

# SISTEMA – Safety of controls on machines



Project Speedy 500 all variants – 8014

File Date: 5/5/2015: Report date: 5/5/2015: Checksum: e5631223c2d17baefddd55aa16852a2d

---

## PR Project name: Speedy 500 all variants – 8014

---

Author:	Huber Jochen
Danger point / machine:	Processing area
Documentation:	
Document:	
File name:	C:\Users\huberj\AppData\Local\Temp\tmp5CCB.ssm
Version of the software:	1.1.6
Version of the standard:	ISO 13849-1:2006, ISO 13849-1/Cor1:2009, EN ISO 13849-1:2006, EN ISO 13849-1:2008
Checksum:	e5631223c2d17baefddd55aa16852a2d
Options:	<input checked="" type="checkbox"/> Use DC intermediate stages to calculate the PFH (more precisely) <input type="checkbox"/> Increase MTTFd cap for Category 4 from 100 to 2500 years
Status:	yellow
Please note:	For the project (or its subordinate basic elements), there are yellow status alerts on hand. Please note the information stored there.

### Included safety features

**SF** Name: All openable covers are secured with two switches.

The interconnection is built to be redundant and diverse.

Required: PLr d

Achieved: PL e

PFH [1/h]: 4.29E-8

Status: yellow

---

# SISTEMA – Safety of controls on machines



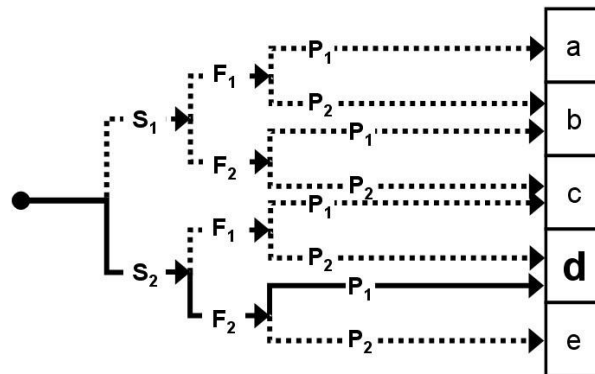
Project Speedy 500 all variants – 8014

File Date: 5/5/2015: Report date: 5/5/2015: Checksum: e5631223c2d17baefddd55aa16852a2d

**SF Safety function: All openable covers are secured with two switches.  
The interconnection is built to be redundant and diverse.**

Type of safety function:	Safety-related stop function, initiated by a protective device	
Triggering event:	Opening of a cover	
Reaction:	Switching off the power to the laser source and switching off the enable signal of the laser source.	
Safe condition:	The laser source produces no emissions.	
Documentation:	Usage, spatial, temporal, and other limits Combustion Processing area Commissioning, settings The laser beam can cause skin burns.	
Document:		
Achieved PL:	e	PFH [1/h]: 4.29E-8
PLr (by risk graph):	d	
Severity of injury (S):	Serious (usually irreversible) injury, including death	
Frequency / duration of exposure (F):	Frequent to permanent / long duration of exposure	
Possibility of avoidance (P):	Possible under certain conditions Risk	

graph:



Status: yellow

**Subsystems:**

**SB** Name: Interlock circuit

PL: e	PFH [1/h]: 4.29E-8
Cat.: 3	Service life [a]: 20
DCavg [%]: 90 (moderate)	CCF points: 95 (fulfilled)
MTTFd [a]: 100 (high)	
<i>Documentation subsystem</i>	
Documentation:	
Document:	



**SF Safety function: All openable covers are secured with two switches. The interconnection is built to be redundant and diverse.**

*Category subsystem*

Documentation / reason:

Source (e.g. norm) Category:

File:

- Requirements of the category: Basic safety principles are applied. [fulfilled]
- Proven safety principles are applied. [fulfilled]
- A one-error tolerance is given. [fulfilled]
- MTTFd is Low or Moderate or High. [fulfilled]
- DCavg is Low or Moderate. [fulfilled]
- The achieved score of the CCF rating is at least 65. [fulfilled]

*Common cause failure in subsystem*

- CCF measures: Separation / isolation (15 points)  
Physical separation between the signal paths, separation of wiring / tubing, sufficient clearance and creep distances on printed circuits.
- Diversity (20 points)  
Differing technologies / designs or physical principles are used, for example: the first channel in programmable electronics and the second channel hardwired, type of initiation, pressure, and temperature, measurement of distance and pressure, digital and analog. Components from various manufacturers.
- Design / application / experience (5 points)  
Use of tried and tested components
- Design / application / experience (15 points)  
Protection against overvoltage, overpressure, overcurrent, etc.
- Competence / education (5 points)  
Have designers / fitters been trained to understand the causes and effects of common cause failures?
- Environment (25 points)  
Protection against contamination and electromagnetic interference (EMC) against CCF in accordance with the appropriate standards.  
Fluidic systems: Filtration of the pressure medium, prevention of dirt entry, drainage of compressed air, e.g. in accordance with the manufacturer's requirements for the purity of the pressure medium, electrical systems: Has the system been tested for electromagnetic immunity, e.g. as specified in applicable standards against CCF? For combined fluidic and electrical systems, both aspects should be considered.

# SISTEMA – Safety of controls on machines



Project Speedy 500 all variants – 8014

File Date: 5/5/2015: Report date: 5/5/2015: Checksum: e5631223c2d17baefddd55aa16852a2d

**SF** Safety function: All openable covers are secured with two switches.  
The interconnection is built to be redundant and diverse.

Environment (10 points)  
Other influences. Have all requirements for insensitivity to all relevant environmental conditions such as temperature, shock, vibration, humidity (e.g. as defined in the applicable standards) been taken into account?

## Status / Notes Subsystem

Status: yellow

## Channels / Test Channel:

**CH** Name: Channel 1

MTTFd [a]: 103.68

### Blocks:

**BL** Name: Interlock circuit 1

MTTFd [a]: 103.68 (high)

DC [%]: 90 (moderate)

Service life [a]: 20

## Documentation block

Documentation:

Document:

## Status / Notes block

Status: yellow

## Elements:

**EL** Name: Switch 1 of the cover

B10d [cycles]: 1000000

nop [cycles/a]: 96000

T10d [a]: 10.42

MTTFd [a] (via B10d): 104.17 (high)

Service life [a]: 10

DC [%]: 90 (moderate)

## Documentation element

Technology: electromechanical

Documentation:

Document:

## Degree of diagnostic coverage for element

Action: Temporal and logical program run monitoring by the watchdog, wherein the test device performs plausibility tests of the behavior of the logic.

# SISTEMA – Safety of controls on machines



Project Speedy 500 all variants – 8014

File Date: 5/5/2015: Report date: 5/5/2015: Checksum: e5631223c2d17baefddd55aa16852a2d

**SF** Safety function: All openable covers are secured with two switches.  
The interconnection is built to be redundant and diverse.

(logic)  
(90%)

### Status / Notes element

Status: yellow

Notes [Note status]: For the intended architectures, a typical service life of 20 years is assumed.  
A service life of 10 years has been entered for the element (see MTTFd tab), which undercuts this value. Timely replacement of the element is recommended.  
[yellow]

For the intended architectures, a typical service life of 20 years is assumed. The element has a limited operating time (T10d) of 10.42 years (see tab MTTFd), which undercuts this value.  
Timely replacement of the element is recommended.  
[yellow]

### Elements:

**EL** Name: **Switch 1 of the left cover**

B10d [cycles]: 1000000 nop [cycles/a]: 50

T10d [a]: 20000 MTTFd [a] (via B10d): 200000 (high)

Service life [a]: 20

DC [%]: 90 (moderate)

### Documentation element

Technology: electromechanical

Documentation:

Document:

### Degree of diagnostic coverage for element

Action: Temporal and logical program run monitoring by the watchdog, wherein the test device performs plausibility tests of the behavior of the logic.

(logic)  
(90 %)

### Status / Notes element

Status: green

Notes [Note status]:

# SISTEMA – Safety of controls on machines



Project Speedy 500 all variants – 8014

File Date: 5/5/2015: Report date: 5/5/2015: Checksum: e5631223c2d17baefddd55aa16852a2d

**SF** Safety function: All openable covers are secured with two switches.  
The interconnection is built to be redundant and diverse.

## Elements:

**EL** Name: **Switch 1 hatch at the back**

B10d [cycles]: 1000000

nop [cycles/a]: 400

T10d [a]: 2500

MTTFd [a] (via B10d): 25000 (high)

Service life [a]: 20

DC [%]: 90 (moderate)

### *Documentation element*

Technology:

electromechanical

Documentation:

Document:

### *Degree of diagnostic coverage for element*

Action:

Temporal and logical program run monitoring by the watchdog, wherein the test device performs plausibility tests of the behavior of the logic.

(logic)  
(90 %)

### *Status / Notes element*

Status:

green

Notes [Note status]:

## Channels / Test Channel:

**CH** Name: Channel 2

MTTFd [a]: 103.68

### Blocks:

**BL** Name: **Interlock circuit 2**

MTTFd [a]: 103.68 (high)

DC [%]: 90 (moderate)

Service life [a]: 20

### *Documentation block*

Documentation:

Document:

### *Status / Notes block*

Status:

yellow

# SISTEMA – Safety of controls on machines



Project Speedy 500 all variants – 8014

File Date: 5/5/2015: Report date: 5/5/2015: Checksum: e5631223c2d17baefddd55aa16852a2d

**SF** Safety function: All openable covers are secured with two switches.  
The interconnection is built to be redundant and diverse.

## Elements:

**EL** Name: **Switch 2 of the cover**

B10d [cycles]: 1000000

nop [cycles/a]: 96000

T10d [a]: 10.42

MTTFd [a] (via B10d): 104.17 (high)

Service life [a]: 10

DC [%]: 90 (moderate)

### *Documentation element*

Technology:

electromechanical

Documentation:

Document:

### *Degree of diagnostic coverage for element*

Action:

Temporal and logical program run monitoring by the watchdog, wherein the test device performs plausibility tests of the behavior of the logic.

(logic)  
90 %

### *Status / Notes element*

Status:

yellow

Notes [Note status]:

For the intended architectures, a typical service life of 20 years is assumed.  
A service life of 10 years has been entered for the element (see MTTFd tab), which undercuts this value. Timely replacement of the element is recommended.  
[yellow]

For the intended architectures, a typical service life of 20 years is assumed. The element has a limited operating time (T10d) of 10.42 years (see tab MTTFd), which undercuts this value.  
Timely replacement of the element is recommended.  
[yellow]

## Elements:

**EL** Name: **Switch 2 of the left cover**

B10d [cycles]: 1000000

nop [cycles/a]: 50

T10d [a]: 20000

MTTFd [a] (via B10d): 200000 (high)

Service life [a]: 20

DC [%]: 90 (moderate)

# SISTEMA – Safety of controls on machines



Project Speedy 500 all variants – 8014

File Date: 5/5/2015: Report date: 5/5/2015: Checksum: e5631223c2d17baefddd55aa16852a2d

**SF** Safety function: All openable covers are secured with two switches.  
The interconnection is built to be redundant and diverse.

### Documentation element

Technology: electromechanical

Documentation:

Document:

### Degree of diagnostic coverage for element

Action: Temporal and logical program run monitoring by the watchdog, wherein the test device performs plausibility tests of the behavior of the logic.

(logic)

90 %

### Status / Notes element

Status: green

Notes [Note status]:

### Elements:

**EL** Name: **Switch 2 hatch at the back**

B10d [cycles]: 1000000 nop [cycles/a]: 400

T10d [a]: 2500 MTTFd [a] (via B10d): 25000 (high)

Service life [a]: 20

DC [%]: 90 (moderate)

### Documentation element

Technology: electromechanical

Documentation:

Document:

### Degree of diagnostic coverage for element

Action: Temporal and logical program run monitoring by the watchdog, wherein the test device performs plausibility tests of the behavior of the logic.

(logic)

(90 %)

### Status / Notes element

Status: green

Notes [Note status]:



Project Speedy 500 all variants – 8014

File Date: 5/5/2015 Report date: 5/5/2015 Checksum: e5631223c2d17baefddd55aa16852a2d

---

## DISCLAIMER

The software has been carefully prepared according to the state of the art in science and technology. It is provided to the user free of charge.

Any use of the software is at the user's own risk. Any liability – for whatever legal reason – is excluded, as far as legally permissible. In particular for material and legal defects of the software, as well as of the related documentation and information – especially in view of their correctness, absence of errors, absence of intellectual property rights of third parties, up-to-dateness, completeness and / or usability –, no liability will be assumed, except in case of intent or bad faith.

The IFA endeavors to keep its homepage virus-free, but the software and information provided cannot be guaranteed to be virus-free. The user is therefore advised to independently ensure adequate safety precautions and virus scanning before downloading any software, documentation, or information.

## CONTACT

Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA)

Fachbereich 5: Unfallverhütung – Produktsicherheit

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

Department 5: Accident Prevention – Product Safety]

Alte Heerstr. 111, D-53757 Sankt Augustin

Email: [sistema@dguv.de](mailto:sistema@dguv.de) [www.dguv.de/ifa](http://www.dguv.de/ifa)

(Web code: d3022)

---

Date, signature of author

---

Date, signature of tester

---