Implementation of International Safety Standard EN ISO 13849 into Machinery of Tyre Industry

N. Wongpiriyayothar, S. Chitwong

Abstract— **This paper presents application of international safety standard in risk assessment and risk reduction following by machinery directive. Many industries using machinery for manufacturing products have tendency to take risk from poor-quality of machinery design which may not be produced according to international safety standard. This can lead dangerous situation to machine user. The new standard EN ISO 13849-1 [1] which replaced the old standard EN 954-1 [2] definitely in December 2011 made machine designer not be familiar with the new concept and feel confused due to most of concerned parameters shown in term of statistic value that there are difficulty in interpretation and understanding. In the present, there is still lack of examples of implementation this standard into machinery of specific industry, especially in tyre industry. Therefore the objective of this paper is made for implementation this safety standard into machinery of tyre industry in order to build a safe situation for machine user.**

Keywords— **Safety-Related Parts of Control System (SRP/CS), Performance Level (PL), Mean Time to Dangerous Failure (MTTFd), Common Cause Failure (CCF), Diagnostic Coverage (DC).**

I. Introduction

Tyre industry machinery processes starting from mixing process of raw material, preparing process of material, tyre building process, tyre curing process and final inspection process respectively which all processes caused unsafe situation to machine user, especially in tyre building process that most of unsafe situations came from pinch point and rotation point of automatic building unit in front of machine.

Most of machineries in tyre industry are automation machine using safety control circuits in order to prevent entering to moving part of machine and/or to prevent unexpected starting up of machine by generating stop function to hold machine in safe stage. The well-known safety rule explained about procedure of risk assessment and risk reduction is EN ISO 12100 [3] following five-step method, i.e. (1) determination of the limits of the machinery , (2) hazard identification, (3) risk estimation, (4) risk evaluation, and (5) risk reduction. In the risk reduction process consisting of three-step method which all suitable protective measures must be followed, i.e. first step, inherently safe design measures, second step, safeguarding and/or complementary protective measures, the last step, information for uses.

Manuscript received December 22, 2016; revised January 12, 2017. N. Wongpiriyayothar and S. Chitwong are with the department of Instrumentation and Control Engineering, King Mongkut's Institute of Technology Ladkrabang, Ladkrabang, Bangkok 10520 THAILAND.
(e-mail : engineer_napat1@hotmail.com, sakreya.ch@kmitl.ac.th)

Therefore, the machine designer must eliminate hazard and/or reduce risks as much as possible by following three-step method of risk reduction process respectively in order to let machine perform safety function effectively and to provide safe situation for machine user.

This paper mainly focuses on the second step of risk reduction process that this part was regarded as belonging to standard EN ISO 13849 [1]. Thus, the purpose of this paper is to review and verify design of safety function of old machinery in tyre industry by comparing PLr (Performance level required) to PL (Performance level designed). If PL is greater than or equal to PLr (PL $\geq$ PLr), it means that machine can guarantee to perform the safe stage and meet requirement with design principles of international safety standard, on the other hand, if the verification result does not meet with requirement. What does machine designer need to do to eliminate hazard. These will be more explained in this paper.

II. Background of Machinery Safety Standard

A. EN 954-1

In the past, the well-known machinery safety standard EN 954-1 [2] was introduced in 1996 which this version is familiar to most of machine designers and is used in many automation industrials broadly, especially in European region. This standard defined Safety Categories to manage fault under foreseeable condition to prevent loss of safety function. These categories are divided into five levels, termed Categories B, 1, 2, 3 and 4 which Cat-4 can provide the highest safety level with redundant configuration. The procedure of this standard is quite simple and easy to understand for machine designer due to most of concerned criteria that are presented in term of deterministic approach following these steps, i.e. firstly identify safety function required to eliminate hazard, secondly consider whether fault condition can lead to loss of safety function or not and finally select safety category to manage fault condition.

B. EN ISO 13849-1

Standard EN ISO 13849-1 [4] was introduced first time in 1999 (original version), then was revised in 2006 (second version, [1]). The purpose of this standard is to replace the old standard EN 954-1 [2] which is going to be retired in December 2011. The concept of this standard is not only focusing on the deterministic approach (Category), but also statistic approach (PL, MTTFd, CCF and DC). Moreover, there is determining the designated architectures of category to perform a safety function which may be implemented by one or more SRP/CS. Combination of SRP/CS to perform a safety function (see Figure 1) consisting of input (SRP/CS_a), logic/processing (SRP/CS_b), output/power control elements (SRP/CS_c) and interconnecting means (i_{ab}, i_{bc}). However, this standard is quite difficult to understand for machine designers due to most of concerned criteria and calculated parameters presented in term of both deterministic and statistic approach leading most of them to use some kind of commercial computerization program to provide the quick result without understanding the basic principle in calculation and source of those formulas having an effect on poor quality in risk reduction process. Thus, these will be introduced in the next part of this paper to be the guideline and overview for general principles of this standard.

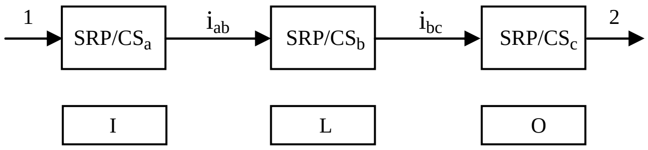

Figure 1 — Diagrammatic presentation of combination of safety-related parts of control systems for processing typical safety function

III. General Principles of EN ISO 13849-1

A. Overview

The purpose of this international safety standard is to provide machine designers, machine developers and machine manufacturers with an overall scope and guideline for design safety-related parts of control system (SRP/CS). The ability of safety-related parts of control systems is to perform a safety function under foreseeable conditions classified into five levels, called performance levels (PL) in term of PL a, b, c, d and e. These performance levels are defined in terms of probability of dangerous failure per hour (PFHD), (see Table I). The probability of dangerous failure of the safety function depends on several factors, consisting of designated architecture of SRP/CS (Category), reliability of components (MTTFd, CCF), fault detection of mechanisms (DC), design process, operating stress, environmental conditions and operation procedures. In order to achieve PL, the concept of this standard based on the categorization of structures following specific design criteria and specific behaviors under fault conditions. These categories are classified into five levels, termed Categories B, 1, 2, 3 and 4. For example of SRS/CS (input elements: interlocking devices, electro-sensitive protective devices, pressure sensitive devices…etc.), (logic elements: Program Logic Controller devices (PLC), Monitoring System, Data Processing Unit…etc.), and (output elements: Contactors, Relays, Valves…etc.).

Table I — Classification of Performance levels (PL)

PL	Average probability of dangerous failure per hour (PFHD) (1/h)
a	$\geq 10^{-5}$ to $< 10^{-4}$
b	$\geq 3 \times 10^{-6}$ to $< 10^{-5}$
c	$\geq 10^{-6}$ to $< 3 \times 10^{-6}$
d	$\geq 10^{-7}$ to $< 10^{-6}$
e	$\geq 10^{-8}$ to $< 10^{-7}$

NOTE Besides the average probability of dangerous failure per hour other measures are also necessary to achieve the PL

This standard is developed to provide a clear cut concept in application of SRP/CS on machinery which can be assessed and audited by third party to certify whether safety function was designed correctly according to machinery directive or not.

B. Concept of EN ISO 13849-1

After we completed in risk assessment and risk reduction following EN ISO 12100 [3] if the result of risk reduction is required to implement protective measures on machinery in order to eliminate hazard and/or reduce risk. This will lead to part of EN ISO 13849-1 [1] which concerns with general principles for design of SRP/CS. Then, the iterative process for design of SRP/CS shall be followed according to EN ISO 13849-1 [1] (Page 13, Figure 3) following these steps, i.e. (1) identify the safety functions to be performed by SRP/CSs, (2) determined the required performance level (PLr), (3) design safety function and identify SRP/CS to carry out safety function, (4) evaluate PL by considering Category, MTTFd, DC and CCF, (5) verify PL of safety function (PL ≥ PLr or not), (6) validate (meet with all requirements or not) sequentially. In step (5) and (6), if verification and validation step did not meet with requirement, this iterative process should be reconsidered.

Determination of PLr by Risk Graph Method

Risk Graph Method is part of standard EN ISO 13849-1 [1], using in determining PLr for each safety function to be carried out by SRP/CS (see Figure 2). There are concerned parameters using in estimation of risk following these, i.e. Severity of injury represented by S "(S1, slight injury), (S2, serious injury)", Frequency/Exposure of hazard represented by F "(F1, seldom happened/exposure time is short), (F2, continuously happened/exposure time is long)", Possibility of avoiding hazard/limiting harm represented by P "(P1, possible under specific condition), (P2, impossible)", and point number 1 is starting point of this method. Thus, the result of this method will let us know the level of risk (low, medium or high) and required PLr in selection each SRP/CS to perform safety function. This method given here is to provide as the guideline concept to machine designer in estimation of risk.

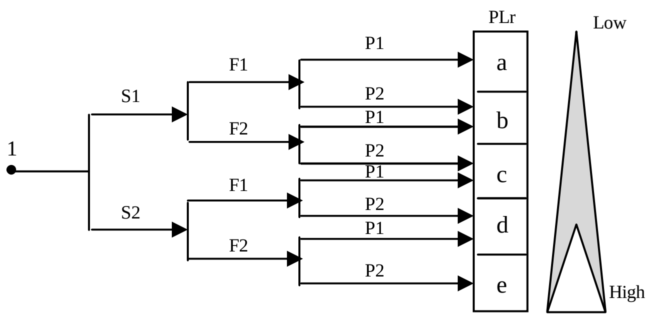

Figure 2 — Risk Graph for determining required PLr for safety function

C. Evaluation of PL by Category, MTTFd, DC and CCF

The ability of SRP/CS to perform safety function shall be expressed through PL and determined by estimation following these aspects: *(1) Category, (2) MTTFd, (3) DC and (4) CCF.*

ISBN: 978-988-14047-7-0
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

(1) Category

System requirement and system behavior to withstand fault condition are explained in term of Categories. SRP/CS shall be met with requirement of one of the five categories, termed Categories B, 1, 2, 3 and 4 (see Figure 3, 4, 5 and 6).

Category B is the basic category in which occurrence of fault can lead to the loss of safety function. This category provides the lowest safety level.

Category 1 is developed from Cat-B in which the occurrence of a fault can lead to the loss of safety function, but the ability to withstand fault is higher than Cat-B by using the concept of selection and implementation of well-tried components and well-tried safety principles.

Category 2 is required to apply Cat-B and Cat-1. In addition, the safety function shall be checked by machine control system periodically in which the occurrence of a fault can lead to the loss of safety function during checking period and the loss of safety function can be detected by the check.

Category 3 is required to apply Cat-B and Cat-1. In addition, safety-related parts shall be designed to ensure that single fault cannot lead the loss of safety function and single fault will be detected properly in case of reasonable practice in which the occurrence of the accumulated fault can lead to the loss of safety function.

Category 4 is required to apply Cat-B and Cat-1. In addition, safety-related parts shall be designed to ensure that single fault and accumulated fault cannot lead to the loss of safety function and the fault will be detected in time to prevent the loss of safety function. This category provides the highest safety level. For more explain in detail of categories are provided in EN ISO 13849-1 [1] (Page 38, Table 10 – summary of requirements for categories).

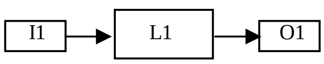

Figure 3

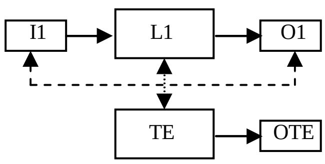

Figure 4

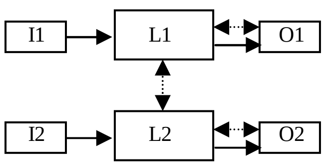

Figure 5

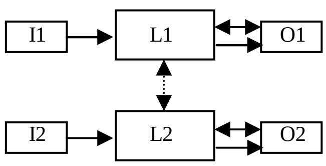

Figure 6

Figure 3 — Designated architecture for category B and category 1
Figure 4 — Designated architecture for category 2
Figure 5 — Designated architecture for category 3
Figure 6 — Designated architecture for category 4

(2) MTTFd (Mean time to dangerous failure)

MTTFd is classified into three levels (low, medium and high). This value describes the failure rate of component (reliability of component) in unit of years. The lowest MTTFd is 3 years and the highest MTTFd is 100 years to be taken into account (see Table II).

TABLE II — MEAN TIME TO DANGEROUS FAILURE OF EACH CHANNEL (MTTFd)

Denotation of each channel	Range of each channel
Low	3 years ≤ MTTFd < 10 years
Medium	10 years ≤ MTTFd < 30 years
High	30 years ≤ MTTFd ≤ 100 years

Calculating or Evaluating MTTFd for single components

To evaluate the statistic value of MTTFd for each component, these value can be referred from standard value of components which are manufactured according to basic and well-tried safety principles as shown in EN ISO 13849-1 [1] (Page 50–56, Table C.1-C.7) or can be calculated from B_{10d}, this is another statistic parameter provided by suppliers that they need to evaluate and declare into manufacturer data sheet. For terminology (see Table III).

Calculation of MTTFd from B_{10d} can be referred from these formulas; "(1)" and "(2)".

$$MTTFd = \frac{B_{10d}}{0.1x(n_{op})} \tag{1}$$

$$n_{op} = \frac{(d_{op})x(h_{op})x3{,}600\,(s/h)}{t_{cycle}} \tag{2}$$

TABLE III - TERMINOLOGY

Symbol	Definition of abbreviate word
n_{op}	The mean number of annual operations.
d_{op}	The mean operation, in days per year.
h_{op}	The mean operation, in hours per day.
B_{10d}	The mean number of cycles until 10% of components failure dangerously.
t_{cycle}	The mean time between the beginning of two successive cycles of the component. (e.g. switching of a valve) in seconds per cycle.

Calculating or Evaluating MTTFd for each channel

The MTTFd values of all single components which are part of the channel can be calculated by formula "(3)".

$$\frac{1}{MTTFd} = \frac{1}{MTTFd_1} + \frac{1}{MTTFd_2} + \ldots \frac{1}{MTTFd_n} \tag{3}$$

(3) DC (Diagnostic coverage)

The diagnostic coverage is ratio between failure rate of dangerous failure that can be detected and failure rate of total dangerous failure (total dangerous failure consists of dangerous failure which can be detected and cannot be detected). The DC is presented in term of statistic value to measure effectiveness of diagnostics, classified into four levels (see Table IV). DC can be estimated from EN ISO 13849-1 [1] (Page 59–61, Table E.1).

TABLE IV — DIAGNOSTIC COVERAGE (DC)

Denotation	Range
None	DC < 60 %
Low	60% ≤ DC < 90%
Medium	90% ≤ DC < 99%
High	99% ≤ DC

ISBN: 978-988-14047-7-0
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

For SRP/CS consisting of several parts, DC can be estimated by an average value of DC, so-called DC_{avg} and can be calculated by formula “(4)”.

$$DC_{avg} = \frac{\frac{DC_1}{MTTFd_1} + \frac{DC_2}{MTTFd_2} + \dots \frac{DC_n}{MTTFd_n}}{\frac{1}{MTTFd_1} + \frac{1}{MTTFd_2} + \dots \frac{1}{MTTFd_n}} \quad (4)$$

(4) CCF (Common cause failure)

CCF concept is to provide a checklist to let machine designer take into account to evaluate whether common problem had already been solved or not following check list in EN13849-1 [1] (Page 63, Table F.1). Maximum of evaluation score is 100 points. If evaluation score is less than 65 points, means that does not meet with requirement. Thus, machine designer should select appropriate measures to improve this factor to get score higher than 65 points.

Evaluation of PL

After completed in considering of Category, MTTFd, DC and CCF, then machine designer can evaluate PL of SRP/CS by following EN ISO 13849-1 [1] (Page 81-82, Table K.1). To meet with requirement, machine designer has to verify that PL is greater than or equal to PLr. In case of PL is less than PLr, the iterative process should be reconsidered.

IV. EXAMPLE OF IMPLEMENTATION

Life time to review and verify risk assessment of old machinery in tyre industry will be conducted every 5 years periodically in order to ensure whether safety function work properly according to concept of international safety standard or not by using *Risk Graph Method* to determine PLr and compare with PL. If PL is greater than or equal to PLr (PL $\geq$ PLr), this can guarantee that safety function meet with requirement but if PL is less than PLr (PL < PLr), then safety function and design feature of machinery must be reconsidered.

The old tyre building machine was reviewed following period of 5 years. For the required participants to verify risk assessment consist of machine designer, machine user (e.g. maintenance member, operation member, tooling change member and quality assurance member) and site safety officer to brainstorm any ideas in risk assessment and risk reduction to eliminate hazardous situation and/or reduce risk as much as possible.

V. RESULT OF RISK ASSESSMENT AND RISK REDUCTION

Risk of tyre building machine concerned with *Pinch Point* and *Rotation Point* of automatic building unit in front of machine (see Figure 7). The result of risk assessment following risk graph method which was evaluated by concerned participants is S2, F2, and P1. Thus, PLd is required for eliminating hazardous situation.

After completed in risk assessment process of old tyre building machine, we found 2 points of SRP/CS must be improved following second step of risk reduction process by implementing of safeguarding and complementary protective measures that consist of First point, upgrading system of emergency stop is needed due to the original design of this system was designed by category-1 (see Figure 9) which provided only PLc (not meet requirement with PLd), and Second point, implementing system of safety light curtain is needed due to the original design of this system was designed without protective measures in front of automatic building unit that can lead to unsafe situation when maintenance member access to dangerous zone to repair machine or operator access to verify specification of product or quality assurance member access to verify quality of product or tooling change member access to change equipment for producing the new size of tyre following daily production planning …etc. All of these behaviors have a chance to take risk from unexpected start-up of machine function and cause of serious injury eventually.

Therefore, these 2 points must be improved in order to eliminate hazardous situation and/or reduce risk.

VI. VERIFICATION PL OF SAFETY FUNCTION

A. Original design of emergency stop system (see Figure 9)

Safety function explanation:

- When emergency stop device E1 was activated, control voltage of contactor K1 will be interrupted and de-energized power out of movement part (Motor). Then, hazardous situation of will be eliminated.
- This was designed by category-1 that cannot maintain all component failures. Safety function depends on reliability of components only. There is no implementing of fault detection that can lead to the loss of the safety function.
- The stopping function of emergency stop device is implementing of complementary protective measure to hazardous area.

Design feature:

- Meet requirement with category-B, implement of well-tried components and well-tried safety principles.
- Design of the closed-circuit current and earth connection regard to well-tried safety principles concept.
- Selection of emergency stop device E1 regards to well-tried components concept in according with IEC 60947-5-1 [5].
- Selection of contactor K1 regards to well-tried components concept in according with table D.4 of EN ISO 13849-2 [6].
- Wiring control signal to contactor in according with stop category type 0 of EN 60204-1 [7].

Result of PFHD and PL:

- MTTFd was calculated by emergency stop E1 is standard emergency stop device according to table C.1 of EN ISO 13849-1 [1], the life time of switching operation (B_{10d}) is 100,000 cycles and to be activated 3 times per day before starting each shift following standard operation procedure for testing safety device (3 shifts/day, 365 working day/year), Therefore n_{op} is 1,095 cycles/year and MTTFd is 913 years.
- MTTFd was calculated by contactor K1 according to table C.1 of EN ISO 13849-1 [1], B_{10d} is 2,000,000 cycles and start/stop to be activated 6 times/day before starting/stopping of each shift (3 shifts/day , 365

ISBN: 978-988-14047-7-0
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

working days/year), Therefore n_{op} is 2,190 cycles/year and MTTFd is 9,132 years.

- PL was defined by using $MTTFd_{avg}$ between E1 and K1 which is 830 years (consider at maximum value 100 years, high) and designated architecture which is category-1 according to Table K.1 of EN ISO 13849-1 [1], therefore the PFHD of this system is $1.14x10^{-6}$ per hour. *This corresponds to PLc.*

B. Upgrading design of emergency stop system (see Figure 10)

Safety function explanation:

- When emergency stop device E1 was activated, control voltage of contactor K1 and K2 will be interrupted and de-energized power out of movement part (Motor). Then, hazardous situation will be eliminated.
- This was designed by category-3 that both feedback signal of emergency stop E1 and feedback signal of redundant contactors K1, K2 were monitored by the monitoring safety relay (MSR1). But this cannot maintain an accumulation of undetected faults that can lead to the loss of the safety function.
- The stopping function of emergency stop device is implementing of complementary protective measure to hazardous area.

Design feature:

- Meet requirement with category-B, implement of well-tried components and well-tried safety principles.
- Design of the closed-circuit current and earth connection regard to well-tried safety principles concept.
- Selection of emergency stop device E1 regards to well-tried components concept in according with IEC 60947-5-1 [5].
- Selection of contactor K1, K2 regards to well-tried components concept in according with table D.4 of EN ISO 13849-2 [6].
- The monitoring safety relay (MSR1) meet requirement with category-4, PLe, MTTFd is $4.35x10^{-9}$ per hour according to manufacturer datasheet.

Result of PFHD and PL:

- MTTFd calculated by emergency stop E1, is 913 years (Same concept as previous mentioned).
- MTTFd calculated by contactor K1, is 9,132 years. (Same concept as previous mentioned).
- MTTFd calculated by contactor K2, is 9,132 years. (Same concept as previous mentioned).
- DC_{avg} and CCF are relevant in category-3, Therefore DC_{avg} of E1 and K1, K2 are 90% according to table E.1 of EN ISO13849-1 [1] and CCF of this system are 85 according to table F.1 of EN ISO 13849-1 [1].
- PL was defined by using $MTTFd_{avg}$ between E1 and K1, K2 which is 761 years (consider at maximum value 100 years, high) and designated architecture which is category-3 and DC_{avg} is 90% (medium) according to Table K.1 of EN ISO 13849-1 [1], PFHD is $4.29x10^{-8}$ per hour. Following additional of subsystem MSR1that PFHD is $4.35x10^{-9}$ per hour. Therefore the average PFHD of this system is $4.73x10^{-8}$ per hour. *This corresponds to PLe.*

C. Implementing of protective measure by safety light curtain system (see Figure 11)

Safety function explanation:

- When safety light curtain device (LC1) was activated, control voltage of contactor K1 and K2 will be interrupted and de-energized power out of movement part (Motor). Then, hazardous situation will be eliminated.
- This was designed by category-3 that both feedback signal of safety light curtain device (LC1) and feedback signal of redundant contactors K1, K2 were monitored by MSR1. But this cannot maintain an accumulation of undetected faults that can lead to the loss of the safety function.
- The stopping function of safety light curtain device (LC1) is implementing of complementary protective measure to hazardous area.

Design feature:

- Meet requirement with category-B, implement of well-tried components and well-tried safety principles.
- Design of the closed-circuit current and earth connection regard to well-tried safety principles concept.
- Selection of contactor K1, K2 regards to well-tried components concept in according with table D.4 of EN ISO 13849-2 [6].
- The monitoring safety relay (MSR1) meet requirement with category-4, PLe, MTTFd is $4.35x10^{-9}$ per hour according to manufacturer datasheet.
- The safety light curtain device (LC1) meet requirement with category-4, PLe, MTTFd is $7.93x10^{-9}$ per hour according to manufacturer datasheet.

Result of PFHD and PL:

- MTTFd calculated by contactor K1, is 9,132 years. (Same concept as previous mentioned).
- MTTFd calculated by contactor K2, is 9,132 years. (Same concept as previous mentioned).
- DC_{avg} and CCF are relevant in category-3, Therefore K1 and K2 are 90% according to table E.1 of EN ISO13849-1 [1] and CCF of this system are 85 according to table F.1 of EN ISO 13849-1 [1].
- PL was defined by using $MTTFd_{avg}$ between K1 and K2 which is 4,566 years (consider at maximum value 100 years, high) and designated architecture which is category-3 and DC_{avg} is 90% (medium) according to Table K.1 of EN ISO 13849-1 [1], PFHD is $4.29x10^{-8}$ per hour. Following additional of subsystem MSR1that PFHD is $4.35x10^{-9}$ per hour and LC1 that PFHD is $7.93x10^{-9}$ per hour. Therefore the average PFHD of this system is $5.52x10^{-8}$ per hour. *This corresponds to PLe.*

VII. SUMMARY AND CONCLUSION

From the result of risk assessment of the old tyre building machine, the result showed that PLd is required to eliminate hazardous situation and/or reduce risk. However, not only the original design of emergency stop system (see Figure 9) that provide PLc is not enough to reduce risk, but also there are lacking of protective measure in front of hazardous area that can lead unsafe situation to machine user. Therefore the purpose of this paper is want to implement SRP/CS by upgrading design of emergency stop system (see Figure 10) and implementing of protective measure by safety light curtain system (see Figure 11) following international safety standard requirement. Both of these systems provide PLe (see Table V) which is more than enough to reduce risk and can ensure that machine will be able to perform safe stage and build safe situation for machine user (see Figure 8).

By the writer's opinions and experiences, all processes of risk assessment and risk reduction are not easy to achieve and get more effective result. The important parameters which need to be taken into account are experience and knowledge of participants who involved in this activity. If they are lack all of these, they cannot identify "where are the risk points which need to be eliminated" and cannot offer any improvement idea "how to develop SRP/CS to eliminate hazardous situation". Therefore, in order to get more effective result the chairman and/or project leader should require concerned participants who have an experience related with machinery up to 5 years in different domains to do this activity. Machine designer is not only the person in charge of this activity, but other domains also are essential to exchange any different point of view in eliminating risk and optimization of investment cost should be considered also.

REFERENCES

[1] ISO 13849-1:2006, Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design.
[2] CEN EN 954-1:1996, Safety-related parts of control systems.
[3] ISO 12100:2010, Safety of machinery — General principles for design — Risk assessment and risk reduction.
[4] ISO 13849-1:1999, Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design.
[5] IEC 60947-5-1:2003, Low-voltage switchgear and controlgear – Part 5: Control circuit devices and switching elements – Section 1: Electromechanical control circuit devices.
[6] EN ISO 13849-2:2010, Safety of machinery - Safety-related parts of control systems - Part 2: Validation
[7] EN 60204-1:2009, Safety of machinery – Electrical equipment of machines – Part 1: General requirements
[8] BGIA Report 2:2008, Functional safety of machine controls – Application of EN ISO 13849.

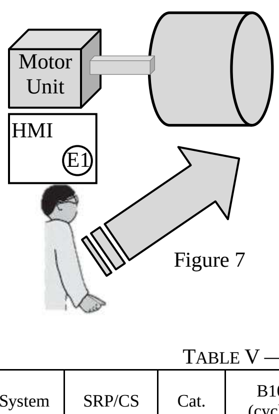

Figure 7

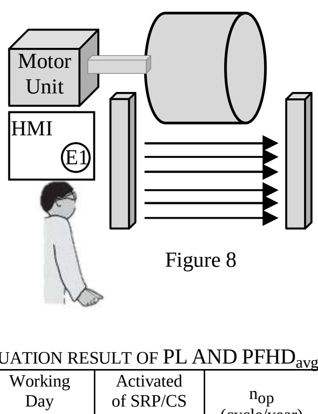

Figure 8

Figure 7 — Hazardous situation from pinch and rotation point
Figure 8 — Implemented of SRP/CS to eliminate hazardous situation

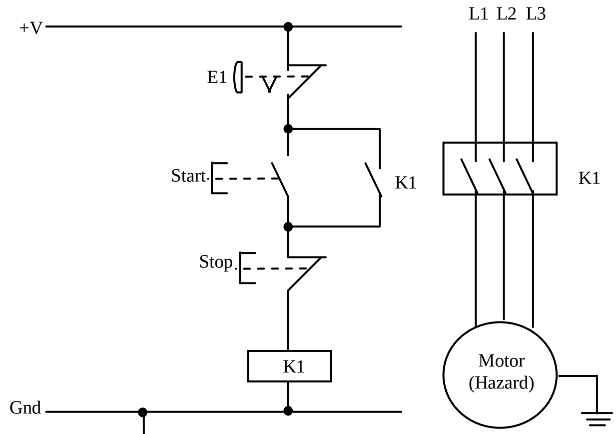

Figure 9

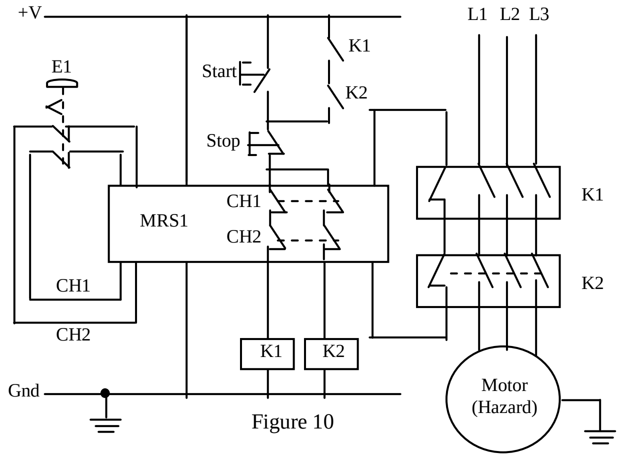

Figure 10

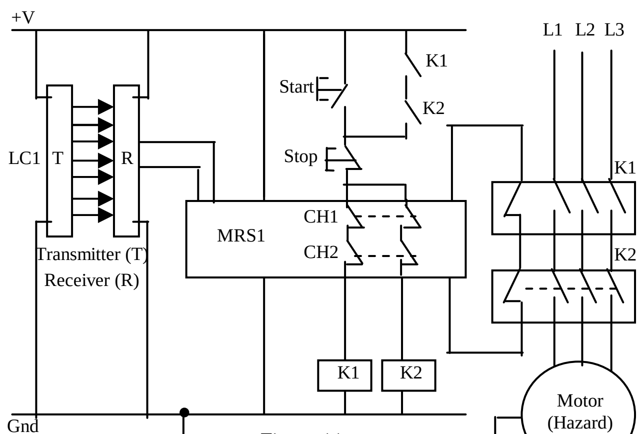

Figure 11

Figure 9 — Original design of emergency stop system
Figure 10 — Upgrading design of emergency stop system
Figure 11 — Implementing of protective measure by safety light curtain

TABLE V — EVALUATION RESULT OF PL AND $PFHD_{avg}$ OF EACH SYSTEM BY CATEGORY, MTTFd, DC AND CCF

System	SRP/CS	Cat.	B10d (cycles)	Working Day (days/year)	Activated of SRP/CS (cycle/day)	n_{op} (cycle/year)	MTTFd (years)	MTTFd (avg.)	DC (%)	DC_{avg} (%)	CCF (points)	PL	PFHD (1/h)	$PFHD_{avg}$ (1/h)	*
Figure 9	E1	Cat.1	100,000	365	3	1095	913	830	N/A	N/A	N/A	PLc	$1.14x10^{-6}$	$1.14x10^{-6}$	(1)
	K1	Cat.1	2,000,000	365	6	2190	9132		N/A		N/A				(1)
Figure 10	E1	Cat.3	100,000	365	3	1095	913	761	90	90	85	Ple	$4.29x10^{-8}$	$4.73x10^{-8}$	(1)
	K1	Cat.3	2,000,000	365	6	2190	9132		90						(1)
	K2	Cat.3	2,000,000	365	6	2190	9132		90						(1)
	MRS1	Cat.4	N/A	N/A	N/A	N/A	355	355	N/A	N/A		Ple	$4.35x10^{-9}$		(2)
Figure 11	LC1	Cat.4	N/A	N/A	N/A	N/A	20	20	N/A	N/A	85	Ple	$7.93x10^{-9}$	$5.52x10^{-8}$	(2)
	MRS1	Cat.4	N/A	N/A	N/A	N/A	355	355	N/A	N/A		Ple	$4.35x10^{-9}$		(2)
	K1	Cat.3	2,000,000	365	6	2190	9132	4566	90	90		Ple	$4.29x10^{-8}$		(1)
	K2	Cat.3	2,000,000	365	6	2190	9132		90						(1)

* **Note: (**1) Means that data of B10d refer from EN ISO 13849-1 [1] (Page 50, Table C.1) and calculation data of nop, MTTFd, DC, CCF and PFHD refer from method of standard EN ISO 13849-1 [1], (2) Means that data of MTTFd, PL and PFHD refer from manufacturer datasheet.

ISBN: 978-988-14047-7-0
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)