = 2650 \approx 4 month \qquad (13)$$

Which means that the safety function should be checked at least once every three months.

4.3. A system of category 3

Another example consists in the system in which a light curtain is employed to monitor the access to the dangerous zone of an automatic assembly machine. In such a system there arises a hazard of amputation, the access to the dangerous zone is required every 1 minute and the hazard can be easily avoided. In that case the risk assessment leads to the required performance level PL_r of *d* and $10^{-7} \leq \lambda_r < 10^{-6}$.

In view of high frequency of its activation the system of category 3 according ISO 13849-1, the scheme of which is shown in Fig. 3, was chosen to perform the safety function. Light curtain LC has been certified as to be applied in systems up to category 4, SIL CL 3, PFH_D LC = 5x10^{-8}, as an input sensor with two line signalising interaption of detection zone. The signal from the curtain is transmitted to a standard PLC, therefore one should assume MTTF PLC = 25 years. The PLC switches contactor Q2, which disconnects the motor. Safety relay SR makes the redundant channel for PLC and it satisfies the requirements of category 4. In the manufacturer’s declaration is specified that PFH_D SR = 3x10^{-8}. The controller switches contactor Q1, which also disconnects the motor. In the manufacturer’s declaration of contactors Q1 and Q2 it is specified that the value of parameter B_{10} Q1, Q2 = 10^6. The PLC also monitored suplementary contact of Q1 and Q2. According ISO 13849-1, Annex E in this case the diagnostic coverage is DC=90%.

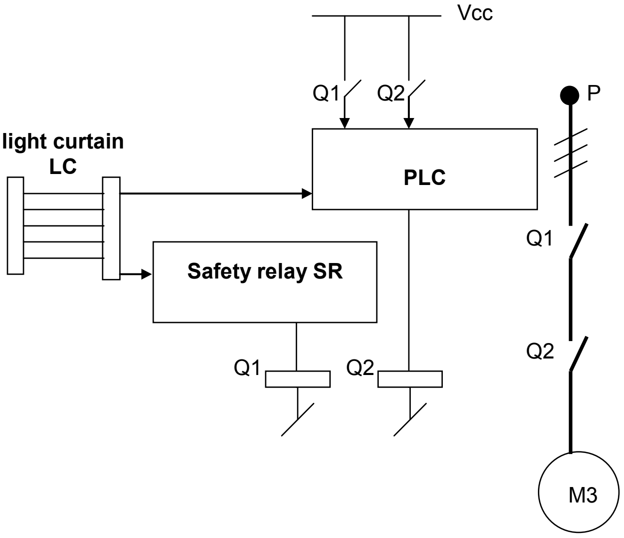

Fig. 3. Sample control system of category 3

The Reliability Block Diagram of the safety function is shown in Fig. 4.

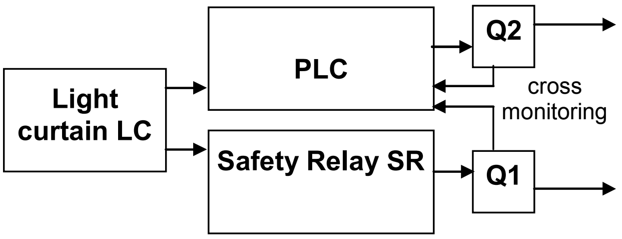

Fig. 4. Sample control system of category 3

Upon the assumption that the automatic machine works double shifts for 220 days per year and taking into consideration the demand frequency of the safety function we arrive at:

$$\begin{aligned} &MTTFQ1,Q2 = 47.3 years \\ &MTTF_D Q1,Q2 = 94.6 years \end{aligned} \tag{14}$$

Now, we can determine the value of MTTF for each channel:

$$\begin{aligned} &MTTF_D LC,PLC,Q2 = 19.77 years \\ &MTTF_D LS,SR,Q1 = 94.5 years \end{aligned} \tag{15}$$

and:

$$\begin{aligned} &MTTFLC,PLC,Q2 = 16.36 years \\ &MTTFLC,SR,Q1 = 47.2 years \end{aligned} \tag{16}$$

Upon application of the symmetrization formula (5) we have:

$$\begin{aligned} &MTTF_D = 65.28 years \\ &MTTF = 34.27 years \end{aligned} \tag{17}$$

According to ISO 13849-1, Table K1 we can assume:

$$\begin{aligned} &PFH_D = 2.13*10^{-7} \\ &\lambda = 3.33*10^{-6} \end{aligned} \tag{18}$$

In the aforementioned case the periodic inspection consists in actuation of the safety function and observation of light signals generated by the light curtain and controllers S1 and PLC. The frequency of periodic inspection can be determined uising formula (6):

$$T_0 = \frac{1}{3.33*10^{-6}} \sqrt{2(1-0.99956)} = 8906h \approx 1 year \tag{19}$$

5. CONCLUSIONS

The discussion presented above as well as the case study results prove that the assessment problem of resistance to faults revealed by a machine control system can be solved in a relatively simple way. Finnaly, we have found that the calculated periods of periodical inspections agree with commonly accepted rules for their conductance. The manufacturers of machines and protective devices should make such calculations and include the results into the "User manual" according to the requirements of Machinery Directive 2006/42/WE.

REFERENCES

1. **Dźwiarek, M.** (2004), An analysis of Accident Caused by Improper Functioning of Machine Control Systems, *International Journal of Occupational Safety and Ergonomics,* Vol. 10 No. 2, 129-136.
2. **Dźwiarek, M.** (2006), Assessment of software and hardware safety of programmable control systems of machinery, In: C. Guedes Soares & E. Zio (ed.) *Safety and Reliability for Managing Risk*, 2325-2330, Taylor & Francis Group, London, ISBN 978-0-415-42315-2.
3. **Dźwiarek, M.** (2007), Functional safety of machinery control systems - general consideration. In: Kosmowski K. T. (ed.) *Functional Safety Management in Critical Systems*: 101-114, Fundacja Rozwoju Uniwersytetu Gdańskiego, ISBN 978-83-7531-006-1.
4. **Dźwiarek**, **M.,** (2010), Basic Principles for Protective Equipment Application, In: *Handbook of Occupational Safety and Health* Koradecka, D., (ed.) © CRC Press, Taylor & Francis Group, LCC, *ISBN 978-1-4398-0684-5,* p.p. 579-592.
5. **Dźwiarek, M., Hryniewicz, O.** (2011), Periodical inspection frequency of safety related control systems of machinery – practical recommendations for the determination, In: Grall & Soares (eds.) *Advances in Safety, Reliability and Risk Management,* Taylor & Francis Group, London, ISBN 978-0-415-68379-1, 495 – 502.
6. **Dźwiarek, M., Hryniewicz, O.** (2012), Practical examples of determination of periodical inspection of safety related control systems of machinery (in Polish), *Przegląd Elektrotechniczny* 5a/2012, 290-295.
7. **Grabowski A., Kosiński R., Dźwiarek M.**, (2011) Vision safety system based on cellular neural *networks, Machine Vision and Applications,* Vol. 22, Issue 3 (2011), 581-590.
8. **Hryniewicz, O. H.** (2008), Optimal inspection intervals for maintainable equipment, In: Matorell S., Guedes Soares C., Barnett J. (Eds.): *Safety, Reliability and Risk Analysis. Theory, Methods and Applications,* Vol. 1., CRC Press, Boca Raton 2008, 581-586.
9. **Taghipour, S., Banjevic, D., Jardine, A.K.S**. (2010), Periodic inspection optimization model for a complex repairable system, *Reliability Engineering and System Safety*, 95, 944-952.

This paper has been prepared basing on the results obtained from a research task carried out within the scope of two first stages of the National Programme "Improvement of safety and working conditions" partly supported in 2008-2013 – within the scope of state services – by the Ministry of Labour and Social Policy. The Central Institute for Labour Protection – National Research Institute acts as the main coordinator of the Programme.