PR Project name: AKINROBOTICS UV-C STERILIZASYON ROBOTU - ISO 13849-1 PL Analysis

Project file name:	C:\Users\ekera\Desktop\Work\SISTEMA Docs\Projects\AKIN ROBOTICS .ssm
Creation date:	27.10.2020 12:47:11
Project status:	Completed
Project number:	LVD-633-02
Project version:	---
Authors:	Anil EKER
Project managers:	Timur GÜSER
Inspectors:	Yüksel YILDIZ
Dangerous point/machine:	Moving and operating without human control
Documentation:	This machine moves automatically or remote control. UV lighting over the machine provides cleaning of air and surfaces in the room. The machine is intended to be used in human restricted areas. Thus, human presense is not expected during normal operation. -Human or object sense in front of the moving direction of the robot while in automatic mode (No human control over the machine) (This analysis cannot be performed due to data absence of Lidar and depth sense camera). -Emergency Stop -Overheating For "Emergency Stop" and "Overtemperature Control" functions, PLr is decided as b in risk graph. Both functions conform PL b level.
Document:	
Version of software:	2.0.8 build 4
Version of standard:	ISO 13849-1:2015, ISO 13849-2:2012
Checksum:	ab9822f6a047d19a9cdc51b8863c770b
Options:	☑ Use DC intermediate levels for calculation of PFHD (more precise) ☐ MTTFD capping for category 4 lower from 2500 to 100 years.
Status:	green
Note:	There are no warnings listed for this project (or it's subordinate basic elements).

Print options

- ☑ Show device details
- ☑ Show documentations on SF, SB, BL and EL
- ☑ Show CCF and DC measures in detail
- ☑ Show requirements on PL and Category
- ☑ Show parameter documentations on PLr, PL, Category, CCF, MTTFD and DC
- ☐ Show messages

Contained safety functions

SF Name: Emergency Stop Function [Pressing to emergency button]

Required: PLr b	Reached: PL b	PFHD [1/h]: 5,3E-6	Status: green

SF Name: Overtemperature Control

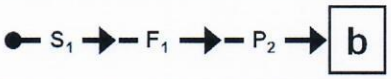
PR Project name: AKINROBOTICS UV-C STERILIZASYON ROBOTU - ISO 13849-1 PL Analysis

Required: PLr b	Reached: PL b	PFHD [1/h]: 5,1E-6	Status: green

SF Safety function: Emergency Stop Function

Identifier of the Safety function:	Pressing to emergency button
Safety function type:	Emergency stop function
Triggering event:	Pressing to emergency button
Reaction and Behaviour on power failure:	The mechine stops in power failure.
Safe state:	Stopping of motion and UV light.
Operation mode:	---
Demand rate:	Once in 2 hours (Assumption)
Running-on time:	---
Priority:	---
Documentation:	The manufacturer informed that machine software have self testing and validation features with redundant test modules. Thus, category 2 is chosen for this subsystem.
Document:	

Required Performance Level Safety function

PLr (by risk graph):	b
Severity of injury (S): True	Slight (normally reversible) injury
Frequency / exposure times to hazard (F):	Seldom to less often / exposure time is short
Possibility of avoiding (P):	Scarcely possible
Risk graph:	

Documentation:	
Document:	

Performance Level Safety function

Reached PL: b **PFHD [1/h]: 5,3E-6**

Status / Messages Safety function

Status:	green

Subsystems (1 / 1)

SB Name: Emergency stop

Reference designator: Unknown **Inventory number: N/A**

Device details Subsystem

Device Manufacturer:	Unknown
Device Identifier:	Unknown
Device group:	Unknown
Part number:	**Revision:**

SF Safety function: Emergency Stop Function

Function:	☑ Input ☑ Logic ☐ Output ☐ unknown
Use case:	The manufacturer shall change the emergency stop button with an approved equivalent one. Further analysis done according to assupmtion of approved emergency button. Otherwise, this analysis is not valid.
Description of the use case:	

Documentation Subsystem

Documentation:	
Document:	

Performance Level Subsystem

PL determination:	Determine PL/PFHD from Category, MTTFD and DCavg
Software suitable up to PL:	b
PL requirements:	fulfilled
The PL shall be determined by the estimation of the following aspects:	- Behaviour of the safety function under fault conditions (see clause 6) [fulfilled] - safety-related software according to clause 4.6 or no software included [fulfilled] - systematic failure (see Annex G) [fulfilled] - Ability to perform a safety function under expected environmental conditions [fulfilled]
Reached PL: b	**PFHD [1/h]: 5,3E-6**
Documentation:	

Category Subsystem

Cat.:	2
Category requirements:	fulfilled
Requirements of the Category:	- Accordance with relevant standards to withstand the expected influences. [fulfilled] - Basic safety principles are being used. [fulfilled] - Well-tried safety principles are being used. [fulfilled] - The requirements for the test frequency are satisfied. [fulfilled] - MTTFD is at least Low or Medium or High. [fulfilled] - DCavg is at least Low or Medium; [fulfilled] - The MTTFD of the test channel is greater than or equals half of the tested systems MTTFD. [fulfilled] - The achieved score of the CCF-rating is at least 65. [fulfilled]
Documentation:	
Source (e.g. standard) Category:	
File:	

MTTFD and Mission time Subsystem

SF Safety function: Emergency Stop Function

MTTFD [a]:	9,7 (Low)
Mission time [a]: 20	**Shortest mission time [a]: 20**

Diagnostic coverage Subsystem

DCavg [%]:	90 (Medium)

Common cause failure Subsystem

CCF Points:	90 (fulfilled)
CCF Measures:	- Separation / Segregation (15 Points) Physical separation between signal paths, for example: — separation in wiring/piping; — detection of short circuits and open circuits in cables by dynamic test; — separate shielding for the signal path of each channel; — sufficient clearances and creepage distances on printed-circuit boards. - Diversity (20 Points) Different technologies/design or physical principles are used, for example: — first channel electronic or programmable electronic and second channel electromechanical hardwired, — different initiation of safety function for each channel (e.g. position, pressure, temperature), and/or digital and analog measurement of variables (e.g. distance, pressure or temperature) and/or Components of different manufactures. - Design / application / experience (15 Points) Protection against over-voltage, over-pressure, over-current, over-temperature, etc. - Design / application / experience (5 Points) Components used are well-tried. - Environmental (25 Points) For electrical/electronic systems, prevention of contamination and electromagnetic disturbances (EMC) to protect against common cause failures in accordance with appropriate standards (e.g. IEC 61326–3-1). 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. NOTE For combined fluidic and electric systems, both aspects should be considered. - Environmental (10 Points) Other influences Consideration of the requirements for immunity to all relevant environmental influences such

SF Safety function: Emergency Stop Function

CCF Measures:	as, temperature, shock, vibration, humidity (e.g. as specified in relevant standards).
Documentation:	
Document:	

Status / Messages Subsystem

Status:	green

Channels / Test channels (1 / 2)

CH Name: Channel 1

MTTFD [a]: 9,7

Blocks (1 / 2)

BL Name: Stop button

Reference designator:		**Inventory number:**	

Device details Block

Device Manufacturer:	---		
Device Identifier:	---		
Device group:	---		
Part number: ---		**Revision: ---**	
Function:	☑ Input ☐ Output	☐ Logic ☐ unknown	
Technology:	electromechanic		
Category:	B		
Use case:	The manufacturer shall change the emergency stop button with an approved equivalent one. Further analysis done according to assupmtion of approved emergency button. Otherwise, this analysis is not valid.		
Description of the use case:			

Documentation Block

Documentation:	
Document:	

MTTFD and Mission time Block

MTTFD [a]: 342,5 (High)			
Mission time [a]: 20		**Shortest mission time [a]: 20**	
B10D [cycles]: 100000		**nop [cycles/a]: 2920**	
Nop parameter:	**Days: 365**	**Hours: 16**	**Seconds: 7200**
Documentation:	Typical component values stated in ISO EN 13849-1 are considered.		

SF Safety function: Emergency Stop Function

Diagnostic coverage Block

DC [%]: 90 (Medium)

Measure:	Temporal and logical monitoring of the logic by the watchdog, where the test equipment does plausibility checks of the behaviour of the logic (Logic) (90 %)
Documentation:	

Status / Messages Block

Status:	green

Blocks (2 / 2)

BL Name: EKLEM KONTROL-SÜRÜCÜ STM32G473CET6 RS485

Reference designator: ST **Inventory number: STM32G473CET6**

Device details Block

Device Manufacturer:	ST
Device Identifier:	ST
Device group:	
Part number: STM32G473CET6	**Revision: ---**
Function:	☐ Input ☐ Output ☑ Logic ☐ unknown
Technology:	electronic
Category:	2
Use case:	STM32G473CET6 PIC is used in control board. For MTTFd value of the PIC, data available on the net is used as approxiamately 15 years. For total MTTFd value, resistors, capacitors, diodes etc. are all considered.
Description of the use case:	

Documentation Block

Documentation:	
Document:	

MTTFD and Mission time Block

MTTFD [a]: 10 (Medium)

Mission time [a]: 20 **Shortest mission time [a]: 20**

Rate of dangerous failure [FIT]: 11415,5

Documentation:	STM32G473CET6 PIC is used in control board. For MTTFd value of the PIC, data available on the net is used as approxiamately 15 years. For total MTTFd value, resistors, capacitors, diodes etc. are all considered. Typical MTTFd

SF Safety function: Emergency Stop Function

Documentation:	values of electronic components are obtained from ISO EN 13849-1. 37 capacitor carbon 7 capacitor tantalum 51 resistors 11 general ICs 6 transistors 27 diodes 1 STM32G4

Diagnostic coverage Block

DC [%]: 90 (Medium)

Measure:	Temporal and logical monitoring of the logic by the watchdog, where the test equipment does plausibility checks of the behaviour of the logic (Logic) (90 %)
Documentation:	

Status / Messages Block

Status:	green

Channels / Test channels (3 / 2)

TE Name: Test channel

MTTFD [a]: 10

Blocks (1 / 1)

BL Name: EKLEM KONTROL-SÜRÜCÜ STM32G473CET6 RS485

Reference designator: ST **Inventory number: STM32G473CET6**

Device details Block

Device Manufacturer:	ST	
Device Identifier:		
Device group:		
Part number: STM32G473CET6	**Revision:**	
Function:	☐ Input ☐ Output	☑ Logic ☐ unknown
Technology:	electronic	
Category:	2	
Use case:		
Description of the use case:		

Documentation Block

Documentation:

SF Safety function: Emergency Stop Function

Document:

MTTFD and Mission time Block

MTTFD [a]: 10 (Medium)

Mission time [a]: 20 **Shortest mission time [a]: 20**

Rate of dangerous failure [FIT]: 11415,5

Documentation:

STM32G473CET6 PIC is used in control board. For MTTFd value of the PIC, data available on the net is used as approxiamately 15 years. For total MTTFd value, resistors, capacitors, diodes etc. are all considered. Typical MTTFd values of electronic components are obtained from ISO EN 13849-1.

37 capacitor carbon
7 capacitor tantalum
51 resistors
11 general ICs
6 transistors
27 diodes
1 STM32G4

Status / Messages Block

Status: green

SF Safety function: Overtemperature Control

Identifier of the Safety function:	
Safety function type:	Monitoring of safety–related parameters
Triggering event:	Overtemperature
Reaction and Behaviour on power failure:	
Safe state:	Stopping of the machine (No UV light, no motion).
Operation mode:	
Demand rate:	
Running-on time:	
Priority:	
Documentation:	
Document:	

Required Performance Level Safety function

PLr (by risk graph):	b
Severity of injury (S): True	Slight (normally reversible) injury
Frequency / exposure times to hazard (F):	Seldom to less often / exposure time is short
Possibility of avoiding (P):	Scarcely possible
Risk graph:	

Documentation:	
Document:	

Performance Level Safety function

Reached PL: b	PFHD [1/h]: 5,1E-6

Status / Messages Safety function

Status:	green

Subsystems (1 / 1)

SB Name: Overtemperature control with sensors and CPU

Reference designator:	Inventory number:

Device details Subsystem

Device Manufacturer:	
Device Identifier:	
Device group:	
Part number:	Revision:
Function:	☐ Input ☐ Output ☐ Logic ☑ unknown

SF Safety function: Overtemperature Control

Use case:	
Description of the use case:	

Documentation Subsystem

Documentation:	
Document:	

Performance Level Subsystem

PL determination:	Determine PL/PFHD from Category, MTTFD and DCavg
Software suitable up to PL:	b
PL requirements:	fulfilled
The PL shall be determined by the estimation of the following aspects:	- Behaviour of the safety function under fault conditions (see clause 6) [fulfilled] - safety-related software according to clause 4.6 or no software included [fulfilled] - systematic failure (see Annex G) [fulfilled] - Ability to perform a safety function under expected environmental conditions [fulfilled]

Reached PL: b	**PFHD [1/h]: 5,1E-6**
Documentation:	

Category Subsystem

Cat.:	2
Category requirements:	fulfilled
Requirements of the Category:	- Accordance with relevant standards to withstand the expected influences. [fulfilled] - Basic safety principles are being used. [fulfilled] - Well-tried safety principles are being used. [fulfilled] - The requirements for the test frequency are satisfied. [fulfilled] - MTTFD is at least Low or Medium or High. [fulfilled] - DCavg is at least Low or Medium; [fulfilled] - The MTTFD of the test channel is greater than or equals half of the tested systems MTTFD. [fulfilled] - The achieved score of the CCF-rating is at least 65. [fulfilled]
Documentation:	
Source (e.g. standard) Category:	
File:	

MTTFD and Mission time Subsystem

MTTFD [a]:	10 (Medium)
Mission time [a]: 20	**Shortest mission time [a]: 20**

Diagnostic coverage Subsystem

SF Safety function: Overtemperature Control

DCavg [%]:	90 (Medium)

Common cause failure Subsystem

CCF Points:	70 (fulfilled)
CCF Measures:	- Separation / Segregation (15 Points) Physical separation between signal paths, for example: — separation in wiring/piping; — detection of short circuits and open circuits in cables by dynamic test; — separate shielding for the signal path of each channel; — sufficient clearances and creepage distances on printed-circuit boards. - Design / application / experience (15 Points) Protection against over-voltage, over-pressure, over-current, over-temperature, etc. - Design / application / experience (5 Points) Components used are well-tried. - Environmental (25 Points) For electrical/electronic systems, prevention of contamination and electromagnetic disturbances (EMC) to protect against common cause failures in accordance with appropriate standards (e.g. IEC 61326–3-1). 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. NOTE For combined fluidic and electric systems, both aspects should be considered. - Environmental (10 Points) Other influences Consideration of the requirements for immunity to all relevant environmental influences such as, temperature, shock, vibration, humidity (e.g. as specified in relevant standards).
Documentation:	
Document:	

Status / Messages Subsystem

Status:	green

Channels / Test channels (1 / 2)

CH Name: Channel 1

MTTFD [a]: 10

Blocks (1 / 2)

BL Name: LM35DZ temp sensor

SF Safety function: Overtemperature Control

Reference designator: **Inventory number: LM35DZ**

Device details Block

Device Manufacturer:	Texas Instruments
Device Identifier:	LM35DZ
Device group:	
Part number: LM35DZ	**Revision:**
Function:	☑ Input ☐ Logic ☐ Output ☐ unknown
Technology:	electronic
Category:	B
Use case:	
Description of the use case:	

Documentation Block

Documentation:	
Document:	

MTTFD and Mission time Block

MTTFD [a]: 4,1E8 (High)

Mission time [a]: 20	**Shortest mission time [a]: 20**
MTBF [a]: 408000000	**RDF [%]: 100**
Documentation:	Gathered from component manufacturer's website.

Diagnostic coverage Block

DC [%]: 90 (Medium)

Measure:	Temporal and logical monitoring of the logic by the watchdog, where the test equipment does plausibility checks of the behaviour of the logic (Logic) (90 %)
Documentation:	

Status / Messages Block

Status:	green

Blocks (2 / 2)

BL Name: EKLEM KONTROL-SÜRÜCÜ STM32G473CET6 RS485

Reference designator: **Inventory number: STM32G473CET6**

Device details Block

Device Manufacturer:	ST

SF Safety function: Overtemperature Control

Device Identifier:	
Device group:	
Part number: STM32G473CET6	**Revision:**
Function:	☐ Input ☐ Output ☑ Logic ☐ unknown
Technology:	electronic
Category:	2
Use case:	STM32G473CET6 PIC is used in control board. For MTTFd value of the PIC, data available on the net is used as approxiamately 15 years. For total MTTFd value, resistors, capacitors, diodes etc. are all considered.
Description of the use case:	

Documentation Block

Documentation:	
Document:	

MTTFD and Mission time Block

MTTFD [a]: 10 (Medium)	
Mission time [a]: 20	**Shortest mission time [a]: 20**
Rate of dangerous failure [FIT]: 11415,5	
Documentation:	STM32G473CET6 PIC is used in control board. For MTTFd value of the PIC, data available on the net is used as approxiamately 15 years. For total MTTFd value, resistors, capacitors, diodes etc. are all considered. Typical MTTFd values of electronic components are obtained from ISO EN 13849-1. 37 capacitor carbon 7 capacitor tantalum 51 resistors 11 general ICs 6 transistors 27 diodes 1 STM32G4

Diagnostic coverage Block

DC [%]: 90 (Medium)	
Measure:	Temporal and logical monitoring of the logic by the watchdog, where the test equipment does plausibility checks of the behaviour of the logic (Logic) (90 %)
Documentation:	

Status / Messages Block

SF Safety function: Overtemperature Control

Status: green

Channels / Test channels (3 / 2)

TE Name: Test channel

MTTFD [a]: 10

Blocks (1 / 1)

BL Name: EKLEM KONTROL-SÜRÜCÜ STM32G473CET6 RS485

Reference designator: **Inventory number: STM32G473CET6**

Device details Block

Device Manufacturer: ST

Device Identifier:

Device group:

Part number: STM32G473CET6 **Revision:**

Function: ☐ Input ☐ Output ☑ Logic ☐ unknown

Technology: electronic

Category: 2

Use case: STM32G473CET6 PIC is used in control board. For MTTFd value of the PIC, data available on the net is used as approxiamately 15 years. For total MTTFd value, resistors, capacitors, diodes etc. are all considered.

Description of the use case:

Documentation Block

Documentation:

Document:

MTTFD and Mission time Block

MTTFD [a]: 10 (Medium)

Mission time [a]: 20 **Shortest mission time [a]: 20**

Rate of dangerous failure [FIT]: 11415,5

Documentation: STM32G473CET6 PIC is used in control board. For MTTFd value of the PIC, data available on the net is used as approxiamately 15 years. For total MTTFd value, resistors, capacitors, diodes etc. are all considered. Typical MTTFd values of electronic components are obtained from ISO EN 13849-1.

37 capacitor carbon
7 capacitor tantalum
51 resistors
11 general ICs
6 transistors

SF Safety function: Overtemperature Control

Documentation:	27 diodes 1 STM32G4

Status / Messages Block

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.

Die Software wurde gemäß dem Stand von Wissenschaft und Technik sorgfältig erstellt. Sie wird dem Nutzer unentgeltlich zur Verfügung gestellt.

Die Haftung des IFAs/ DGUV ist damit auf Vorsatz und grobe Fahrlässigkeit (§ 521 BGB) bzw. bei Sach- und Rechtsmängel auf arglistig verschwiegene Fehler beschränkt (523, 524 BGB).

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 e561582)

Name in block letters:	Date, signature: 11.11.2020
Authors Anıl EKER	Authors TIMUR GÜSER
Inspectors Yüksel Yıldız Yurtlu	Inspectors