Designing machine safety control system according to an international standard

Suad Ibrahimkadić*, Slobodan Lubura **
* Tobacco factory Sarajevo/Maintenance department, Sarajevo, Bosnia and Herzegovina
** Faculty of Electrical Engineering/Automation and electronic department, Istočno Sarajevo, Bosnia and Herzegovina
suad.ibrahimkadic@fds.ba; slobodan.lubura@etf.unssa.rs.ba

Abstract – Since the safety has always been an important part of a control system, the new international standard EN ISO 13849-1 for safety of machinery is an important document that needs to be thoroughly read and applied in new projects. This paper provides some basic information about the standard and the way how it is used. The control system from a real project will be used as an example for design of some safety functions.

I. INTRODUCTION

Safe operation for human, as well as for the machinery, has always been an extremely important requirement for every industrial control system. As the technology advances, these requirements have been also becoming more demanding through the history.

In the 70's, the focus was on the safety of the manually operated presses, which was the most dangerous machine of that time [1].

During the 80's, the industrial robots started to become common part of a manufacturing process. These introduced new risks and new challenges to the safety, like unwanted start-up of a machine or safe stop of the machine. In the mid 80's, the first international machine safety standard was introduced (Safety in Industrial Robot Systems EN775/ISO 775).

During the 90's, the machine directive was a start of a very important international effort in creating a unified European standards for safety for machinery and safety devices. The experience from different countries contributed in creating work in safety much easier.

From the 2000 onwards, the work on safety was intensified within the ISO (The International Organization for Standardization). The aim was to have the safety requirements and standards within ISO as within EN (European Norm).

Currently, in the area of machine safety, two standards are being used:

1. EN 13849-1: Safety of machinery

2. EN 61508: Functional safety of electrical/electronic/ programmable electronic safety-related devices

These standards use different approaches, but lead to the same level of safety. While EN ISO 13849-1 is technology-independent, the EN 61508 is limited only to electrical/electronic/programmable electronic safety devices.

Currently, efforts are being made to take the best things from both of these standards and to create only one new standard that will be easier to follow. The job is expected to be finished by 2018.

Since the EN ISO 13849-1 applies to all safety-related parts of control systems (SRP/CS), regardless of the type of energy used in these systems (e.g. electrical, mechanical, pneumatic or hydraulic systems), the focus in this paper will be on this standard.

II. PROCESS TECHNOLOGY DESCRIPTION

In this chapter a brief introduction to the technology and hazards of the example manufacturing process will be presented.

A. Quick overview

Hot-dip galvanization plant, situated in company Surtec-Eurosjaj d.o.o. in Konjic, BiH, is a plant consisted of three main parts:

1. Chemical preparation
2. Preheating
3. Galvanization

Chemical preparation of the material is done in specially prepared boxes, where each of the boxes is filled with adequate liquid, depending on the technological effect required. There are 10 different boxes, in which the material passes through the following phases: Degreasing, Pickling, Washing, Fluxing and Drying.

The process starts at the filling station, where the material is manually loaded into the bins, so called drums. The drums are carried by a crane from one box to another, according to a predefined procedure. The crane operation mode can be manual or automatic. For each box a set of parameters are defined, including for example liquid temperature, remanence time, maximum time to be served etc. These parameters are a part of a recipe, which in general can be different for different boxes and different batches. In this way, full process flexibility is achieved.

After the last processing box is passed, the crane brings the drum into the unloading position, where the content of the drum is manually unloaded on a conveyor belt.

This is where the second segment of the plant starts. The preheating process consists actually of only one machine, called Preheating Tunnel. The conveyor belt carries the unloaded material through a heated chamber, exposing it to a controlled air temperature for predefined amount of time. The time is defined by the conveyor speed, which is, together with the air temperature, also parameter of a recipe. At the exit of the tunnel, a small industrial scale is installed with a metal bucket on it. When the scale weights more than a predefined value, the loading is stopped and the bucket is transferred to the third part of the plant.

The third segment of the plant consists of molten zinc bath, centrifugal device, cooling box and emptying station. The bucket is conveyed through these units by means of a second crane. The units to pass and processing to follow in these units are selected through the recipe. After the completion, the bucket is placed on the emptying station, where it is manually emptied.

B. Safety risks in the plant

Prior to identifying and analyzing the risks present in the plant, it is necessary to define the scope of the space that will be covered by this assessment. In this case, only the machinery itself, including the operator's working area, is included in this phase.

Due to the fact that the plant is situated on more than 80 square meters, with the presence of areas with liquids at extremely high temperatures (over 400 degrees Celsius), moving cranes, acids, rotating parts etc, there are numerous points where serious injuries or even death can occur. This is why particular attention must be paid to create adequate protections, and to bring the safety risk to a minimum level.

As already stated, there are numerous danger points, but in the following only a few of them will be mentioned:

1. Possibility for any of the cranes to stop out of the target point. In this case, either in manual or automatic mode, the drum can hit the wall of the processing box. Equipment can be damaged.
2. Possibility for the second crane to enter the molten zinc at a speed that is too high, so an furious reaction with spraying hot zinc can occur, causing serious or deadly wounds.
3. Closing the centrifugal unit. Heavy cover can be closed unintentionally, while an operator's inspection is being made. Serious injuries can occur.
4. Unexpected start-up of a crane can happen, during the operator's intervention. Serious injuries can occur.
5. Unexpected start-up of the moving platform in the centrifugal unit, while operator's intervention is being done.

Once the risks are identified, usually most of them can be avoided at the design stage. In some cases, the risk can be decreased to an acceptable level through installation of different protection barriers, visible danger signs, sound and/or light warnings etc.

In any case, information about the danger and the correct procedure to handle it must be provided in the manual supplied with the machinery.

However, if the identified risks could not be decreased to an acceptable level, or if it doesn't seem to be a practical and easy to use solution, then the design of control system should include safety devices. If the risk reduction is done in this way, the safety-related part of this control system needs to be designed according to EN ISO 13849-1.

III. DESIGNING SAFETY SYSTEM ACCORDING TO EN ISO 13849-1

In this chapter some basic information will be provided about the procedure to design safe machine control system.

A. Basic workflow

The EN ISO 13849-1 stipulates a workflow that needs to be followed until the safety function is validated [2]. The workflow is shown on Figure 1.

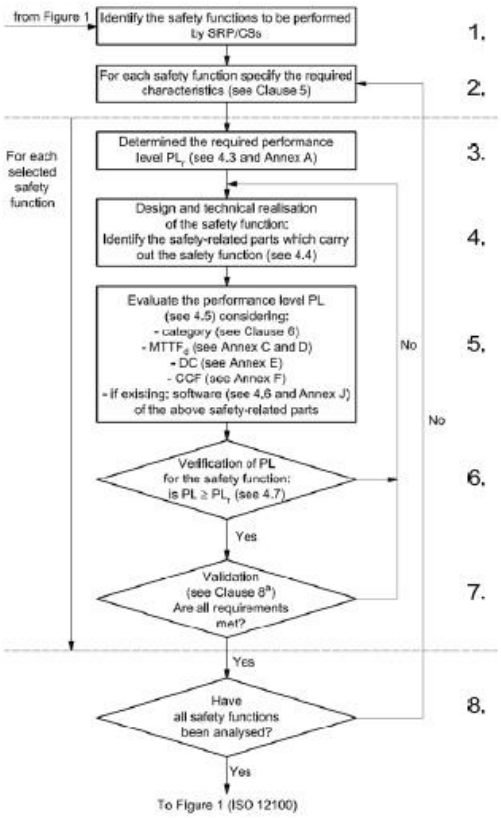


Figure 1: Safety system validation workflow

Once all of the safety functions have been identified (step 1), for all of these functions a specification of required characteristics must be done (step 2). After this, a more detailed description for each safety function has to be prepared (step 3). This includes also determination of required performance level (PL_r).

In the step 4, design and technical realization of the safety function is done. Here the designer chooses safety-related parts of the control system (SRP/CS) that perform the safety function.

In the step 5, evaluation of the performance level (PL) for selected safety-related parts of the control system is done. This may include evaluation and/or calculation of different parameters as a precondition.

Once the PL is evaluated, in step 6 it should be verified, meaning that in this step, the designer checks if the achieved performance level (PL) is higher than the performance level required (PL_r):

$$PL \geq PL_r$$

After this step, the designer checks if all other conditions are met (for example no additional risks are created), before he/she starts with the next safety function. If everything is ok, and there are no additional safety functions, the job is done and safe system is created.

B. Determining performance level required (PL_r)

According to the standard, there are 5 different performance levels, named as: PL_a, PL_b, PL_c, PL_d and PL_e.

In order to evaluate the performance level required, the standard introduces a few parameters that need to be determined in order to select the correct level. These are as follows:

S - Severity of injury can be low(S1) or high (S2)

F - Frequency of injury or exposure to a hazard. It can be low (F1) or high (F2).

P - Possibility to avoid hazard or limiting harm can be possible under some circumstances (P1) or barely possible (P2).

Once these parameters are determined for the safety function, the required performance level for that function is determined using the risk graph shown at the Figure 2.

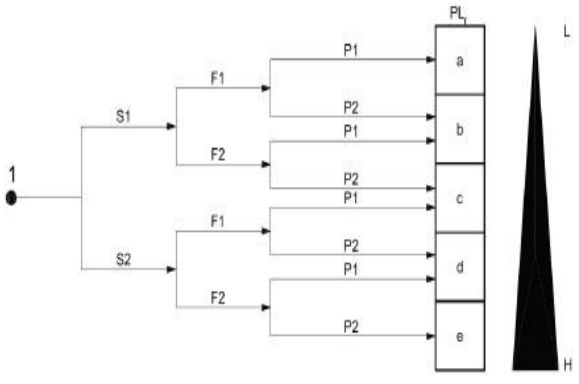
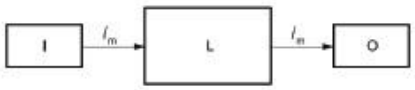


Figure 2: Risk graph

C. Design and the technical implementation of a safety function

EN ISO 13849-1 defines some structures for implementation of safety functions. These structures are called categories. There are 5 different categories (Category B, 1, 2, 3 and 4) and they all differ in terms of their resistance to the hardware faults. This resistance changes by changing the structure or by selection of hardware components.

Category B is represented by the structure shown on Figure 3.



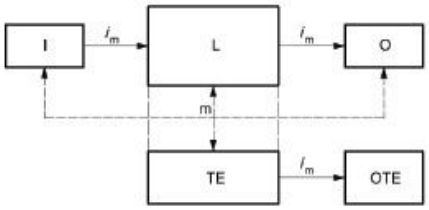
Key

i_m interconnecting means
I input device, e.g. sensor
L logic
O output device, e.g. main contactor

Figure 3: Category B structure

Category 1 has the same structure, but it differs from Category B in selection of hardware components which are characterized by well-tried safety principles and well-tried components.

Category 2 has the structure shown on Figure 4.



Dashed lines represent reasonably practicable fault detection.

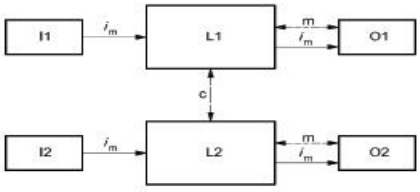
Key

i_m interconnecting means
I input device, e.g. sensor
L logic
m monitoring
O output device, e.g. main contactor
TE test equipment
OTE output of TE

Figure 4: Category 2 structure

In parallel to the single-channel structure used in lower categories, this category use additional test equipment to test and monitor the Input, Logic and Output parts of the basic channel and to send a separate output to the test output hardware.

Category 3 is shown on Figure 5.



Dashed lines represent reasonably practicable fault detection.

Key

i_m interconnecting means
c cross monitoring
I1, I2 input device, e.g. sensor
L1, L2 logic
m monitoring
O1, O2 output device, e.g. main contactor

Figure 5: Category 3 structure

The main feature of this category is redundancy. Practically, it is a two-channel system with monitoring of Inputs and Outputs, meaning it is a single-fault tolerant system.

Category 4 has the same structure as Category 3, but it uses the hardware that is more resistant to faults.

One of the basic differences between EN 954-1 and EN ISO 13849-1 is in the fact that the later consider also the hardware reliability. This is done by introducing additional factors, like:

1. $MTTF_d$ - Mean Time To Fault that leads to a dangerous state
2. DC - Diagnostic Coverage, or ratio of number of failures that lead to a dangerous state that are detected by some diagnostic mechanism in the control system and the total number of failures that lead to a dangerous state (in percentage).

The standard provides formulas for estimation of $MTTF_d$ for a component of a system (electromechanical, pneumatic, etc.) as well as for the complete system.

The expression for evaluation of $MTTF_d$ for a component is given by:

$$MTTF_d = \frac{B_{10d}}{0{,}1 n_{op}}$$

where:

B_{10d} – Number of operation until of a set of electromechanical components can operate until 10% of the set of components failed dangerously. This value is given by manufacturer of the component.

n_{op} – Mean number of annual operations for the component. This value is estimated by designer of SRP/CS.

The expression for evaluation of $MTTF_d$ for complete SRP/CS is given by:

$$\frac{1}{MTTF_{d,channel}} = \sum_{i=1}^{K} \frac{n_i}{MTTF_{d,i}}$$

Where:

$channel$ - Structure in which fault in SRP/CS will lead to a failure of the safety function

i – Is the component type

n_i - Number of different elements of the component i within the channel

K – Is the number of different component types within the channel

Diagnostic Coverage is estimated using the formula:

$$DC_{avg} = \frac{\sum_{n=1}^{k} \frac{DC_n}{MTTF_{d,n}}}{\sum_{n=1}^{k} \frac{1}{MTTF_{d,n}}}$$

Where:

n - Is the component type

DC_n - Diagnostic coverage of the component within the channel

$MTTF_{d,n}$ – Mean time to dangerous failure of the component within the channel

These two factors, together with the previously mentioned categories, can be used in order to define the technical realisation of a safety function that will satisfy the requested performance level PL_r. This can be done using the graph from the Figure 6 [5].

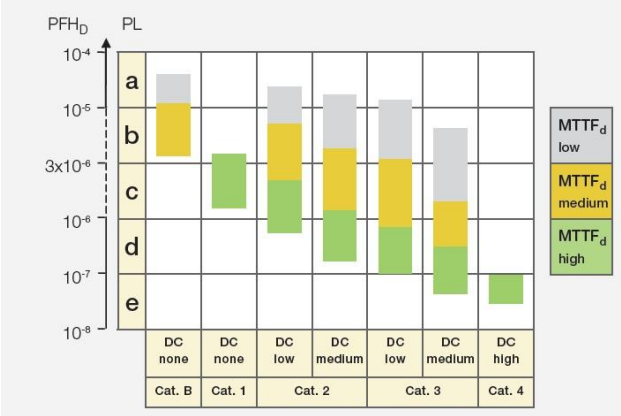


Figure 6: Relationship between $MTTF_d$, DC and Categories

IV. Safety Function Implementation

In this chapter three safety functions will be implemented.

In the risk analysis, three hazards, among others, were identified, which required protection using safety devices:

1. Unexpected start-up of a crane

2. Winch motor stop failure

3. Unexpected start-up of moving plate of centrifugal unit

A. *Unexpected start-up of a crane*

In order to reduce the risk, some additional assumptions about the plant operation were established:

- the plant is intended to run three shifts a day

- the hazard is expected during operator's intervention, which should not happen more often than once in two hours (gives us the frequency parameter F2)

- when the hazard happen, the operator doesn't have the possibility to avoid it (gives us the level of possibility to avoid hazard of P2)

- when the hazard happen, then slight, reversible injuries are expected (gives us the severity of S1)

Having all these in mind, and using the risk graph from Figure 2, we can conclude that the performance level required for this risk is:

PL_r = c (S1,F2,P2) = PL_c.

As the risk reduction measure, the emergency stop is selected. The switch is connected to a safety logic system which deactivates a contactor, in order to cut the power to the inverter. From the graph on Figure 6 it can be seen that one of the ways to meet PL_r for this safety function is choosing Category 1 structure with hardware that features high $MTTF_d$.

The selected emergency safety switch is Eaton's M22-PV/KC02/IY and estimated $MTTF_d$ (according to manufacturer's data sheet and assumed one operation per hour) is:

$$MTTF_d = 114.$$

This switch is connected to input safety terminal EL1904 from Beckhoff, then to logic terminal EL6900 from Beckhoff, and output terminal EL2904 from Beckhoff. All these terminals feature value of $MTTF_d$>100 (according to manufacturer's data sheets).

The output terminal is connected to Eaton's DILM12 contactor. According to manufacturer's documentation and assumed one operation per hour, estimated $MTTF_d$ for this contactor is:

$$MTTF_d = 1484.$$

For the selected category, the calculation of total $MTTF_d$ and the values from table K.1 from the standard give:

$$PL = b$$

So, the Category 1 couldn't be used. This is why the Category 2 is selected, which implies that two separate contactors should be installed in order to cut the power to the inverters.

The $MTTF_d$ value for the complete channel is estimated to:

$$MTTF_d = 19.$$

The DC_{avg}value for the complete channel is estimated to:

$$DC_{avg} = 98.$$

This implies that DC_{avg} is of Medium level, which, according to table K.1 of the standard, gives the PL of:

$$PL = c$$

B. Winch motor stop failure

The risk analysis of the crane unit showed the presence of additional hazards. One that is particularly dangerous is the case of winch motor stop failure. For this motor the following assumptions can be made:

- the plant is intended to run three shifts a day

- the hazard is expected during operator's intervention, which should not happen more often than once in two hours (gives us the frequency parameter F2)

- when the hazard happen, the operator does have the possibility to avoid it, under specific conditions (gives us the level of possibility to avoid hazard of P1)

- when the hazard happen, then serious injuries are expected (gives us the severity of S2)

Using the risk graph from Figure 2, we can conclude that the performance level required for this risk is:

PL_r = e (S2,F2,P1) = PL_d.

As the risk reduction measure, a frequency drive with safety integrated functions has been used. The function has been realized using a combination of stop commands (stop push button, emergency stop and standard PLC software stop command) connected to the logic module, which sends the safe stop command to the drive. The drive features integrated safe break management function, so after receiving safe stop command the load remains in the same vertical position. In addition, the motor is equipped with a break. The break is activated in parallel to the safe stop command sent to the drive.

Using manufacturers' data sheets, the calculation of $MTTF_d$ value is done in a similar way to one expressed in the first described safety function.

Using system with Category 3, this value corresponds to performance level of

$$PL = d$$

C. Unexpected start-up of a movable plate of the centrifugal unit

Just like in the first explained safety function, some risk-related assumptions were established:

- the plant is intended to run three shifts a day

- the hazard is expected during operator's intervention, which should not happen more often than once in a shift (gives us the frequency parameter F2)

- when the hazard happen, the operator doesn't have the possibility to avoid it (gives us the level of possibility to avoid hazard of P2)

- when the hazard happen, then serious, irreversible injuries are expected (gives us the severity of S2)

Having all these in mind, and using the risk graph from Figure 2, we can conclude that the performance level required for this risk is:

PL_r = e (S2,F2,P2) = PL_e.

As the risk reduction measure, the interlock door switch is selected. Two separate interlock switches are installed, with monitoring of NO and NC contacts for discrepancies. These switches should detect the door are opened, and the logic equipment should cut the power to the motors of the centrifugal unit, via redundant contactors used for feeding the motor. It can be seen from the graph on Figure 6 that one of the ways to meet PL_r for this safety function can be by choosing Category 3 structure with hardware that features high $MTTF_d$.

The selected interlock is Schmersal's AZ17-02ZI-B1 and estimated $MTTF_d$ (according to manufacturer's data sheet and assumed five operations per hour) is:

$$MTTF_d = 450.$$

The selected input, logic and output modules are of the same type and the same manufacturer as in the previous safety function (Beckhoff). The same applies to the selected contactor, which is again Eaton's DILM12.

For the selected category, the calculation of total $MTTF_d$ and the values from table K.1 from the standard give:

$$PL = d$$

So, the Category 3 couldn't be used. This is why the Category 4 is selected. Due to the fact that the interlock switches are of well-tried components, these satisfy the Category 4 requirements, just like the rest of the equipment.

This implies that DC_{avg} is of High level, which, according to table K.1 of the standard, gives the PL of:

$$PL = e$$

This means the designed system is safe according to EN ISO 13849-1.

V. CONCLUSION

With the tendency of reducing the risk in machine operation, saving the costs, and standardizing market conditions, a new standard for safety of machinery has been created: EN ISO 13849-1.

This standard includes hardware reliability in safety systems. Comparing to its predecessor, EN 954-1, the new standard is more flexible in using the categories. As the result of risk assessment, it defines the required Performance Level (PL_r), which can be achieved in different ways: either by selecting a different category or by choosing the hardware that is more reliable.

LITERATURE

[1] ABB, "ABB Safety Handbook, Machine safety - Jokab Safety Products", 2013.

[2] J. Hedberg, A. Soderberg, J. Tegehall, "How to design safe machine control systems - a guideline to EN ISO 13849-1", SP - Technical Research Institute of Sweden, 2011.

[3] Rockwell Automation, "SAFEBOOK 4: Safety related control systems for machinery - Principles, standards and implementation", 2011

[4] Schneider Electric, "Functional safety & Implementation of the Machinery Directive 2006/42/EC", 2012.

[5] ABB AB Jokab Safety, "Safety in control systems according to EN ISO 13849-1", 2011

[6] Eaton Industries Gmbh, "Overview of safety relevant characteristic values for Eaton components according to EN ISO 13849-1 and IEC 62061", 2014.

[7] Beckhoff Automation Gmbh & Co.KG, "EL1904 TwinSAFE input terminal with 4 fail-safe inputs", Version 1.5.1, 2015.

[8] Beckhoff Automation Gmbh & Co.KG, "EL2904 TwinSAFE output terminal with 4 fail-safe outputs", Version 1.6.1, 2015.

[9] Beckhoff Automation Gmbh & Co.KG, "EL6900 TwinSAFE Logic terminal version 1.5.1", 2015.

[10] K.A. Schmersal Gmbh & Co.KG, "Datasheet - AZ17-02ZI-B1", www.schmersal.net, 2015.