Erkki Ojalehto

Safety device upgrade for robotic cells

Machine safety

Bachelor's Thesis

Spring 2014

School of Technology

Automation Engineering

Seinäjoen ammattikorkeakoulu
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Thesis abstract

Faculty: School of Technology

Degree programme: Automation Engineering

Specialisation: Machine Automation

Author: Erkki Ojalehto

Title of thesis: Safety device upgrade for robotic cells

Supervisor: Martti Lehtonen

Year: 2014 Number of pages: 62 Number of appendices: 4

The purpose of this thesis was to improve the safety of robotic cells at Valio Ltd's factories of edible fat. All safety devices, used in the cells, were inspected. Based on the perceptions, mechanical improvements were made.

The safety switches of the robotic cells' service doors were estimated insufficient in reliability. For this reason, improvements for the cells' safety-related control system were designed. Improvements were planned to the other parts of the palletising system at the same time.

The theory part concentrates on standards, risk assessment, and especially the safety-related control system. For the improvement of the robotic cells, a new performance level was calculated with the help of standard ISO 13849-1 and the SISTEMA software.

Keywords: machine safety, risk reduction, safety-related control system

SEINÄJOEN AMMATTIKORKEAKOULU

Opinnäytetyön tiivistelmä

Koulutusyksikkö: Tekniikan yksikkö

Koulutusohjelma: Automaatiotekniikka

Suuntautumisvaihtoehto: Koneautomaatio

Tekijä: Erkki Ojalehto

Työn nimi: Turvalaite päivitys robottisoluille

Ohjaaja: Martti Lehtonen

Vuosi: 2014 Sivumäärä: 62 Liitteiden lukumäärä: 4

Opinnäytetyön tarkoitus oli parantaa Seinäjoen Valio Oy:n ravintorasvatehtaan robottisolujen turvallisuutta. Työssä tarkastettiin kaikki soluissa käytetyt turvalaitteet. Tarkastusten perusteella tehtiin mekaanisia parannuksia turvalaitteisiin.

Robottisolujen huolto-ovia valvovat turvarajat arvioitiin riittämättömän luotettaviksi. Tästä syystä soluihin suunniteltiin parannuksia turvallisuuteen liittyvään ohjausjärjestelmään. Parannuksia suunniteltiin samalla muihin lavausjärjestelmän osiin.

Teoria osassa on perehdytty standardeihin, riskiarviointiin, sekä erityisesti turvallisuuteen liittyvään ohjausjärjestelmään. Robottisolujen parannukselle laskettiin uusi suoritustaso standardia ISO 13849-1 ja SISTEMA ohjelmaa käyttäen.

Avainsanat: koneturvallisuus, riskin vähentäminen, turvallisuuteen liittyvä ohjausjärjestelmä

TABLE OF CONTENTS

List of figures

List of tables

Terms and abbreviations

AC-drive	Alternating Current drive
B10	Number of cycles until 10% of the components will fail.
$B10_d$	Number of cycles until 10% of the components will fail dangerously.
Cat	Category
CCF	Common Cause Failure
DC	Diagnostic Coverage
DC_{avg}	average Diagnostic Coverage
F-CPU	Fail-safe Central Processing Unit
I/O	Inputs and Outputs
IEC	International Electrotechnical Commission
ISO	International Standard Organisation
IWLAN	Industrial Wireless Local Area Network
MTTF	Mean Time To Failure
$MTTF_d$	Mean Time To dangerous Failure
PFHd	Probability of a dangerous Failure per Hour
PL	Performance Level
PLr	required Performance Level
PLC	Programmable Logic Controller
RFID	Radio Frequency IDentification

SIL	Safety Integrity Level
SS1	Safe Stop 1
STO	Safe Torque Off

1 INTRODUCTION

1.1 Valio Ltd

Valio Ltd is a Finnish dairy company, which is owned by 18 dairy cooperatives. Company has 15 production plants in Finland and five subsidiaries in other countries. Valio Ltd was founded in 1905 in order to increase butter export and to improve the quality of the butter. Demand for Valio Ltd's dairy products increased quickly, so the company started to refine also other products to the markets. The sales in 2012 were 2 billion euros, when the share of domestic market was 64 percent. Valio Ltd gives the market profits to milk producers through dairy cooperatives. Milk employs around 30 000 people in Finland from which Valio Ltd employs 4600. (Valio Ltd 2014a)

Valio Ltd's production plant in Seinäjoki produces modern milk powders, edible fats and perishables. The products are made in three individual factory units in Seinäjoki. The production plant in Seinäjoki employs in total 360 people in production and laboratory. Familiar products made in Seinäjoki production plant are for example Valio butter, Valio Oivariini®, KevytLevi®, Valio Gefilus® power drinks and Valio HeVi™ shots. Production plant's raw milk is collected from 1000 milk producers. (Valio Ltd 2014b)

All Valio Ltd's edible fats and spreads are made in the fat factory unit in Seinäjoki. The fat factory unit has four production lines for butter and ten different packaging lines. The fat factory unit's final products are wrapped butter, spreads and bigger butter bricks for industrial purposes. (Valio Ltd 2014b)

Figure 1 Logo of Valio Ltd.
(Valio Ltd 2014b)

1.2 Backround

The purpose of this thesis was to improve the safety level of a pallet loading system, used in the fat factory unit. The research work focused on the pallet loading system's robotic cells and their safety devices. With the gained information and actions conducted through this thesis, possible hazard situations can be prevented in the robotic cells.

Actualised hazard situations during production initiated the research work. Safety device failures associated to robotic cells took place in the perishables' factory unit. Safety device checks were considered necessary also in the fat factory unit.

Human access to the hazard zones is prevented with fences and service doors. Service doors' position is supervised with a safety switch, which prevents the robot from operating if the door is open. Service doors' function was inspected and improved so that hazard situations are henceforth extremely improbable.

1.3 Structure of the research

Report starts with a theory part about machine safety. Standard ISO 13849-1 is dealt with by its outlines. This standard is essential for this research because the standard is dealing with the safety-related control system. Control systems can be dealt with the standard IEC 62061 also, but because of the SISTEMA program used in this work, standard ISO 13849-1 was selected. SISTEMA uses standard 13849-1 to determine the performance level of a safety device or devices.

The theory section of the thesis includes basic information about machine safety standards, risk evaluation and machine modifications and also safety components - and fieldbus technology used in Valio Ltd's robotic cells. The experimental part of the thesis deals with the pallet loading system's working principle and the notes made during inspections. Safety device improvements were verified with ISO 13849-1 standard and SISTEMA program. SISTEMA calculation report is attached to the annex part of this thesis.

2 MACHINE SAFETY

2.1 General information about machine safety standards

Machine safety standards are divided into three groups, A-, B- and C-type of standards.

- Type A standards are basic safety standards, which outline basic concepts, principles for design, and general aspects that can be applied to all machinery.

- Type B standards are generic safety standards dealing with one safety aspect or one type of safeguard that can be used across a wide range of machinery.

- Type C standards are machine safety standards dealing with detailed safety requirements for a particular machine or group of machines.

(Schneider Electric 2009)

2.2 Machine modifacation or modernization

Modification of old machines, or addition of new equipment can convert the old machine in a way that it must be considered as a new machine. This signifies that machine’s entirety has changed in terms of machine safety. The new machine must fulfil these demands:

- Machine safety regulation annex 1

- Declaration of conformity

- Technical structure report

- Equipped with CE marking

(Siirilä 2008, p55)

Even if the planned changes do not create a new machine, it is still important to make a contract between the orderer and supplier of the changing work stating that who will be responsible for the safety. Unless otherwise agreed, the owner of the machine will have the responsibility. (Siirilä 2008, p55)

The machine modernization belongs to the scope of the labour protection act. The implementer has an obligation to complete the work in client's order so that the end result is safe. The owner has a responsibility to use an implementer which is capable of achieving the modernization in such a way that the end result is safe. In addition, the owner must define work safety issues to the implementer related to the modernization and ensure that the equipment suppliers provide suitable devices for the new application. (Sundquist 2010)

2.3 Machine’s risk assessment

Potential risks are searched from the machine with a risk assessment. These risks can be, for example, machine’s spinning sprockets or shafts. There are several methods for defining the risk. The method chosen for the risk assessment in this thesis is from Siirilä’s machine safety book 2008, where risks are assessed by their severity (Table 1) and probability (Table 2). As a result a numeric value for a risk has been created (Table 3), and used to determine what kind of actions need to take place in order to reduce the risk (Table 4). The risk can be reduced for example with different kinds of physical obstacles like fences. The risk must be low enough before the machine can be used.

Table 1 Severity of the harm.
(Siirilä 2008, p98)

Severity	
100	Death, coma, brain damage
90	Two limb loss, blinding, become paralyzed
80	Two limb loss, blinding, become paralyzed
70	Limb -, eye -, hearing loss, or several amount of finger loss
60	Limb -, eye -, hearing loss, or several amount of finger loss
50	Big bone fracture, serious injuries (curable), incurable light injuries
40	Big bone fracture, serious injuries (curable), incurable light injuries
30	Light bone fracture or minor injuries (curable)
20	Wound, chafe, illness
10	Scratches, bruises
1	No consequenses

Table 2 Probability of the harm.
(Siirilä 2008, p108)

Probability	
1	Occurrence is certain
0,9	Occurrence almost certain, would be surprising if not happen
0,8	Very certain
0,7	Possible, occurrence would be not unconventional or surprising
0,6	Happening and not happening are about as likely
0,5	Happening and not happening are about as likely
0,4	Possible, but unusual
0,3	Unusual
0,2	Very Unusual, thinkable
0,1	Extremely implausible, almost impossible

The numeric value of the risk consists of the severity and probability of harm by multiplying with each other. The risk is divided into five areas, see tables 3 and 4. Table 4 states required actions for each risk area. (Siirilä 2008, p107-108)

Table 3 Determination of the risk by the severity and probability of harm multiplied with themselves.
(Siirilä 2008, p109)

Probability \ Severity	1	10	20	30	40	50	60	70	80	90	100
1	1	10	20	30	40	50	60	70	80	90	100
0,9	0,9	9	18	27	36	45	54	63	72	81	90
0,8	0,8	8	16	24	32	40	48	56	64	72	80
0,7	0,7	7	14	21	28	35	42	49	56	63	70
0,6	0,6	6	12	18	24	30	36	42	48	54	60
0,5	0,5	5	10	15	20	25	30	35	40	45	50
0,4	0,4	4	8	12	16	20	24	28	32	36	40
0,3	0,3	3	6	9	12	15	18	21	24	27	30
0,2	0,2	2	4	6	8	10	12	14	16	18	20
0,1	0,1	1	2	3	4	5	6	7	8	9	10

Table 4 Required actions based on the risk.
(Siirilä 2008, p108)

Risk level		**Required actions**	
Value	**Description**	**Existing machinery**	**New machines**
0.1 ... 5	Slight risk	Actions not needed	Actions not needed
6 ... 15	Tolerable risk	Machine can be used but tracking is necessary	Machine can be used but tracking is necessary
16 ... 28	Moderate risk	Machine can be used, but required fixes must be planned and implemented soon as possible.	Planning must be continued, risk must be lowered.
29 ... 48	Significant risk	Production interruptions must be considered. If production is proceeded, fixes must be carried out immediately and lots of resources must be used.	Planning must be continued, risk must be lowered
49 ... 100	Intolerable risk	Production must be interrupted immediately. Production can proceed again when the risk is lower or equal than tolerable.	Planning must be continued, risk must be lowered

2.4 Control system's examination with help of standard

Standard ISO 13849-1 can be used to evaluate the structure and safety of the machine's safety-related control system. The control system's safety evaluation can also be carried out with an alternative standard IEC 62061. Table 5 describes the recommended applications for both standards. The use of either of these standards, in accordance with their scopes, can be presumed to fulfil the relevant essential safety requirements. (SFS EN ISO 13849-1, p13)

Table 5 Suggested applications of ISO 13849-1 and IEC 62061.
(SFS EN ISO 13849-1, p13)

	Technology implementing the safety-related control function(s)	ISO 13849-1	IEC 62061
A	Non-electrical, e.g. hydraulics	X	Not covered
B	Electromechanical, e.g. relays, and/or non complex electronics	Restricted to designated architectures [a] and up to PL = e	All architectures and up to SIL 3
C	Complex electronics, e.g. programmable	Restricted to designated architectures [a] and up to PL = d	All architectures and up to SIL 3
D	A combined with B	Restricted to designated architectures [a] and up to PL = e	X [c]
E	C combined with B	Restricted to designated architectures (see Note 1) and up to PL = d	All architectures and up to SIL 3
F	C combined with A, or C combined with A and B	X [b]	X [c]
X	indicates that this item is dealt with by the International Standard shown in the column heading.		
[a] Designated architectures are defined in 6.2 in order to give a simplified approach for quantification of performance level.			
[b] For complex electronics: use designated architectures according to this part of ISO 13849 up to PL = d or any architecture according to IEC 62061.			
[c] For non-electrical technology, use parts in accordance with this part of ISO 13849 as subsystems.			

In standard ISO 13849-1 control system's safety is called performance level (PL). The ability to perform a safety task is divided into five performance levels a, b, c, d, e. The highest safety performance is achieved with PL e, and the lowest with PL a.

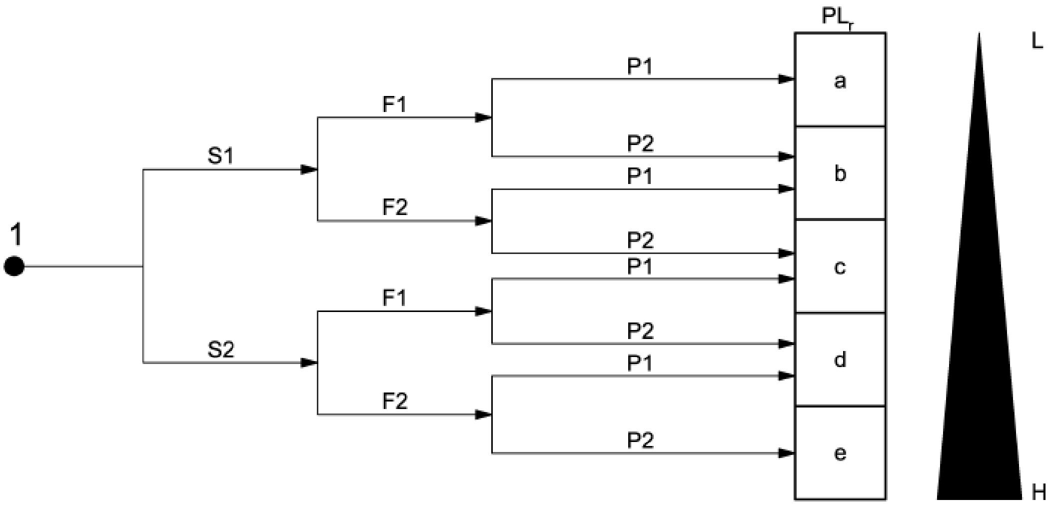
If the standard IEC 62061 is used, safety is called safety integrity level (SIL). Safety integrity level is divided into four levels, SIL 1, SIL 2, SIL 3 and SIL 4.

SIL 4 is intended to be used for process industrial purposes to prevent catastrophes. It isn't meaningful for machine safety usage. Table 6 presents the relation between performance level and safety integrity level. PL has no correspondence on the SIL scale and it is mainly used to reduce the risk of slight injuries. (SFS EN ISO 13849-1, p45)

Table 6 Relation between performance level (PL) and safety integrity level (SIL). (SFS EN ISO 13849-1, p45)

PL	**SIL** (IEC 61508-1, for information) high/continuous mode of operation
a	No correspondence
b	1
c	1
d	2
e	3

The required performance level of the machine’s safety devices is defined according to the risk (Figure 2). A safety device which has been implemented with a control system always consists of several safety components. The required performance level is a combination of these components.



Key

1 starting point for evaluation of safety function's contribution to risk reduction

L low contribution to risk reduction

H high contribution to risk reduction

PL_r required performance level

Risk parameters:

S severity of injury

S1 slight (normally reversible injury)

S2 serious (normally irreversible injury or death)

F frequency and/or exposure to hazard

F1 seldom-to-less-often and/or exposure time is short

F2 frequent-to-continuous and/or exposure time is long

P possibility of avoiding hazard or limiting harm

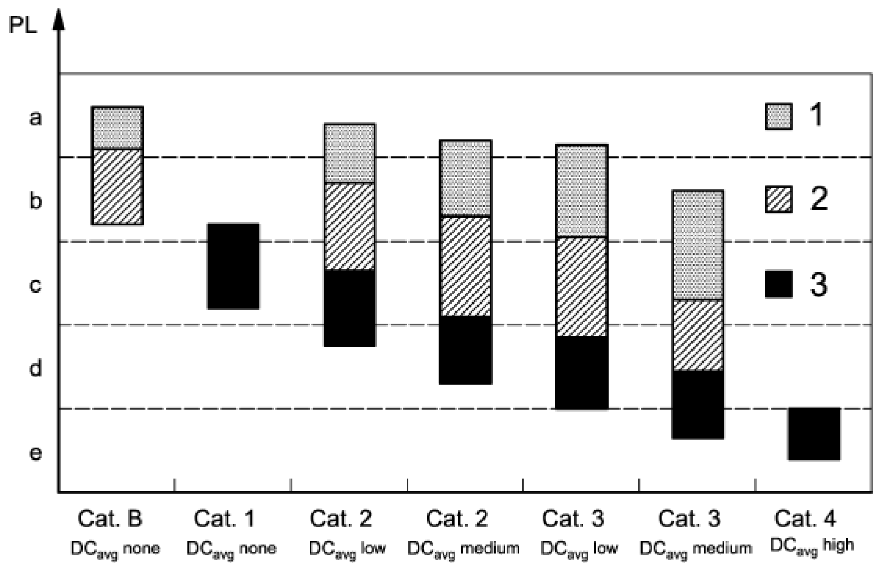
P1 possible under specific conditions

P2 scarcely possible

Figure 2 Definition of the required performance level PL_r.
(SFS EN ISO 13849-1, p101)

2.4.1 Designated architectures

Control system's PL is strongly dependent on the used designated architecture. These architectures are called category B, category 1, category 2, category 3 and category 4. Category B is the most simple and category 4 the most complex. The actual differences between these categories are the mean time to a dangerous failure ($MTTF_d$) and an average diagnostic coverage (DC_{avg}). The given PL can be achieved with many alternative categories as can be seen in figure 3. For example, if a safety device is designed to be used extremely rarely or, if high quality components are used, the PL might be slightly higher.



Key

PL performance level

1 $MTTF_d$ of each channel = low

2 $MTTF_d$ of each channel = medium

3 $MTTF_d$ of each channel = high

Figure 3 Relationship between categories' DC_{avg}, $MTTF_d$ and PL.
(SFS EN ISO 13849-1, p53)

In category B components, which are expected to endure specific conditions, will be used. Basic safety principles will be used. The range of $MTTF_d$ must be from 3 to 29 years. A fault in the system can lead to the loss of the safety function. (Siirilä 2009, p143)

In category 1 the requirements of B, as well as well-tried components and well-tried safety principles, will be used. The range of $MTTF_d$ must be from 30 to 100 years. A fault in the system can lead to the loss of the safety function, but the probability of harm is lower. (Siirilä 2009, p143 – 144)

In category 2 the requirements of B and the well-tried safety principles will be used with an external testing unit. The testing appliances must check the safety device's proper operation, at least 100 times between the needs of the safety device. The range of $MTTF_d$ will be from 3 to 100 years and DC_{avg} can be from 60 to 98 percentages. (Siirilä 2009, p144)

In category 3 the requirements of B and the well-tried safety principles will be used. The control system must be capable to perform a safety task, even though the system has one failure. The majority of failures have to be revealed. The range of $MTTF_d$ will be from 3 to 100 years and DC_{avg} must be from 60 to 98 percentages. (Siirilä 2009, p144)

In category 4 the requirements of B and the well-tried safety principles will be used. The control system must be capable to expose all failures in the control system. The system is implemented with an automatic monitoring system. The range of $MTTF_d$ will be from 30 to 100 years and DC_{avg} must be equal or over 99 percentages. (Siirilä 2009, p144)

Categories B, 1 and 2 are single channel devices. Fault exposing ability is implemented in categories 3 and 4 with two channels. The probability of common cause failures (CCF) must be low in categories 2, 3 and 4.

2.4.2 $MTTF_d$ of single channels

Manufacturers of safety components guarantee service life of their components with B_{10d} - or B_{10} –value, which can be used to calculate $MTTF_d$. The B_{10d} –value means how many cycles component will last until 10% of the components will fail dangerously. The B_{10} -value means component's service life, without considering the dangerous failures. If the ration of dangerous failures of B_{10} is not given by the manufacturer, ration of 50% can be used. B_{10d} and B_{10} are intended for pneumatic - and electromechanical components only. (SFS EN ISO 13849-1, p111)

Single channels' mean time to dangerous failure, indicated with three levels: low, medium and high, presented at table 7. These levels are used for determination of safety related control system's performance level.

Table 7 Mean time to failure of each channel.
(SFS EN ISO 13849-1, p45)

$MTTF_d$	
Denotation of each channel	**Range of each channel**
Low	3 years ≤ $MTTF_d$ < 10 years
Medium	10 years ≤ $MTTF_d$ < 30 years
High	30 years ≤ $MTTF_d$ ≤ 100 years

With the following formulas, single component's - and each channel's $MTTF_d$ –value can be estimated. The formulas are based on to the ISO 13849-1's annexes C and D.

$MTTF_d$ of single component:

$$MTTF_d = \frac{B_{10d}}{0{,}1 \times n_{op}} \quad (1)$$

where

$MTTF_d$ = single component's value.

$$n_{op} = \frac{d_{op} \times h_{op} \times 3600 s/h}{t_{cycle}} \quad (2)$$

h_{op} = mean operation, in hours per day.

d_{op} = mean operation, in days per year.

t_{cycle} = mean time between the beginning of two successive cycles of the component.

$MTTF_d$ of each channel:

When each individual safety component's $MTTF_d$ –value is calculated, whole channel's $MTTF_d$ is calculated with formula as presented below:

$$\frac{1}{MTTF_d} = \sum_{i=1}^{\tilde{N}} \frac{1}{MTTF_{di}} = \sum_{j=1}^{\tilde{N}} \frac{n_j}{MTTF_{dj}} \quad (3)$$

where

$MTTF_d$ = complete channel's value.

$MTTF_{di}$ & $MTTF_{dj}$ = $MTTF_d$ of each component which has a contribution to the safety function.

In two channel control systems, channels can be combined with formula as presented below, if $MTTF_d$ -values differ from each other. It is also permissible to straightaway use the channel, which has lower $MTTF_d$ –value. It is not necessary to combine the channels.

$MTTF_d$ of combined channels:

$$MTTF_d = \frac{2}{3}\left[MTTF_{d\,C1} + MTTF_{d\,C2} - \frac{1}{\frac{1}{MTTF_{d\,C1}} + \frac{1}{MTTF_{d\,C2}}}\right] \qquad (4)$$

where

$MTTF_d$ = combined channels.

$MTTF_{dC1}$ & $MTTF_{dC2}$ = two different redundant channels.

2.4.3 Diagnostic coverage (DC)

Diagnostic coverage means machine's safety-related control system's ability to detect a fault from itself. The DC is divided into four levels, low, medium, high or none (table 8). Levels are used to determine PL of safety-related control systems. To be practicable, the number of ranges is restricted to four. Higher DC –value than 99 percentage is very difficult to achieve in complex systems. (SFS EN ISO 13849-1, p49)

Table 8 Diagnostic coverage.
(SFS-EN ISO 13849-1, p49)

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

According to the standard ISO 13849-1, diagnostic coverage of logic, input – and output devices are determined in tables 9, 10 and 11 according to their testing device' function. Suitable section is evaluated and selected from the tables for each safety device.

Table 9 Evaluation of input devices diagnostic coverage.
(SFS EN ISO 13849-1, annex E)

Measure	**DC**
Input device	
Cyclic test stimulus by dynamic change of the input signals	90 %
Plausibility check, e.g. use of normally open and normally closed mechanically linked contacts	99 %
Cross monitoring of inputs without dynamic test	0 % to 99 %, depending on how often a signal change is done by the application
Cross monitoring of input signals with dynamic test if short circuits are not detectable (for multiple I/O)	90 %
Cross monitoring of input signals and intermediate results within the logic (L), and temporal and logical software monitor of the program flow and detection of static faults and short circuits (for multiple I/O)	99 %
Indirect monitoring (e.g. monitoring by pressure switch, electrical position monitoring of actuators)	90 % to 99 %, depending on the application
Direct monitoring (e.g. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)	99 %
Fault detection by the process	0 % to 99 %, depending on the application; this measure alone is not sufficient for the required performance level e!
Monitoring some characteristics of the sensor (response time, range of analogue signals, e.g. electrical resistance, capacitance)	60 %

Table 10 Evaluation of logics diagnostic coverage.
(SFS-EN-ISO 13849-1, annex E)

Measure	**DC**
Logic	
Indirect monitoring (e.g. monitoring by pressure switch, electrical position monitoring of actuators)	90 % to 99 %, depending on the application
Direct monitoring (e.g. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)	99 %
Simple temporal time monitoring of the logic (e.g. timer as watchdog, where trigger points are within the program of the logic)	60 %
Temporal and logical monitoring of the logic by the watchdog, where the test equipment does plausibility checks of the behaviour of the logic	90 %
Start-up self-tests to detect latent faults in parts of the logic (e.g. program and data memories, input/output ports, interfaces)	90 % (depending on the testing technique)
Checking the monitoring device reaction capability (e.g., watchdog) by the main channel at start-up or whenever the safety function is demanded or whenever an external signal demand it, through an input facility	90 %
Dynamic principle (all components of the logic are required to change the state ON-OFF-ON when the safety function is demanded), e.g. interlocking circuit implemented by relays	99 %
Invariable memory: signature of one word (8 bit)	90 %
Invariable memory: signature of double word (16 bit)	99 %
Variable memory: RAM-test by use of redundant data e.g. flags, markers, constants, timers and cross comparison of these data	60 %
Variable memory: check for readability and write ability of used data memory cells	60 %
Variable memory: RAM monitoring with modified Hamming code or RAM self-test (e.g. “galpat” or “Abraham”)	99 %
Processing unit: self-test by software	60 % to 90 %
Processing unit: coded processing	90 % to 99 %
Fault detection by the process	0 % to 99 %, depending on the application; this measure alone is not sufficient for the required performance level “e”!

Table 11 Evaluation of output devices diagnostic coverage.
(SFS-EN-ISO 13849-1, annex E)

Measure	**Diagnostic coverage (DC)**
Output device	
Monitoring of outputs by one channel without dynamic test	0 % to 99 % depending on how often a signal change is done by the application
Cross monitoring of outputs without dynamic test	0 % to 99 % depending on how often a signal change is done by the application
Cross monitoring of output signals with dynamic test without detection of short circuits (for multiple I/O)	90 %
Cross monitoring of output signals and intermediate results within the logic (L) and temporal and logical software monitor of the program flow and detection of static faults and short circuits (for multiple I/O)	99 %
Redundant shut-off path with no monitoring of the actuator	0 %
Redundant shut-off path with monitoring of one of the actuators either by logic or by test equipment	90 %
Redundant shut-off path with monitoring of the actuators by logic and test equipment	99 %
Indirect monitoring (e.g. monitoring by pressure switch, electrical position monitoring of actuators)	90 % to 99 %, depending on the application
Fault detection by the process	0 % to 99 %, depending on the application; this measure alone is not sufficient for the required performance level "e"!
Direct monitoring (e.g. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)	99 %
NOTE 1 For additional estimations for DC, see, e.g., IEC 61508-2:2000, Tables A.2 to A.15. NOTE 2 If medium or high DC is claimed for the logic, at least one measure for variable memory, invariable memory and processing unit with each DC at least 60 % has to be applied. There may also be measures that used other than those listed in this table.	

Entire safety feature's diagnostic coverage is called average diagnostic coverage (DC_{avg}). This is defined from each individual control system's component that participates into safety function. Both values, $MTTF_d$ and DC are used to calculate the DC_{avg}. Average diagnostic coverage is necessary for defining the performance level of the safety function and it is calculated with the formula presented below. The formula is from ISO 13849-1's, annex E.

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{d1}} + \frac{DC_2}{MTTF_{d2}} + \cdots + \frac{DC_N}{MTTF_{dN}}}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + \cdots + \frac{1}{MTTF_{dN}}} \qquad (5)$$

where

DC_{avg} = safety feature's control system's average diagnostic coverage.

$MTTF_{d1}$, $MTTF_{d2}$, $MTTF_{dN}$ = $MTTF_d$ of each component which has a contribution to the safety function.

2.4.4 Common cause failure (CCF)

Common cause failure means a failure that has simultaneously affectivity to more than one component. Safety-related control system’s must be able to cope from CCF problems and keep system safety. (Siirilä 2009, p.155)

The avoidance of CCF is given scores from 0 to 100. Sufficient prevention of CCF will be reached when the points are a total of 65 or more. The following table 12 shows the different methods for preventing the CCF. [SFS-EN ISO 13849-1, annex F]

Table 12 Common cause failures' prevention with ISO 13849-1. (SFS EN ISO 13849-1, annex F)

No.	Measure against CCF	Score
1	**Separation/ Segregation**	
	Physical separation between signal paths: separation in wiring/piping, sufficient clearances and creep age distances on printed-circuit boards.	**15**
2	**Diversity**	
	Different technologies/design or physical principles are used, for example: first channel programmable electronic and second channel hardwired, kind of initiation, pressure and temperature, Measuring of distance and pressure, digital and analog. Components of different manufactures.	**20**
3	**Design/application/experience**	
3.1	Protection against over-voltage, over-pressure, over-current, etc.	**15**
3.2	Components used are well-tried.	**5**
4	**Assessment/analysis**	
	Are the results of a failure mode and effect analysis taken into account to avoid common-cause-failures in design.	**5**
5	**Competence/training**	
	Have designers/ maintainers been trained to understand the causes and consequences of common cause failures?	5
6	**Environmental**	
6.1	Prevention of contamination and electromagnetic compatibility (EMC) against CCF in accordance with appropriate standards. Fluidic systems: filtration of the pressure medium, prevention of dirt intake, drainage of compressed air, e.g. in compliance with the component manufacturers' requirements concerning purity of the pressure medium. Electric systems: Has the system been checked for electromagnetic immunity, e.g. as specified in relevant standards against CCF? For combined fluidic and electric systems, both aspects should be considered.	**25**
6.2	Other influences Have the requirements for immunity to all relevant environmental influences such as, temperature, shock, vibration, humidity (e.g. as specified in relevant standards) bee considered?	**10**
	Total	**[max. achievable 100]**

Total score	**Measures for avoiding CCF**[a]
65 or better	Meets the requirements
Less than 65	Process failed ⇒ choose additional measures

[a] Where technological measures are not relevant, points attached to this column can be considered in the comprehensive calculation.

2.5 Performance requirements for robot's safety-related parts

According to the robot standard EN ISO 10218-2:

> Safety-related parts of control systems shall be implemented so that they comply with PL d with category 3 as described in EN ISO 13849-1. If IEC 62061 is used in the designation, control systems safety related parts will be designed so that they comply with SIL 2 with hardware fault tolerance of 1. (EN ISO 10218-2, p10)

2.6 Starting the machine

The machine can be started locally or by remote control. The remote controller can be used when it is ensured that the risk does not arise. In most cases, machines are equipped with a manual reset button. Button's function is to prevent unexpected start of the machine. Machine's reset function can be executed a way that several buttons must be pushed in the correct order to allow the machine to start. If the machine has hazardous zones, where user cannot see clearly, the multi-reset system gives a safety benefit. Additional reset button should be installed place, with a clear view to the danger zone. (SFS EN ISO 13849-1, p68-70)

2.7 Stopping the machine

When machine receives a stop command, the machine must slow the speed down to standstill as fast as possible. The stop command is prioritized to the highest level of the machine program. So by pressing the start and stop buttons at the same time, the stop is activated. (SFS EN ISO 13849-1, p68)

An emergency stop command might cause difficulties into production, particular to the re-starting of the machine. If the machine must necessarily do the movement completely, the machine could be equipped with an interlocking device. Interlocking device prevents human to access dangerous zones when machine moves. The locking devices are opened and accession allowed to hazard zones, once the machine is standstill. (SFS-EN ISO 13849-1, p70)

Interlocking devices are generally applied to machines that cannot be stopped quickly for reason such as high inertia. Machine's flywheel might have such a spinning mass that the machine cannot be stopped quickly.

Machine stoppages are divided into three classes according to ISO 13 850 and EN 60204-1 by. Classes differ from each other by their stop functionality. Safety-related stoppages are often classes 0 or 1. The class depends on to the machine-specific C-type standard. (Siirilä 2009, p278)

- In **class 0** stop, power supply is switched off immediately. Machine's movements will slow down freely or with assisted brake.
- In **class 1** stop, machine's power is maintained to provide controlled stop. The power supply is switched off after the stop.
- In **class 2** stop, machine's power is maintained to provide controlled stop. The power can be used to keep the machine in place.

(Siirilä 2009, p277)

2.8 Muting function

When muting function is activated, the safety device is switched off temporarily. The muting function shall not cause additional risk of injury. Safety must be carried out with other way. (SFS-EN ISO 13849-1, p72)

Passivation is used in automatic systems, for example transporting product between different stages of the process. Most commonly used safety devices, used for muting, are light curtains and light grids. The muting function requires additional sensors that the function can be executed. The product must have effect to the sensors in correct order and time. The sensors will detect the wrong type of object this way. Figure 4 illustrates the muting function. (Siirilä 2008 p160)

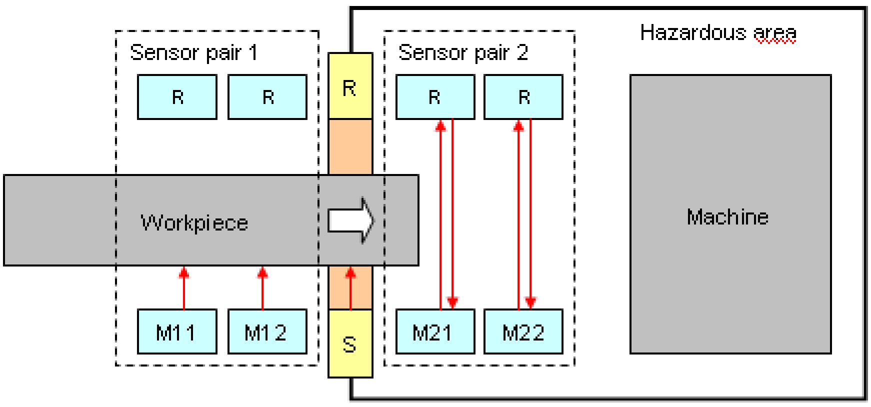


Figure 4 Muting system with safety light grid.
(Siemens 2012)

3 SAFETY COMPONENTS

3.1 Fail-safe CPU

Standard data as well as the safety data is handled by the fail-safe CPU. The fail-safe CPU, also called safety-PLC, provides an efficient control and monitoring for industrial purposes, when machine - or process safety is needed. Safety-PLC is connected via fieldbus technology to a variety of sensors and engine management components. An integrated complex system can be executed with safety-PLC. Diagnostics can be used to find causes of faults and production interruptions are therefore shorter. The system utilizes the open fieldbus communications systems such as PROFIBUS DP, PROFINET or wireless security communication IWLAN. STEP 7 –program and its safety license is needed to communicate with the safety-program. The safety-programming is made with the LAD and FBD programming languages in STEP 7, S7 Distributed Safety - or TIA Portal environment. (Siemens 2014a)

Figure 5 Siemens fail-safe programmable logic controller.
(Siemens 2014a)

3.2 Safety relay

The purpose of safety relay is to ensure circuit's operability and safety. The safety relays can be found wide variety of uses and is selected according to the usage. The safety relay has the following uses:

- Monitoring emergency stop buttons, safety switches and light curtains.
- Monitoring contactors and control valves.
- Monitoring safety circuits against short-circuits.
- Monitoring engine stop.
- Monitoring safety relay's own activities.
- Short-circuit supervision.

Figure 6 shows circuit that does not have a safety relay. The following problems are possible:

- Circuit's control voltage may conduct directly to the contactor in case of short circuits.
- The control button's contact damage can cause contactor to remain on.
- Contact's sticking can cause hazard or breakdown.

(OEM)

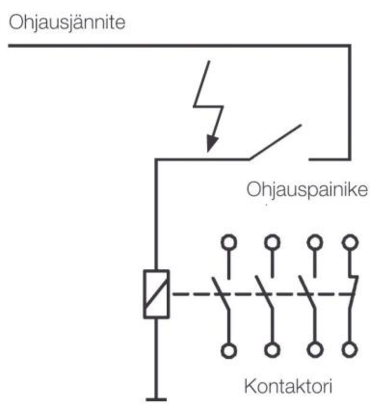


Figure 6 System without safety relay
(OEM)

3.3 Safety switcgear

This section contains safety sensors, used types of hatches and doors. The safety switchgear consists of two parts, the safety switch and the separate actuator. When door or hatch is in production position, the safety switch and its actuator are close to each other.

3.3.1 Safety switch

The safety switch is made up of two parts, the safety switch and the separate actuator key. The switches include a force guided contacts, which are directed to the influence of actuator key. Safety interlocking switch locks the actuator key inside the switch. The safety switch can be equipped with a unique coding. Actuator key and switch are shaped in a way that works only together. The coding is made central section of the actuator key as in figure 7. Coding prevents manipulation of the safety switch with an external actuator.

Even if the safety switch has two-channels, it has a single-channel mechanic (the key part). A single safety switch might be suitable for PL a, b and c applications. If can be ensured that the mechanics does not break, the device could be suitable for applications PL d. If two single channel safety switches are used to execute the same safety feature, PL e is possible.

Figure 7 Typical safety switch.
(Schmersal 2011)

3.3.2 Safety sensors

Magnetic, inductive and RFID-sensors are the typical safety sensors. The main advantage of the sensors compared to conventional safety switches is contactless technology. External mechanical wear will not happen.

Magnetic safety sensor consists of two separate components, the sensor, as well as the counter-magnetic actuator, see figure 8. Actuator's magnets are in a certain order, so that any magnet cannot activate the sensor. The magnetic sensor includes a reed contacts which are operated with the magnets.

The difference between the magnetic-, Inductive- and RFID-sensor are a little more complexity in their structure. Inductive- and RFID-sensors can be equipped with a unique coding. Coding will reduce the possibility to manipulation.

Figure 8 Schmersal magnetic safety sensor.
(Schmersal 2012a)

3.4 Safety light curtain and safety light grid

The safety light curtains and - light grids consists of a transmitter and a receiver. The transmitter sends infrared light to receiver, which monitors the coming light with safety monitor. Light curtains are used to prevent access to the danger zones. If a light beam is interrupted between transmitter and receiver, the safety monitor detects this and sends a signal to the safety-related control system for the necessary actions. The main difference between safety light curtain and light grid is quantity of the light beams. (Schmersal 2013)

The typical light grid has 1, 2, 3, or 4 light beams. The light is emitted directly horizontally from the transmitter to the receiver. Sometimes beams are directed to emit light from corner to corner creating a cross to the middle of light grid.

Figure 9 Pallet wrapping machine’s safety light grids (four yellow posts, two at front and two further behind the wrapping machine).

3.5 Safety components of AC-drives

The AC-drives can be stopped without need to cut power down immediately. The AC-drive can be equipped with a specific Safe Torque Off -safety circuit board, which integrates the AC-drive into the safety-related control system. This feature eliminates drive’s start up delay and ease use of the drive. (Vacon 2014)

Figure 10 illustrates the behaviour of the motor during safety-related stop. After stop command (red arrow), the motor slows down the speed linearly to till standstill (blue line). A moment after standstill, AC-drive is triggered to the Safe Torque Off –state (STO arrow). An external timer is needed to execute Safe Stop 1 (SS1) function. The timer could be OFF-delayed safety relay which delay time is the Δt in picture 10. During class 0 STO -function, STO state is launched immediately when stop is requested and motor slows the speed down freely. (Vacon 2014)

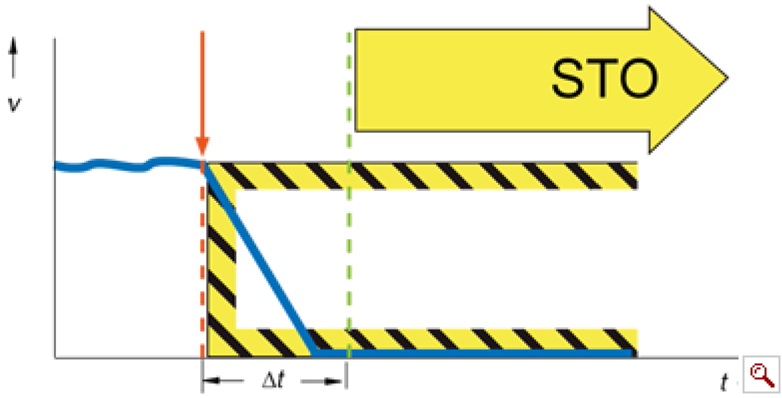


Figure 10 Safe Stop 1 (SS1).
(Siemens 2014b)

4 FIELDBUSSES

4.1 AS-interface

The AS-i fieldbus consists of one master device and maximum quantity of 31 slave devices. Four input - and four output devices can be connected into each slave. The master unit and the slaves are connected to each other with the same two-wire cable. Cable length can be up to 100 meters and with repeater the length can be extended up to 300 meters. The system may use any topology selected. AS-i field bus is used to reduce the maintenance and installation costs. New AS-i components can be easily connected to the existing system. The new component is connected to the nearest AS-i cable. (AS-interface)

The AS-interface is called AS-i Safety at Work if safety-related data is transferred simultaneously with standard data through the same AS-i bus. (Siirilä 2009, p 128)

Each safety-related slave is identified with 8x4 bit code table. Each slave's code table is taught to the AS-i master. During the production the master device compares the received and taught tables. The AS-i master cause machine to stop if found any of following deviations:

- Communication is interrupted.
- Transmitted 8*4 bit tables are wrong.
- Safe slave is missing or destroyed.
- Delayed slave responses were detected.

(AS-interface)

4.2 ProfiBUS

The Profibus is an open, digital communication system with wide range of applications, particularly in the fields of factory and process automation. The

Profibus is suitable for both fast, time-critical applications and complex communication tasks. (PROFIBUS user organisation 2002)

Profibus DP (Decentralized Periphery) is the simple, fast, cyclic and deterministic process data exchange between a bus master and the assigned slave devices. Profibus DP has three versions DP-V0, DP-V1 and DP-V2. The newest version DP-V2 provides for direct slave-to-slave communication with an isochronous bus cycle. (PROFIBUS user organisation 2002)

The Profibus is called PROFIsafe if safety-related data is transferred simultaneously with standard data through the same bus. (Siirilä 2009, p 128)

4.3 DP / AS-i F-link

The AS-i devices are connected to the fail-safe CPU via Profibus DP. The AS-i and the Profibus DP are linked to each other with the DP / AS-i F-Link -device. The DP / AS-I F-Link provide data communication between AS-i slaves and fail-safe CPU. The DP / AS-i F-Link operate at the same time as AS-i master and Profibus DP's slave. Device consists of two AS-i channels: A and B. 62 standard slave devices, or 31 safety slave devices can be connected to the DP / AS-I F-Link. (Siemens 2006)

Figure 11 is an example about a system using the DP / AS-i F-Link. The image illustrates interconnection between different devices. Fail-safe CPU monitors AS-i busses emergency stop button, as well as the protective door's safety switches. The fail-safe CPU controls contactors Q1 and Q2 via distributed I / O.

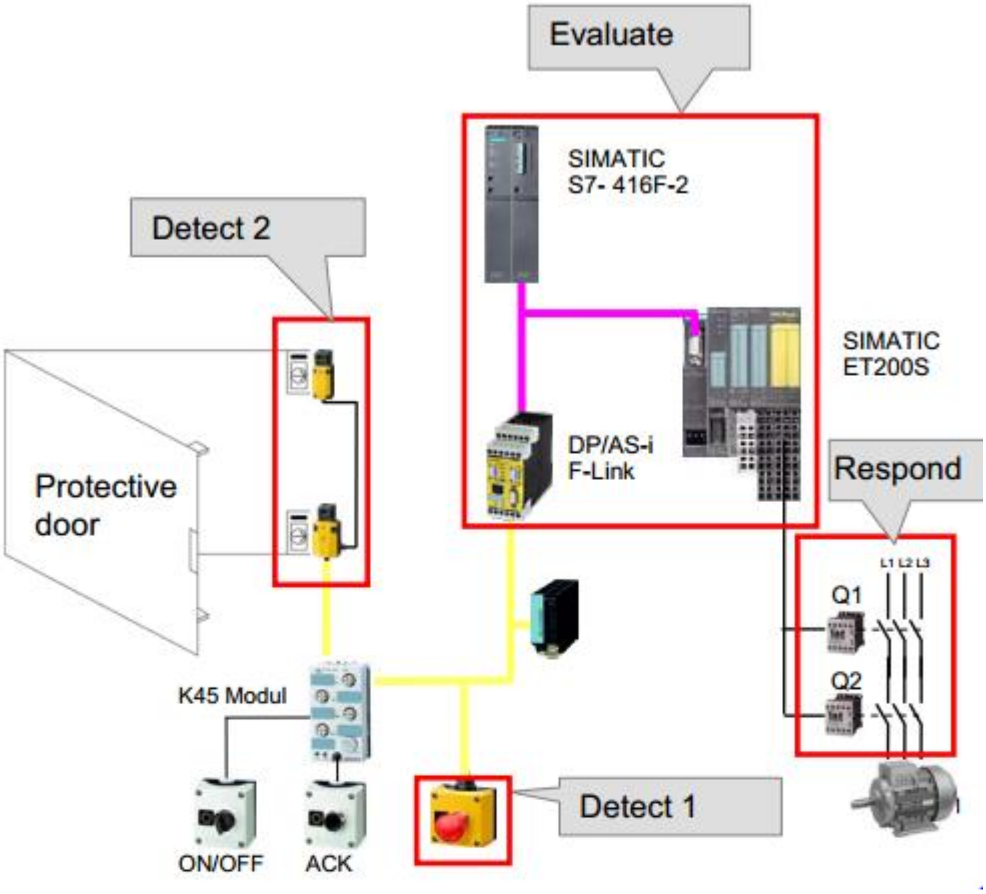


Figure 11 Example of system configuration with DP / AS-i F-Link. (Siemens 2008)

5 PALLETIZING SYSTEM

5.1 System review

Palletizing system includes elevator cells, robotic cells, pallet carrier cell and pallet wrapping cell, see figure 12. Products containing boxes are lifted with elevator cell 2.5 meters above from ground to till conveyors. The conveyors carry the boxes from all cells to robotic cells and if necessary from lines 3, 9 and 10 to till trolley cell. The robotic cells load boxes on to the pallets. The pallet carrier cell carries finished pallets from robotic cells to pallet wrapping machine. Wrapping protects and supports the products during delivery.

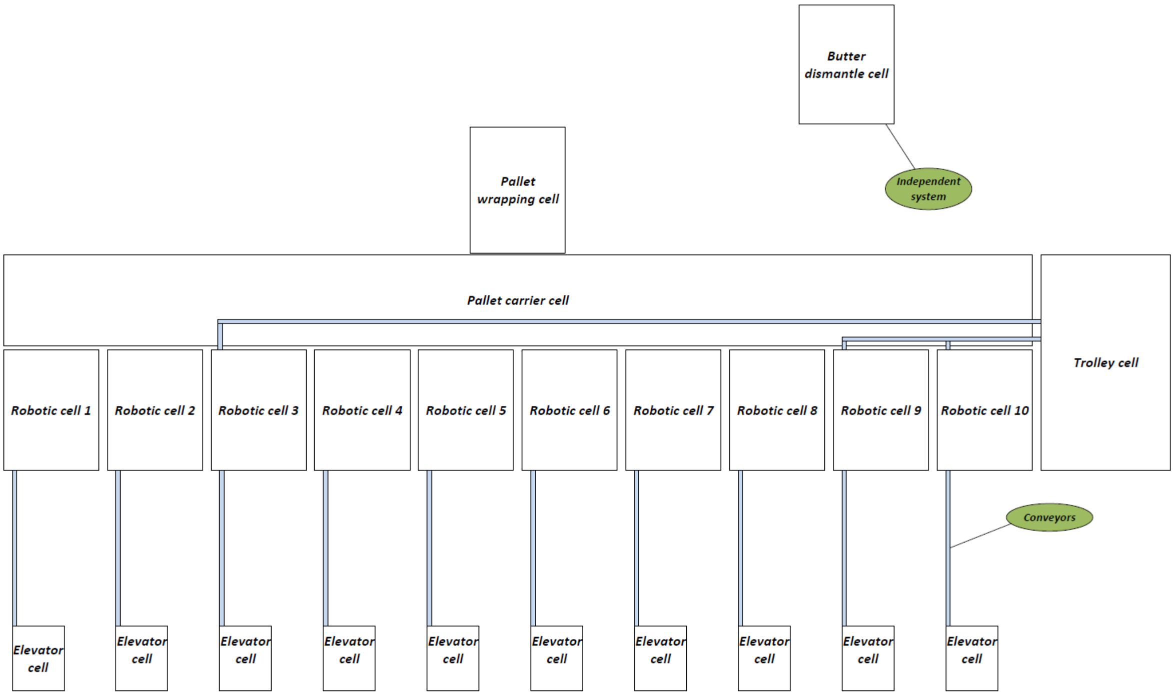


Figure 12 Overview of the palletizing machine.

Palletizing system's data transfer is carried out with the Profibus DP - and the AS-i interfaces. System's execution is present in figure 13. A single fail-safe CPU controls everything except wrapping machine, which have own PLC. However wrapping machine's safety devices are connected to the fail-safe CPU. Each cell and robot has own central electrical units, where distributed I / O and other devices are available.

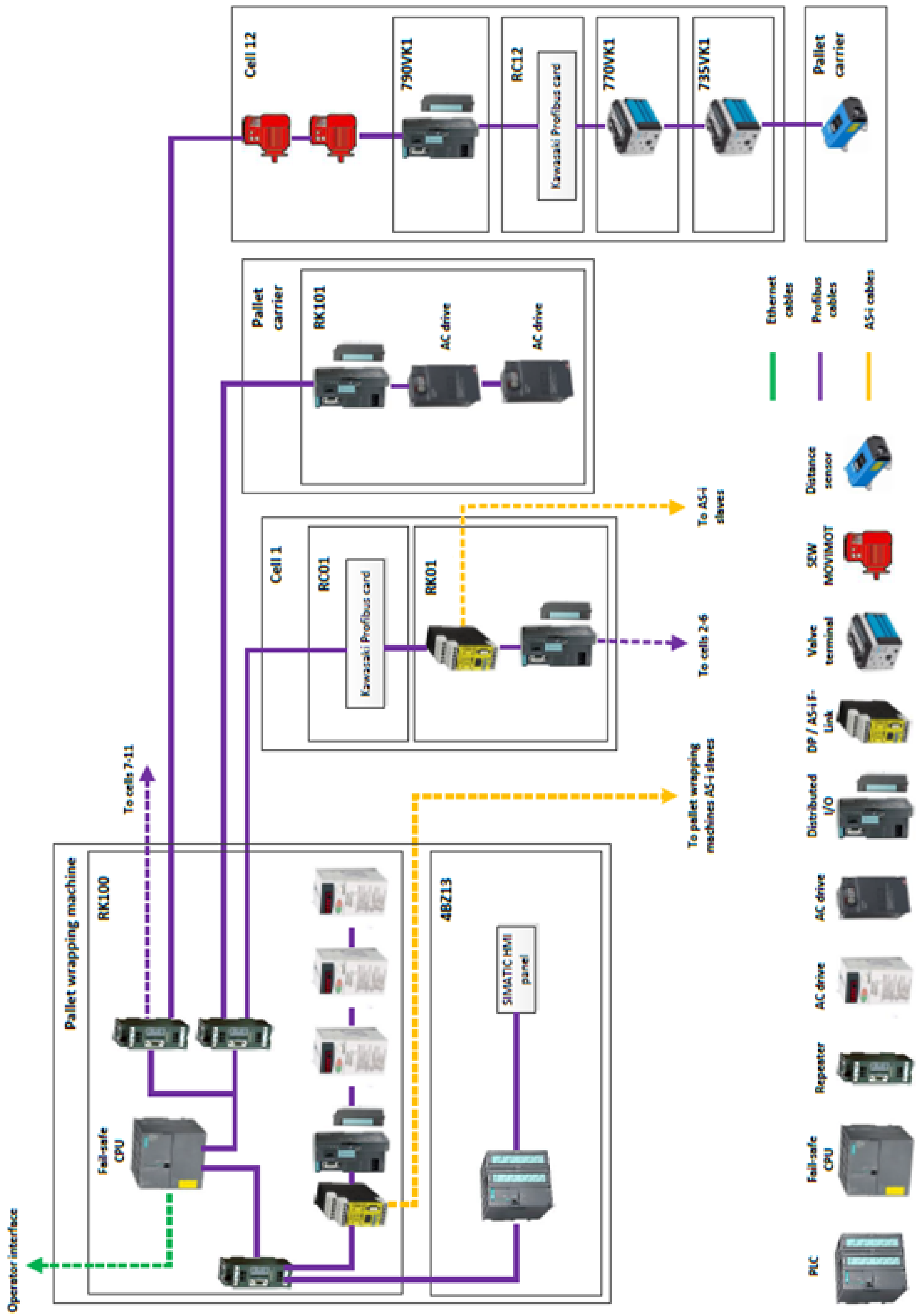


Figure 13 Overview of the palletizing system Profibus - and AS-i busses.

5.2 Risk assessment of robotic cells

The original risk assessments made by manufacturer were not available, so methods from Siirilä's book (Koneturvallisuus, 2008) were used. Guidance from Valio Ltd's own instructions were also used. The risk assessment conducted concerns the robotic cells from 1 to 10, as well as trolley cell. Due to the cells' similar operation, it was not considered necessary to carry out the risk assessment in each cell separately. With the information from risk assessment, conclusions were made as follows: The robot cells' service doors old safety switches are too risky to use and the switches must be upgraded during spring 2014.

5.3 Service doors

The purpose of service doors is to prevent person's access to hazard zones, when robot is operating. The door's position is monitored with AS-i -compatible Siemens safety switch. The service door's locking is executed with sideways movable latch. The safety switch's actuator key is attached to the latch. The latch protects the safety switch and it's actuator against lateral forces, which are caused if the door is pulled, when door latch is in lock position.

During the inspection, it was found that safety switch's actuator key may hit to the door frame, if the latch is in mid-position (figures 15 and 16). Marks on the door frame were detected each hinge equipped door. Failure is fixed by moving the latch so that it extends slightly beyond the safety switch's actuator (figure 17). The failure was easy to repair by drilling new mounting holes and making new treads to them (figure 18 and 19).

Figure 14 Front view of the service door.

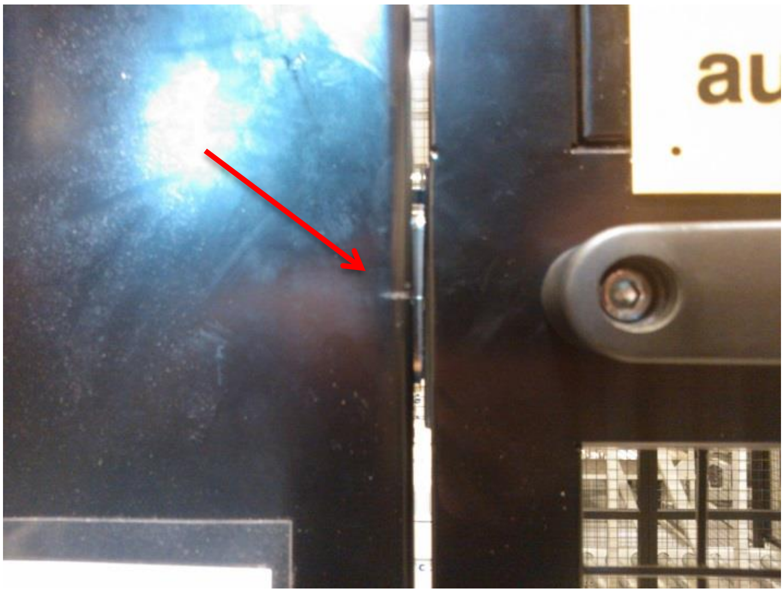


Figure 15 Hitting marks on the door frame.

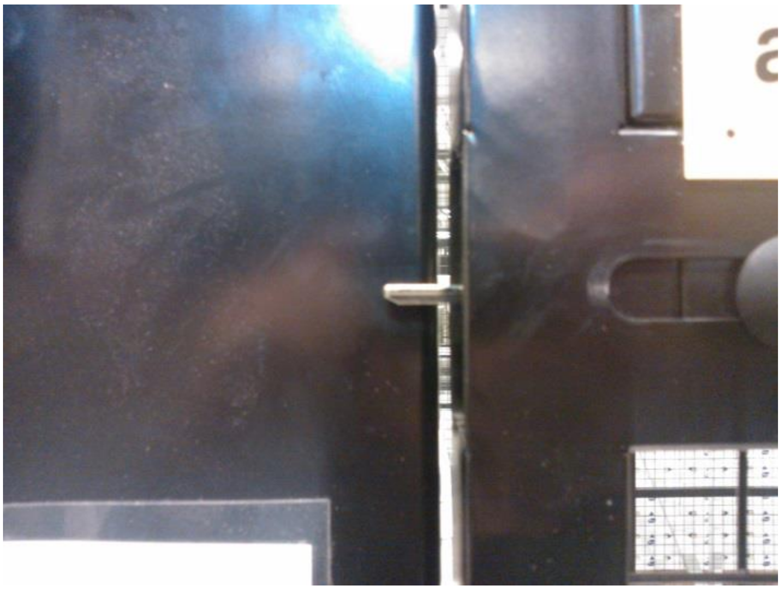


Figure 16 Safety switches actuator key may hit to the door frame.

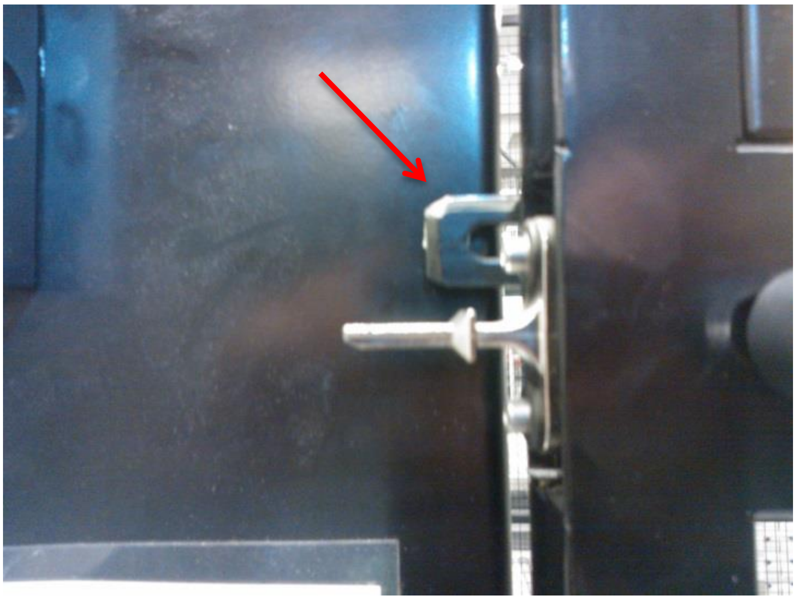


Figure 17 The latch is too short.


Figure 18 Fixing the latches.

Figure 19 Improved latch in place.

If the latch hit hard to the door frame, it can cause fractures into the mounting screws or threads can be damaged. This could cause a serious accident, if the robot is stopped by opening the service door and then partially damaged safety switch's key remain in place.

Referring to the theory section, when safety-related control system is PL d and category 3, control system must be able to carry out a safety feature even if the system has one fault. The requirement to satisfy the claim, the safety switches actuator can't fail. Due to a safety switch's single channel mechanical parts, it was decided to use the additional safety on service doors. Cells 1 to 10 will be equipped with RFID-type of safety sensors (figure 20). Each cell has 32 free, unused AS-i device addresses. Use of two safety devices will allow safety function to be accomplished if either of the devices damages.

Figure 20 Service doors' new RFID-sensor.
(Schmersal 2012b)

The trolley cell does not contain an AS-i fieldbus, so the new safety switch's wirings are executed with the conventional wirings. The cell has a safety input card that has space for two single devices or one dual channel safety device. The dual channel device will be used.

Service door's adequate safety could be achieved by replacing the old safety switch with one non-contact type of safety sensor. However, this is not going to be used, because two switches give a more secure solution. Second idea was to use two single-channel safety switches. The first channel could be the basic safety switch and the second channel's device a hinge switch. The advantage of this kind of system would be a good ability to prevent manipulation. This is not approved, because of the cross-channel asynchronous operation as well as difficulties mounting the hinge-switch.

5.4 Pallet removal doors

Pneumatic operated cylinder opens and closes the pallet removal door. The pallet removal door allows automatic removal of the finished pallets from the cell. The pallet doors' position is monitored with a safety switch. Pallet removal door is open only, when finished pallet moves from the robot cell to the pallet carrier. The safety switch is muted during pallet removal. Doors have had problems with actuators not contacting with the safety device. It was decided that the pallet removal doors are to be equipped with contactless safety sensors. Because of cheap prize, Allen Bradley safety sensors were chosen.

Figure 21 Safety switch's actuator does not always hit to the right place.

5.5 Pallet feeders

Pallets are automatically supplied to the robotic cell with the pallet feeder. Lowest pallet of stack is moved to robotic cell's work zone with help of conveyors and stack lifters. The pallet feeder during production is illustrated in figure 22.

Figure 22 Front view of pallet feeder.

The pallet feeder's safety was considered to be in order. Here again, improvements were planned for the machine. The most likely danger occurs when the pallets are loaded into too high towers to the pallet feeder. However it is not possible to transport very high stacks of pallets inside factory. In addition, employees have been instructed to stack no more than 12 pallet high stacks, see figure 22. If a pallet stack height measurement device would be built, the best result could be obtained with a single light grid. Manipulation would be difficult enough with the light grid.

5.6 Elevator cells

According to the risk assessment, the elevator cells' safety devices were considered to be in order. The cells have two doors and their position is monitored by the Siemens safety switch, same as the service doors' of robotic cells. Any changes to the elevator cells were not required.

Figure 23 Elevator cell.

5.7 Other machines

Pallet carrier cell, wrapping machine and dismantling robot will be equipped with additional safety sensors. The dismantling robot has four service doors where the wrapping machine and the pallet carrier have both two service doors. All eight doors will be equipped with one additional RFID-safety sensor.

5.8 Example calculation of a service doors performance level with additional safety sensor.

The robotic cell’s service doors safety function is executed with:

1. Siemens failsafe CPU
2. Siemens DP / AS-I F-Link

3. Service doors safety position switch 2-channel (Siemens)
4. Service doors safety position sensor 2-channel (Schmersal)
5. Safety relay (robots electrical center needs two relay output contacts)
6. Siemens safety-related distributed output device
7. Robots power supply contactors

Table 13 presents the safety data collected from manufacturers. $B10_d$, $MTTF_d$ and DC_{avg} were calculated from the safety data with the help of the theory section. $MTTF_d$ and DC_{avg} calculations are presented at sections 5.8.1 and 5.8.2. Results and conclusions made, are presented at summary section (5.8.3).

Table 13 Data collected from the manufacturers. $B10_d$ and $MTTF_d$ are calculated values, all DC_{avg} –values estimated.
(* Siemens 2010, ** Schmersal 2012b, *** Sick 2013, ****Schneider Electric 2014)

Data source	Type	Product	SIL	PFHd	PL	Cat	Life time	Ratio of dangerous failures	B10	B10d	MTTFd (years)	Dcavg (%)
*	Siemens CPU 319F	6ES7318-3FL00-0AB0	3	4,00E-09	e	4	20	-	-	-	460	≥99
*	DP / AS-i F-Link	3RK3141-.CD10	3	3,00E-09	e	4	20	-	-	-	750	≥99
*	Safety position switch	Siemens 3SF1...-...V..	-	-	-	-	20	20	1000000	5000000	7576	90
**	Safety sensor	Schmersal RSS36AS	3	5,13E-10	e	4	20	-	-	-	2300	≥99
***	Safety relay	UE48-20S	3	3,00E-08	e	4	20	-	-	-	82	≥99
*	Fail-safe output module	6ES7318-3FB02-0AB0	3	1,00E-10	e	4	20	-	-	-	>2500	≥99
****	Power supply contactors	Schneider electric, TESYS, nominal load	-	-	-	-	20	73	1000000	1369863	2076	99

5.8.1 Total $MTTF_d$ level of safety function

Manufacturers reported PFHD -values were used. Tables of appendixes 1 and 2 were used to convert the PFHD to $MTTF_{d.}$ The tables are based on the ISO 13849-1’s annex K. Lower $MTTF_d$ values than 100 years are converted with appendix 1. Higher $MTTF_d$ values than 100 years can be evaluated with the table that can be found in appendix 2.

Siemens safety switch:

$B10_d$ = B10 / ratio of dangerous failures % = 1 000 000 / 20% = 5 000 000

h_{op} = 15 hours*

d_{op} = 330 days*

t_{cycle} = (15h x 60min x 60s) / 20 = 2700s**

*Production operational in two shifts. (7.5h x 7.5h = 15h).

**On average the door is opened 20 times a day.

$$n_{op} = \frac{d_{op} \times h_{op} \times 3600s/h}{t_{cycle}} \qquad (2)$$

n_{op} = (330d * 15h * 3600s/h) / 2700s = 6600

$$MTTF_d = \frac{B_{10d}}{0{,}1 \times n_{op}} \qquad (1)$$

$MTTF_d$ = 5 000 000 / (0,1 x 6600) = 7575,758 (years)

$MTTF_d$ of Siemens safety position switch is approximately 7576 years.

Schneider electric Tesys contactors:

$B10_d$ = B10 / ratio of dangerous failures % = 1 000 000 / 73% = 1 369 863

h_{op} = 15 hours*

d_{op} = 330 days*

t_{cycle} = (15h x 60min x 60s) / 20 = 2700s**

* Production operational in two shifts. (7.5h x 7.5h = 15h).

**On average the door is opened 20 times a day.

$$n_{op} = \frac{d_{op} \times h_{op} \times 3600s/h}{t_{cycle}} \quad (2)$$

n_{op} = (330d x 15h x 3600s/h) / 2700s = 6600

$$MTTF_d = \frac{B_{10d}}{0,1 \times n_{op}} \quad (1)$$

$MTTF_d$ = 1 369 863 / (0,1 x 6600) = 2075.55 (years)

$MTTF_d$ of Schneider electric contactors are approximately 2076 years.

Next the whole channel's average $MTTF_d$ is calculated. All individual $MTTF_d$ – values are connected.

$$\frac{1}{MTTF_d} = \sum_{i=1}^{\tilde{N}} \frac{1}{MTTF_{di}} = \sum_{j=1}^{\tilde{N}} \frac{n_j}{MTTF_{dj}} \quad (3)$$

$$\frac{1}{MTTF_d} = \frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + \frac{1}{MTTF_{d3}} + \frac{1}{MTTF_{d4}} + \frac{1}{MTTF_{d5}} + \frac{1}{MTTF_{d6}} + \frac{1}{MTTF_{d7}}$$

$$\frac{1}{MTTF_d} = \frac{1}{460} + \frac{1}{750} + \frac{1}{7576} + \frac{1}{2300} + \frac{1}{82} + \frac{1}{2500} + \frac{1}{2076}$$

$MTTF_d$ = 58,306 ~ 58 (years)

5.8.2 DC_{avg} of safety function

Manufacturers do not always give information about their product's diagnostic coverage. All devices which are performance level e, the devices' diagnostic coverage must be at least 99 percent and that is why for individual devices' DC_{avg} was estimated ≥99 percent, see table 13. For Siemens safety switch the DC_{avg} was evaluated and selected with table 9. From table the following part was selected:

- Cyclic test stimulus by dynamic change of the input signals = 90 %.

Contacts must close and open within a specified time and order so that the machine can be started. This way the machine recognizes damaged contact.

For Schneider electric Tesys contactors DC was selected with table 11. From the table the following part was selected:

- Direct monitoring (e.q. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements = 99 %.)

Safety PLC monitors contactors' actual position with auxiliary contacts which are connected directly to the contactors' main contacts. This way safety PLC recognizes damaged contacts. Next the average diagnostic coverage of the service door safety-related control system is calculated with the formulas presented in the theory part:

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{d1}} + \frac{DC_2}{MTTF_{d2}} + \cdots + \frac{DC_N}{MTTF_{dN}}}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + \cdots + \frac{1}{MTTF_{dN}}} \quad (5)$$

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{d1}} + \frac{DC_2}{MTTF_{d2}} + \frac{DC_3}{MTTF_{d3}} + \frac{DC_4}{MTTF_{d4}} + \frac{DC_5}{MTTF_{d5}} + \frac{DC_6}{MTTF_{d6}} + \frac{DC_7}{MTTF_{d7}}}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + \frac{1}{MTTF_{d3}} + \frac{1}{MTTF_{d4}} + \frac{1}{MTTF_{d5}} + \frac{1}{MTTF_{d6}} + \frac{1}{MTTF_{d7}}}$$

$$DC_{avg} = \frac{\frac{99}{460} + \frac{99}{750} + \frac{90}{7576} + \frac{99}{2300} + \frac{99}{82} + \frac{99}{2500} + \frac{99}{2076}}{\frac{1}{460} + \frac{1}{750} + \frac{1}{7576} + \frac{1}{2300} + \frac{1}{82} + \frac{1}{2500} + \frac{1}{2076}}$$

DC_{avg} = 98,931 ~ 98,9 (%)

5.8.3 Summary

Table 7 presents that if system's $MTTF_d$ is 58 years, the channels $MTTF_d$ is high. Table 8 presents that if the average diagnostic coverage is 98,9 percent, the level of DC_{avg} is then medium. With this information the performance level of a single channel of a safety-related control system can be defined with theory section's figure 3. From the picture, it can be concluded that the calculated performance level is d.

Siemens safety switch drops the average diagnostic coverage of whole system from 99 to 98.9 percent and, therefore, PL drops from e to d. However, both the safety devices of the service door are two channelled and working parallel, so they can be perceived as one safety device. If the control system monitors synchronously both the device's opening and closing, the service door's safety switch's combined DC could be 100 percent. Nevertheless by using only the safety sensor, the control system's performance level is e and therefore DC_{avg} is at least 99 percent. Service door's new performance level will be e.

5.9 Requirements for safety program

Service door has two dual-channel safety devices and therefore the total amount of channels is four. The control system will be monitoring all the four channels. The control system will be able to monitor the synchronous closing and opening of both devices. This will allow the detection of a jammed safety device actuator. Pallet removal doors' new safety switches do not need any program changes.

5.10 Implemention of changes

Installing and programming will be done by the palletising system's manufacturer Orfer Oy. The changes will be made during the spring, at a weekend, when the factory unit's production schedule allows a stoppage. Orfer Oy will make the installation of sensors, connections, program changes, as well as the necessary changes to the machinery documentation.

The implementation of changes was given to a third party because of insufficient knowledge about the palletising system program and, in addition, Valio Ltd does not have the required safety licence for accessing the safety program.

6 SUMMARY

Palletising system is made with very high quality components. The switch of the service doors is not the best solution for the robotic safety device which is used quite often. Elsewhere any safety defects were not discovered. Some mechanical problems were found in the existing safety switch installations and they were repaired.

Risk assessment, as well as a more detailed examination of the control system should have been done separately to the wrapping machine and to the pallet carrier cell. These machines do not necessarily need to be equipped with additional new safety sensors. At the beginning, the work was limited to the robotic cells' service doors only, and for this reason risk assessments for the wrapping and pallet carrier machines were not made. However, the improvement costs of the wrapping machine and pallet carrier cells are small. The acquisition of the safety license of STEP 7 will be considered, as it could be used for other factory's applications in the future.

BIBLIOGRAPHY

AS-interface. No date. Facts and advantages. [Web page]. As-interface. [Refered 10.3.2014]. Available: http://www.as-interface.com/knowledge-base/safety-at-work

AS-interface. No date. Safety at work. [Web page]. As-interface. [Refered 10.3.2014]. Available: http://www.as-interface.com/knowledge-base/safety-at-work

DGUV Test. 2012. An introduction to the determination of performance levels in accordance with EN ISO 13849-1. [Online publication]. DGUV Test. [Refered 10.3.2014]. Available: http://www.bgdp.de/pages/medien/auswahl_nach_art/maschinenpruefung/download/Pruefstellen-Info-Nr_926e.pdf

EN ISO 10218-2. 2011. Robots and robotic devices – Safety requirements for industrial robots – Part 2: Robot systems and itegration. Helsinki: Finnish standards association.

OEM AUTOMATIC. No date. Yleistä turvareleistä. [Online publication]. OEM Finland Oy. [Refered 20.03.2014]. Available: http://util.oem.se/pdf/Yleista_turvareleista.pdf

PROFIBUS user organisation. 2002. PROFIBUS, Technology and Application. [Online publication]. PROFIBUS Nutzerorganisation e.V. PNO. [Refered 29.3.2014]. Available: http://www.pacontrol.com/download/profibus-overview.pdf

Schmersal. 2011. AZ 16-12ZI-B6R. [Online catalog]. K.A. Schmersal GmbH & Co. KG. [Refered 29.03.2014]. Available: http://www.schmersal.net/cat?lang=fi&produkt=i3v7352906bqoj9ls9f46312kiyfbd

Schmersal. 2012a. BNS 260-02ZG-L. [Online catalog]. K.A. Schmersal GmbH & Co. KG. [Refered 29.03.2014]. Available: http://www.schmersal.net/cat?lang=fi&produkt=qg273313650yo3phpz549506b9pvbt&tab=Dat

Schmersal. 2012b. RSS 36-I2-ST-AS. [Online catalog]. K.A. Schmersal GmbH & Co. KG. [Refered 29.03.2014]. Available: http://www.schmersal.net/cat?lang=fi&produkt=hvf734770eelptyjru028811p31ub1&tab=Dat

Schmersal. 2013. Turvavaloverhot, turvavalopuomit. [Online catalog]. K.A. Schmersal GmbH & Co. KG. [Refered 29.03.2014]. Available:

http://www.schmersal.net/cat?lang=fi&produkt=8r1732924ckumrn4e6j561158z5fmi#

Schneider Electric. 2014. Schneider Electric SISTEMA Library. [Refered 27.3.2014]. Require use of SISTEMA program. Available: http://www2.schneider-electric.com/sites/corporate/en/solutions/oem/machine-safety/machine-safety.page

Schneider Electric. 2009. Safe Machine Handbook. [Online publication]. Schneider Electric. [Refered 15.3.2014] Available: http://www.schneider-electric.fi/documents/original-equipment-manufacturers/pdf/Machine-safety-guide.pdf

SFS EN ISO 13849-1. 2008. Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design. Helsinki: Finnish standards association.

Siemens. 2006. ASIsafe, DP / AS-i F-Link. [Online publication].Siemens AG. [Refered 10.3.2014]. Available: http://cache.automation.siemens.com/dnl/Tc/Tc5MDY5NwAA_24196041_HB/DP_AS-i_F-Link_Manual_2006-10_X-2011-04_en.pdf

Siemens. 2008. ASIsafe solution PROFIsafe, emergency stop with protective door monitoring. [Online publication]. Siemens AG. [Refered 25.3.2014]. Available: http://cache.automation.siemens.com/dnl/Tc/TcyNjE1MQAA_31895788_Tools/CD-FE-I-049-V30-EN.pdf

Siemens. 2010. Safety evaluation tool. Safety evaluation tool. [Refered 1.2.2014]. Require booking. available: http://www.industry.siemens.com/topics/global/en/safety-integrated/machine-safety/safety-evaluation-tool/Pages/default.aspx

Siemens. 2012. Distributed Use of a Safety Light Curtain on a SIMATIC F-CPU. [www-publication]. Siemens AG. [Refered 29.3.2014]. Available: http://cache.automation.siemens.com/dnl/DU/DU0MDk5OQAA_58793869_Tools/58793869_LIGHT_CURTAIN_DOKU_V10_EN.pdf

Siemens. 2014a. Turvalogiikat. [Web page]. Siemens AG. [Refered 10.3.2014]. Available: http://www.automation.siemens.com/mcms/programmable-logic-controller/en/simatic-s7-controller/s7-300/cpu/fail-safe-cpus/pages/default.aspx

Siemens. 2014b. Safe Stop 1. [Web page]. Siemens AG. [Refered 29.3.2014]. Available: http://www.industry.siemens.com/topics/global/en/safety-integrated/machine-safety/product-portfolio/drive-technology/safety-functions/pages/safe-stop1.aspx

Siirilä, T. 2008. Koneturvallisuus, EU-määräysten mukainen koneiden turvallisuus. 2th renewed edition. Keuruu: Otavan Kirjapaino Oy.

Siirilä, T. 2009. Koneturvallisuus. Ohjausjärjestelmät ja turvalaitteet. 2th renewed edition. Keuruu: Otavan Kirjapaino Oy.

Sick. 2013. Sick SISTEMA library. [Refered 27.3.2014]. Require use of SISTEMA program. Available: http://www.sick.com/group/en/home/products/product_portfolio/safexpert/Pages/safexpert.aspx

Sundquist, M, Sundcon Oy. 2010. Turvallisuusvastuut koneiden modernisoinnissa - eurooppalaiset turvallisuusvaatimukset. [Online publication]. MetSta ry. [Refered 29.3.2014]. Available: http://www.metsta.fi/www/koneturvallisuuden_teemasivut/artikkelit/2010_nro_008.pdf

Vacon. 2014. Vacon 100, OPTBJ, STO- ja ATEX-optiokortti, käyttö- ja turvaopas. [pdf-document]. Vacon Oyj. [Refered 29.3.2014]. Available: http://www.vacon.com/ImageVaultFiles/id_4780/cf_2/Vacon-100-OPTBJ-STO-User-Manual-DPD01057A-FI.PDF

Valio Ltd. 2014a. Valio yrityksenä. [www-document]. Valio Ltd. [Refered 6.1.2014]. Available: http://www.valio.fi/yritys/yritystieto/

Valio Ltd. 2014b. Weeti Portal. Available at Valio Ltd:s internal network.

APPENDICE

APPENDIX 1. $MTTF_d$ to PFHD conversion table.

APPENDIX 2. Extended $MTTF_d$ to PFHD conversion table.

APPENDIX 3. Service doors verification calculation report with SISTEMA

APPENDIX 4. The risk assessment has been deleted for the company's request.

APPENDIX 1

MTTF$_d$ for each channel [years]	Probability of Dangerous Failure per Hour (PFH) [1/h] and related Performance Level (PL)													
	Cat. B DC$_{avg}$ =none	PL	Cat. 1 DC$_{avg}$ =none	PL	Cat. 2 DC$_{avg}$ =low	PL	Cat. 2 DC$_{avg}$ =medium	PL	Cat. 3 DC$_{avg}$ =low	PL	Cat. 3 DC$_{avg}$ =mediuml	PL	Cat. 4 DC$_{avg}$ =high	PL
10	$1,14 \times 10^{-5}$	a			$7,18 \times 10^{-6}$	b	$5,14 \times 10^{-6}$	b	$3,21 \times 10^{-6}$	b	$1,36 \times 10^{-6}$	c		
11	$1,04 \times 10^{-5}$	a			$6,44 \times 10^{-6}$	b	$4,53 \times 10^{-6}$	b	$2,81 \times 10^{-6}$	c	$1,18 \times 10^{-6}$	c		
12	$9,51 \times 10^{-6}$	b			$5,84 \times 10^{-6}$	b	$4,04 \times 10^{-6}$	b	$2,49 \times 10^{-6}$	c	$1,04 \times 10^{-6}$	c		
13	$8,78 \times 10^{-6}$	b			$5,33 \times 10^{-6}$	b	$3,64 \times 10^{-6}$	b	$2,23 \times 10^{-6}$	c	$9,21 \times 10^{-7}$	d		
15	$7,61 \times 10^{-6}$	b			$4,53 \times 10^{-6}$	b	$3,01 \times 10^{-6}$	b	$1,82 \times 10^{-6}$	c	$7,44 \times 10^{-7}$	d		
16	$7,13 \times 10^{-6}$	b			$4,21 \times 10^{-6}$	b	$2,77 \times 10^{-6}$	c	$1,67 \times 10^{-6}$	c	$6,76 \times 10^{-7}$	d		
18	$6,34 \times 10^{-6}$	b			$3,68 \times 10^{-6}$	b	$2,37 \times 10^{-6}$	c	$1,41 \times 10^{-6}$	c	$5,67 \times 10^{-7}$	d		
20	$5,71 \times 10^{-6}$	b			$3,26 \times 10^{-6}$	b	$2,06 \times 10^{-6}$	c	$1,22 \times 10^{-6}$	c	$4,85 \times 10^{-7}$	d		
22	$5,19 \times 10^{-6}$	b			$2,93 \times 10^{-6}$	c	$1,82 \times 10^{-6}$	c	$1,07 \times 10^{-6}$	c	$4,21 \times 10^{-7}$	d		
24	$4,76 \times 10^{-6}$	b			$2,65 \times 10^{-6}$	c	$1,62 \times 10^{-6}$	c	$9,47 \times 10^{-7}$	d	$3,70 \times 10^{-7}$	d		
27	$4,23 \times 10^{-6}$	b			$2,32 \times 10^{-6}$	c	$1,39 \times 10^{-6}$	c	$8,04 \times 10^{-7}$	d	$3,10 \times 10^{-7}$	d		
30			$3,80 \times 10^{-6}$	b	$2,06 \times 10^{-6}$	c	$1,21 \times 10^{-6}$	c	$6,94 \times 10^{-7}$	d	$2,65 \times 10^{-7}$	d	$9,54 \times 10^{-8}$	e
33			$3,46 \times 10^{-6}$	b	$1,85 \times 10^{-6}$	c	$1,06 \times 10^{-6}$	c	$5,94 \times 10^{-7}$	d	$2,30 \times 10^{-7}$	d	$8,57 \times 10^{-8}$	e
36			$3,17 \times 10^{-6}$	b	$1,67 \times 10^{-6}$	c	$9,39 \times 10^{-7}$	d	$5,16 \times 10^{-7}$	d	$2,01 \times 10^{-7}$	d	$7,77 \times 10^{-8}$	e
39			$2,93 \times 10^{-6}$	c	$1,53 \times 10^{-6}$	c	$8,40 \times 10^{-7}$	d	$4,53 \times 10^{-7}$	d	$1,78 \times 10^{-7}$	d	$7,11 \times 10^{-8}$	e
43			$2,65 \times 10^{-6}$	c	$1,37 \times 10^{-6}$	c	$7,34 \times 10^{-7}$	d	$3,87 \times 10^{-7}$	d	$1,54 \times 10^{-7}$	d	$6,37 \times 10^{-8}$	e
47			$2,43 \times 10^{-6}$	c	$1,24 \times 10^{-6}$	c	$6,49 \times 10^{-7}$	d	$3,35 \times 10^{-7}$	d	$1,34 \times 10^{-7}$	d	$5,76 \times 10^{-8}$	e
51			$2,24 \times 10^{-6}$	c	$1,13 \times 10^{-6}$	c	$5,80 \times 10^{-7}$	d	$2,93 \times 10^{-7}$	d	$1,19 \times 10^{-7}$	d	$5,26 \times 10^{-8}$	e
56			$2,04 \times 10^{-6}$	c	$1,02 \times 10^{-6}$	c	$5,10 \times 10^{-7}$	d	$2,52 \times 10^{-7}$	d	$1,03 \times 10^{-7}$	d	$4,73 \times 10^{-8}$	e
62			$1,84 \times 10^{-6}$	c	$9,06 \times 10^{-7}$	d	$4,43 \times 10^{-7}$	d	$2,13 \times 10^{-7}$	d	$8,84 \times 10^{-8}$	e	$4,22 \times 10^{-8}$	e
68			$1,68 \times 10^{-6}$	c	$8,17 \times 10^{-7}$	d	$3,90 \times 10^{-7}$	d	$1,84 \times 10^{-7}$	d	$7,68 \times 10^{-8}$	e	$3,80 \times 10^{-8}$	e
75			$1,52 \times 10^{-6}$	c	$7,31 \times 10^{-7}$	d	$3,40 \times 10^{-7}$	d	$1,57 \times 10^{-7}$	d	$6,62 \times 10^{-8}$	e	$3,41 \times 10^{-8}$	e
82			$1,39 \times 10^{-6}$	c	$6,61 \times 10^{-7}$	d	$3,01 \times 10^{-7}$	d	$1,35 \times 10^{-7}$	d	$5,79 \times 10^{-8}$	e	$3,08 \times 10^{-8}$	e
91			$1,25 \times 10^{-6}$	c	$5,88 \times 10^{-7}$	d	$2,61 \times 10^{-7}$	d	$1,14 \times 10^{-7}$	d	$4,94 \times 10^{-8}$	e	$2,74 \times 10^{-8}$	e
100			$1,14 \times 10^{-6}$	c	$5,28 \times 10^{-7}$	d	$2,29 \times 10^{-7}$	d	$1,01 \times 10^{-7}$	d	$4,29 \times 10^{-8}$	e	$2,47 \times 10^{-8}$	e

APPENDIX 2

MTTFd (y) = PFHd (per hour) [Cat 4; DC=high]			
$100 = 2{,}47 \times 10^{-8}$	$240 = 9{,}81 \times 10^{-9}$	$560 = 4{,}11 \times 10^{-9}$	$1.300 = 1{,}75 \times 10^{-9}$
$110 = 2{,}23 \times 10^{-8}$	$270 = 8{,}67 \times 10^{-9}$	$620 = 3{,}70 \times 10^{-9}$	$1.500 = 1{,}51 \times 10^{-9}$
$120 = 2{,}03 \times 10^{-8}$	$300 = 7{,}76 \times 10^{-9}$	$680 = 3{,}37 \times 10^{-9}$	$1.600 = 1{,}42 \times 10^{-9}$
$130 = 1{,}87 \times 10^{-8}$	$330 = 7{,}04 \times 10^{-9}$	$750 = 3{,}05 \times 10^{-9}$	$1.800 = 1{,}26 \times 10^{-9}$
$150 = 1{,}61 \times 10^{-8}$	$360 = 6{,}44 \times 10^{-9}$	$820 = 2{,}79 \times 10^{-9}$	$2.000 = 1{,}13 \times 10^{-9}$
$160 = 1{,}50 \times 10^{-8}$	$390 = 5{,}94 \times 10^{-9}$	$910 = 2{,}51 \times 10^{-9}$	$2.200 = 1{,}03 \times 10^{-9}$
$180 = 1{,}33 \times 10^{-8}$	$430 = 5{,}38 \times 10^{-9}$	$1.000 = 2{,}27 \times 10^{-9}$	$2.300 = 9{,}85 \times 10^{-10}$
$200 = 1{,}19 \times 10^{-8}$	$470 = 4{,}91 \times 10^{-9}$	$1.100 = 2{,}07 \times 10^{-9}$	$2.400 = 9{,}44 \times 10^{-10}$
$220 = 1{,}08 \times 10^{-8}$	$510 = 4{,}52 \times 10^{-9}$	$1.200 = 1{,}90 \times 10^{-9}$	$2.500 = 9{,}06 \times 10^{-10}$

APPENDIX 3

SISTEMA - Safety Integrity Software Tool for the Evaluation of Machine Applications

Project name: Valio Ltd, edible fat factories robotic cells

File date: 03/04/2014 Report date: 03/04/2014 Checksum: cf16603e4a3c815016db4252afba168b

PR Project name: Valio Ltd, edible fat factories robotic cells

Author:	Erkki Ojalehto
Dangerous point/machine:	Service door
Documentation:	Bachelo's thesis Safety device upgrade for robotic cell Verification calculation about achieved performance level for robotic cell's service door.
Document:	
File name:	C:\Users\Simo\Documents\SISTEMA\Projects\Rasvatehtaan robottisolut.ssm
Version of software:	1.1.6
Version of standard:	ISO 13849-1:2006, ISO 13849-1/Cor1:2009, EN ISO 13849-1:2006, EN ISO 13849-1:2008
Checksum:	cf16603e4a3c815016db4252afba168b
Options:	☑ Use DC intermediate levels for calculation of PFH (more precise) ☐ Raise the MTTFd-capping for Category 4 from 100 to 2500 years
Status:	green
Note:	There are no warnings listed for this project (or it's subordinate basic elements).

Contained safety functions

SF Name: Service door

Required: PLr d	Reached: PL d	PFH [1/h]: 1.05E-7	Status: green

SISTEMA - Safety Integrity Software Tool for the Evaluation of Machine Applications

Project name: Valio Ltd, edible fat factories robotic cells

File date: 03/04/2014 Report date: 03/04/2014 Checksum: cf16603e4a3c815016db4252afba168b

SF Safety function: Service door

Safety function type:	Safety-related stop function initiated by safeguard
Triggering event:	Service door's latche's movement sideways, then safety switche's (Siemens) actuator key moves out of it's position OR / AND service door pulled 2 cm out of closed position, then safety sensor (RSS 36) and its pair diverges from each other.
Reaction:	Two normaly closed contacts of Siemens safety switche's open OR/AND Schmersal pair of actuators (RSS 36) diverge from each other. Safety switch's and sensor's data is transfered via AS-i and PROFIbus fieldbusses' to fail-safe CPU. With the safety switche's data, fail-safe CPU deactivate TESYS contactors via Profibus fieldbus, fail-safe output module and safety relay.
Safe state:	Robots power supply contactors not activated.
Documentation:	AS-i / DP F-Links function is be a link between the AS-i and the Profibus. Data transfer between fail-safe CPU and TESYS contactors is executed with Fail-safe output module and Profibus. Safety relay is needed for activating the power supply contactors.
Document:	
Reached PL:	d PFH [1/h]: 1.05E-7
PLr (by direct input):	d
Documentation/reasoning:	Described in robot standard: Performance requirement Safety-related parts of control systems shall be designed so that they comply with PL=d with structure category 3 as described in ISO 13849-1:2006, or so that they comply with SIL 2 with hardware fault tolerance of 1 with a proof test interval of not less than 20 years as described in IEC 62061:2005.
Source (e.g. standard):	SFS-EN ISO 10218-2 Part 5.2.2
File:	
Status:	green

Subsystems:

SB Name: Siemens fail-safe CPU

PL: e	PFH [1/h]: 4E-9
Cat.: 4	Mission time [a]: 20

Documentation Subsystem

Documentation:	From Siemens_Data document: Page 7/21 Type: CPU 319F 3PN/DP Order number: 6ES7318-3FL00-0AB0 SIL: SIL 3 PL: PL e PFHD: 4.00E-9 Lifetime: 20 years

SISTEMA - Safety Integrity Software Tool for the Evaluation of Machine Applications

Project name: Valio Ltd, edible fat factories robotic cells

File date: 03/04/2014 Report date: 03/04/2014 Checksum: cf16603e4a3c815016db4252afba168b

SF Safety function: Service door

Document:	..\Siemens_Data.pdf

Performance Level Subsystem

Documentation/reasoning:	

Category Subsystem

Documentation/reasoning:	
Source (e.g. standard) Category:	
File:	
Requirements of the Category:	Since the category is given by the manufacturer he is responsible to satisfy the requirements.

Status / Messages Subsystem

Status:	green

Subsystems:

SB Name: Siemens DP / AS-i F-Link

PL: e	PFH [1/h]: 3E-9
Cat.: 4	Mission time [a]: 20

Documentation Subsystem

Documentation:	From Siemens_Data document: Page 4/23 Product: DP/AS-I F-LINK Gateway Order number: 3RK3141-.CD10 SIL: SIL 3 PL: PL e PFHD: 3.00E-9 Lifetime: 20 years
Document:	..\Siemens_Data.pdf

Performance Level Subsystem

Documentation/reasoning:	

Category Subsystem

Documentation/reasoning:	
Source (e.g. standard) Category:	
File:	
Requirements of the Category:	Since the category is given by the manufacturer he is responsible to satisfy the requirements.

SISTEMA - Safety Integrity Software Tool for the Evaluation of Machine Applications

Project name: Valio Ltd, edible fat factories robotic cells

File date: 03/04/2014 Report date: 03/04/2014 Checksum: cf16603e4a3c815016db4252afba168b

SF Safety function: Service door

Status / Messages Subsystem

Status:	green

Subsystems:

SB Name: Safety position switch

PL: e	PFH [1/h]: 4.29E-8
Cat.: 3	Mission time [a]: 20
DCavg [%]: 90 (Medium)	CCF Points: 70 (fulfilled)
MTTFd [a]: 100 (High)	

Documentation Subsystem

Documentation:

From Siemens_Data.pdf document:
Page 18/21:

Product: Safety position switch with separate actuator.
Ordernumber: 3SF1... -..V..
B10 value: 1 000 000
Ration of dangerous failures: 20%
The maxinum useful lifetime: 20 year

Calculations:
The mostly used service door chosen. The Service door is opened aproximately 20 times per day.

B10d = B10 / ratio of dangerous failures = 1 000 000 / 20% = 5 000 000
h_op = 15h
d_op = 330d
t_cycle = (15h x 60min x 60s) / 20 = 2700s
Nop = (d_op x h_op x 3600 s/h) / t_cycle = (330d x 15h x 3600s/h) / 2700s = 6600
MTTFd = B10d / (0,1 x n_op) = 5000000 / (0,1 x 6600) = 7575,76 years

Document: ..\Siemens_Data.pdf

Category Subsystem

Documentation/reasoning:	Single channel mechanics. (Actuator key)
Source (e.g. standard) Category:	
File:	
Requirements of the Category:	Basic safety principles are being used. [fulfilled] Well-tried safety principles are being used. [fulfilled] A single fault tolerance is given. [fulfilled] MTTFd is Low or Medium or High. [fulfilled]

SF Safety function: Service door

	DCavg is Low or Medium. [fulfilled]
	The achieved score of the CCF-rating is at least 65. [fulfilled]

Common cause failure Subsystem

CCF Measures:	Design / application / experience (5 Points) Components used are well-tried Design / application / experience (15 Points) Protection against over-voltage, over-pressure, over-current, etc. Separation / Segregation (15 Points) Physical separation between signal paths: separation in wiring / piping, sufficient clearances and creep age distances on printed-circuit boards. Environmental (10 Points) Other influences. Have the requirements for immunity to all relevant environmental influneces such as temperature, shock, vibration, humidity (e.g. as specified in relevant standards) been considered? Environmental (25 Points) Prevention of contamination and electromagnetic compatibility (EMC) against CCF in accordance with appropriate standards. Fluidic systems: filtration of the pressure medium, prevention of dirt intake, drainage of compressed air, e.g. in compliance with the component manufacturers requirements concerning purity of the pressure medium. Electric systems: Has the system been checked for electromagnetic immunity, e.g. as specified in relevant standards against CCF? For combined fluidic and electric systems, both aspects should be considered.

Status / Messages Subsystem

Status:	green
Message [Status of Message]:	The subsystem MTTFd has been cut from originally 7576 to 100 a. For a subsystem 100 a is the maximum acceptable mean time to a dangerous failure. [green]

Channels / Test channels:

CH Name: Channel 1

Blocks:

BL Name: **Normal Closet contact 1**

DC [%]: 90 (Medium)

Mission time [a]: 20

Documentation Block

Documentation:

SF **Safety function: Service door**

Document:

Diagnostic coverage Block

Measure: Cyclic test stimulus by dynamic change of the input signals (Input devices) (90 %)

Status / Messages Block

Status: green

Channels / Test channels:

CH Name: Channel 2

Blocks:

BL Name: **Normal Closet contact 2**

DC [%]: 90 (Medium)

Mission time [a]: 20

Documentation Block

Documentation:

Document:

Diagnostic coverage Block

Measure: Cyclic test stimulus by dynamic change of the input signals (Input devices) (90 %)

Status / Messages Block

Status: green

Subsystems:

SB Name: RSS 36 ... AS-i safety sensor electronic (Kat 4/ PL e)

PL: e	PFH [1/h]: 5.13E-10
Cat.: 4	Mission time [a]: 20

Documentation Subsystem

Documentation: Safety sensor, electronic coded RFID, with integrated safety AS-interface.

Document: ..\RSS 36 AS-i.pdf

Performance Level Subsystem

Documentation/reasoning: manufacturer information

SF Safety function: Service door

Category Subsystem

Documentation/reasoning:	
Source (e.g. standard) Category:	
File:	
Requirements of the Category:	Since the category is given by the manufacturer he is responsible to satisfy the requirements.

Status / Messages Subsystem

Status:	green

Subsystems:

SB Name: Safety relay UE48-xOS (Release 2012-05)

PL: e	PFH [1/h]: 3E-8
Cat.: 4	Mission time [a]: 20

Documentation Subsystem

Documentation:	Subject to errors and technical modifications. Only the data in the operating instruction of the respective product are binding. The data applies to the following product famillies: UE48-2OS UE48-3OS
Document:	

Performance Level Subsystem

Documentation/reasoning:	The value is valid until 8760 cycles per year (max load). Calculated usage: The Service door is opened aproximately 20 times per day. The robot is in use 330 days a year. 330 x 20 = 6600 6600 < 8760 = OK

Category Subsystem

Documentation/reasoning:	
Source (e.g. standard) Category:	
File:	
Requirements of the Category:	Since the category is given by the manufacturer he is responsible to satisfy the requirements.

SISTEMA - Safety Integrity Software Tool for the Evaluation of Machine Applications

Project name: Valio Ltd, edible fat factories robotic cells

File date: 03/04/2014 Report date: 03/04/2014 Checksum: cf16603e4a3c815016db4252afba168b

SF Safety function: Service door

Status / Messages Subsystem

Status:	green

Subsystems:

SB Name: Robots power supply

PL: e	PFH [1/h]: 2.47E-8
Cat.: 4	Mission time [a]: 20
DCavg [%]: 99 (High)	CCF Points: 75 (fulfilled)
MTTFd [a]: 100 (High)	

Documentation Subsystem

Documentation:	Robot's power feed is implemented with two contactors wired series. System monitors status of both contactors with auxiliary contacts of contactors'.
Document:	

Category Subsystem

Documentation/reasoning:	
Source (e.g. standard) Category:	
File:	
Requirements of the Category:	Basic safety principles are being used. [fulfilled] Well-tried safety principles are being used. [fulfilled] A single fault tolerance is given. [fulfilled] Accumulation of faults does not lead to a loss of the safety funciton. [fulfilled] MTTFd is High. [fulfilled] DCavg is High. [fulfilled] The achieved score of the CCF-rating is at least 65. [fulfilled]

Common cause failure Subsystem

CCF Measures:	Separation / Segregation (15 Points) Physical separation between signal paths: separation in wiring / piping, sufficient clearances and creep age distances on printed-circuit boards. Design / application / experience (15 Points) Protection against over-voltage, over-pressure, over-current, etc. Design / application / experience (5 Points) Components used are well-tried

SF Safety function: Service door

Competence / training (5 Points)
Have designers / maintainers been trained to understand the causes and consequences of common cause failures?

Environmental (25 Points)
Prevention of contamination and electromagnetic compatibility (EMC) against CCF in accordance with appropriate standards. Fluidic systems: filtration of the pressure medium, prevention of dirt intake, drainage of compressed air, e.g. in compliance with the component manufacturers requirements concerning purity of the pressure medium. Electric systems: Has the system been checked for electromagnetic immunity, e.g. as specified in relevant standards against CCF? For combined fluidic and electric systems, both aspects should be considered.

Environmental (10 Points)
Other influences. Have the requirements for immunity to all relevant environmental influneces such as temperature, shock, vibration, humidity (e.g. as specified in relevant standards) been considered?

Status / Messages Subsystem

Status: green

Channels / Test channels:

CH Name: Channel 1

MTTFd [a]: 2075.55

Blocks:

BL Name: **TESYS Contactor (nominal load)**

MTTFd [a]: 2075.55 (High) DC [%]: 99 (High)

Mission time [a]: 20

Documentation Block

Documentation:

The MTTFd value will be calculated depending on the number of operations per year.

Subject to change- please refer always to the data in the instruction sheet.
The information provided in this documentation contains general descriptions and/or technical characteristics of the performance of the products contained herein.
This documentation is not intended as a substitute for and is not to be used for determining suitability or reliability of these products for specific user applications.
It is the duty of any such user or integrator to perform the appropriate and complete risk analysis, evaluation and testing of the products with respect to the relevant specific application or use thereof. Neither Schneider Electric Industries SAS nor any of its affiliates or subsidiaries shall be responsible or liable for misuse of the information contained herein.

Document:

SISTEMA - Safety Integrity Software Tool for the Evaluation of Machine Applications

Project name: Valio Ltd, edible fat factories robotic cells

File date: 03/04/2014 Report date: 03/04/2014 Checksum: cf16603e4a3c815016db4252afba168b

SF Safety function: Service door

Status / Messages Block

Status:	green

Elements:

EL Name: **Contactor TESYS (nominal load)**

B10d [cycles]: 1369863	nop [cycles/a]: 6600
T10d [a]: 207.56	MTTFd [a] (from B10d): 2075.55 (High)
Mission time [a]: 20	
	DC [%]: 99 (High)

Documentation Element

Technology:	electromechanic
Documentation:	TeSys contactor with nominal load. B10 = 1 000 000, % of dangerous failures = 73%, B10d = 1 369 863 The MTTFd value will be calculated depending on the number of operations per year. In a 2-channel assembly and connected to the feedback loop (EDM) of a monitoring device applicable up to PL=e.
Document:	

Diagnostic coverage Element

Documentation/reasoning:	When an NC contact is connected to the feedback loop of a monitoring device (EDM) the DC=99%

Status / Messages Element

Status:	green
Message [Status of Message]:	

Channels / Test channels:

CH Name: Channel 2

MTTFd [a]: 2075.55

Blocks:

BL Name: **TESYS Contactor (nominal load)**

MTTFd [a]: 2075.55 (High)	DC [%]: 99 (High)
	Mission time [a]: 20

Documentation Block

Documentation:	The MTTFd value will be calculated depending on the number of operations per year. Subject to change- please refer always to the data in the

SF Safety function: Service door

instruction sheet.
The information provided in this documentation contains general descriptions and/or technical characteristics of the performance of the products contained herein.
This documentation is not intended as a substitute for and is not to be used for determining suitability or reliability of these products for specific user applications.
It is the duty of any such user or integrator to perform the appropriate and complete risk analysis, evaluation and testing of the products with respect to the relevant specific application or use thereof. Neither Schneider Electric Industries SAS nor any of its affiliates or subsidiaries shall be responsible or liable for misuse of the information contained herein.

Document:

Status / Messages Block

Status: green

Elements:

EL Name: **Contactor TESYS (nominal load)**

B10d [cycles]: 1369863 nop [cycles/a]: 6600

T10d [a]: 207.56 MTTFd [a] (from B10d): 2075.55 (High)

Mission time [a]: 20

DC [%]: 99 (High)

Documentation Element

Technology:	electromechanic
Documentation:	TeSys contactor with nominal load. B10 = 1 000 000, % of dangerous failures = 73%, B10d = 1 369 863 The MTTFd value will be calculated depending on the number of operations per year. In a 2-channel assembly and connected to the feedback loop (EDM) of a monitoring device applicable up to PL=e.
Document:	

Diagnostic coverage Element

Documentation/reasoning: When an NC contact is connected to the feedback loop of a monitoring device (EDM) the DC=99%

Status / Messages Element

Status: green

Message [Status of Message]:

SISTEMA - Safety Integrity Software Tool for the Evaluation of Machine Applications

Project name: Valio Ltd, edible fat factories robotic cells

File date: 03/04/2014 Report date: 03/04/2014 Checksum: cf16603e4a3c815016db4252afba168b

SF Safety function: Service door

Subsystems:

SB Name: Fail-safe output module. (Siemens)

PL: e	PFH [1/h]: 1E-10
Cat.: 4	Mission time [a]: 20

Documentation Subsystem

Documentation:	From Siemens_Data document: Page 4/18 Product: EM138 4 F-DO Order number: 6ES7138-4FB02-0AB0 SIL: SIL 3 PL PL e PFHD 1.00E-10 Lifetime 20 years
Document:	..\Siemens_Data.pdf

Performance Level Subsystem

Documentation/reasoning:

Category Subsystem

Documentation/reasoning:	
Source (e.g. standard) Category:	
File:	
Requirements of the Category:	Since the category is given by the manufacturer he is responsible to satisfy the requirements.

Status / Messages Subsystem

Status:	green

EXCLUSION OF LIABILITY

Care has been taken in production of the software SISTEMA, which corresponds to the state of the art. It is made available to users free of charge.

Use of the software is at the user's own risk. To the extent permissible by law, no liability will be accepted for the software on any legal basis. In particular, no liability will be accepted for material defects or defects in title, whether in the software or in the associated documentation and information, particularly with regard to their correctness, freedom from errors, freedom from property rights and copyright of third parties, up-to-dateness, completeness and/or fitness for purpose, except in cases of malicious or wrongful intent.

The IFA undertakes to keep its website free of viruses; nevertheless, no guarantee can be given that the software and information provided are virus-free. The user is therefore advised to take appropriate security precautions and to use a virus scanner prior to downloading software, documentation or information.

CONTACT

Institute for Occupational Health and Safety of German Social Accident Insurance (IFA)

Division 5: Accident Prevention / Product Safety

Alte Heerstr. 111, 53757 Sankt Augustin

E-mail: sistema@dguv.de

www.dguv.de/ifa (Webcode e20543)

Date, signature of the revisor

Date, signature of the author