

# Manufacturer's declaration of cybersecurity



## Cybersecurity NEW LIFT products

Publisher: NEW LIFT Neue elektronische Wege Steuerungsbau GmbH

Lochhamer Schlag 8  
82166 Gräfelfing

Phone: +49 (0) 89/89 866 – 0

Fax: +49 (0) 89/89 866 – 300

E-mail: [info@newlift.de](mailto:info@newlift.de)

WEB: <http://www.newlift.de>

Document version: 1.2

Created:	TF	Date :	08.03.2024	Page: 1 of 17
Reviewed:	QMB	Date:	10.03.2024	FB_Manufacturer's declaration of cybersecurity.dot
Approved:	AL	Date:	10.03.2024	Stauts 02/2024

# Manufacturer's declaration of cybersecurity



## History of document versions

Document version	Date	Creator	Approval	Comment
1.1	08.03.24	Thomas Früchtl	Yes	Initial creation
1.2	27.06.24	Alexander Linke	Yes	Correction to chapters 3, 5, 5.7.1, 8.4.1, 8.6.1 & overview

## Approved by:

Name	Date	Function	Department	E-mail
Peter Zeitler	27.06.24	GF	GL	<a href="mailto:info@newlift.de">info@newlift.de</a>
Alexander Linke	27.06.24	QMB	GL	<a href="mailto:info@newlift.de">info@newlift.de</a>

## Table of contents

1	General .....	6
2	Standards and norms used .....	6
3	Terms and abbreviations .....	6
4	Product requirements .....	7
4.1	ISO8102-20 Domains of EUC functions.....	7
4.2	Basic requirements from ISO 8102-20.....	7
4.3	Security level .....	7
5	Lift controls FST-(1), FST-2(XT), FST-2(XT)s, FST-3 (FST Family) .....	8
5.1	FR1 Identification and authentication control SL-T 2.....	8
5.1.1	HMI.....	8
5.1.2	Network and RS232 interface .....	8
5.1.3	Result .....	8
5.2	FR2 Usage control SL-T2 .....	8
5.2.1	HMI.....	8
5.2.2	Network and RS232 interface .....	8
5.2.3	Other interfaces such as LON and CAN.....	8
5.2.4	Result .....	8
5.3	FR3 System integrity SL-T2.....	8
5.3.1	HMI.....	8

Created:	TF	Date :	08.03.2024	Page: 2 of 17
Reviewed:	QMB	Date:	10.03.2024	FB_Manufacturer's declaration of cybersecurity.dot
Approved:	AL	Date:	10.03.2024	Stauts 02/2024

# Manufacturer's declaration of cybersecurity



5.3.2	Network and RS232 interface .....	9
5.3.3	Result .....	9
5.4	FR4 Data confidentiality SL-T1 .....	9
5.4.1	Result .....	9
5.5	FR5 Restricted data flow SL-T1 .....	9
5.5.1	Result .....	9
5.6	FR6 Timely response to events -T1 .....	9
5.6.1	Result .....	9
5.7	FR7 Resource availabilitySL-T2 .....	9
5.7.1	FST-2, FST-2XT and FST-2XTs .....	9
5.7.2	FST-3 .....	9
5.7.3	Result .....	9
5.8	Overall result FST.....	9
6	Security systems S1,S2 .....	10
6.1	FR1 Identification and authentication control SL-T 3.....	10
6.1.1	Result .....	10
6.2	FR2 Usage control SL-T2 .....	10
6.2.1	Result .....	10
6.3	FR3 System integrity SL-T2.....	10
6.3.1	Result .....	10
6.4	FR4 Data confidentiality SL-T2.....	10
6.4.1	Result .....	11
6.5	FR5 Restricted data flow SL-T1 .....	11
6.5.1	Result .....	11
6.6	FR6 Timely response to events SL-T1.....	11
6.6.1	Result .....	11
6.7	FR7 Resource availability SL-T2 .....	11
6.7.1	Result .....	11
6.8	Overall result S1,S2.....	11
7	Contactless brake module CBM1 / CBM2 .....	11
7.1	FR1 Identification and authentication control SL-T 3.....	11
7.1.1	Result .....	12
7.2	FR2 Usage control SL-T2 .....	12
7.2.1	Result .....	12
7.3	FR3 System integrity SL-T2.....	12
7.3.1	Result .....	12
7.4	FR4 Data confidentiality SL-T2.....	12
7.4.1	Result .....	12

Created:	TF	Date :	08.03.2024	Page: 3 of 17
Reviewed:	QMB	Date:	10.03.2024	FB_Manufacturer's declaration of cybersecurity.dot
Approved:	AL	Date:	10.03.2024	Stauts 02/2024

# Manufacturer's declaration of cybersecurity



7.5	FR5 Restricted data flow SL-T1 .....	12
7.5.1	Result .....	12
7.6	FR6 Timely response to events SL-T1.....	12
7.6.1	Result .....	13
7.7	FR7 Resource availability SL-T2 .....	13
7.7.1	Result .....	13
7.8	Overall result CBM1, CBM2.....	13
8	Lift controls SST, KST, EST .....	13
8.1	FR1 Identification and authentication control SL-T 2.....	13
8.1.1	HMI.....	13
8.1.2	RS232 Interface.....	13
8.1.3	Result .....	13
8.2	FR2 Usage control SL-T2 .....	13
8.2.1	HMI.....	13
8.2.2	RS232 Interface.....	14
8.2.3	Other Interfaces.....	14
8.2.4	Result .....	14
8.3	FR3 System integrity SL-T2.....	14
8.3.1	HMI.....	14
8.3.2	RS232 Interface.....	14
8.3.3	Result .....	14
8.4	FR4 Data confidentiality SL-T1 .....	14
8.4.1	Result .....	14
8.5	FR5 Restricted data flow SL-T1 .....	14
8.5.1	Result .....	14
8.6	FR6 Timely response to events SL-T1.....	14
8.6.1	Result .....	14
8.7	FR7 Resource availability SL-T2 .....	15
8.7.1	SST,KST and EST – control .....	15
8.7.2	Result .....	15
8.8	Overall result SST,KST and EST – control .....	15
9	Security system SA3-S.....	15
9.1	FR1 Identification and authentication control SL-T 3.....	15
9.1.1	Result .....	15
9.2	FR2 Usage control SL-T2 .....	15
9.2.1	Result .....	15
9.3	FR3 System integrity SL-T2.....	15
9.3.1	Result .....	15
9.4	FR4 Data confidentiality SL-T2.....	15

Created:	TF	Date :	08.03.2024	Page: 4 of 17
Reviewed:	QMB	Date:	10.03.2024	FB_Manufacturer's declaration of cybersecurity.dot
Approved:	AL	Date:	10.03.2024	Stauts 02/2024

# Manufacturer's declaration of cybersecurity



9.4.1	Result .....	16
9.5	FR5 Restricted data flow SL-T1 .....	16
9.5.1	Result .....	16
9.6	FR6 Timely response to events SL-T1.....	16
9.6.1	Result .....	16
9.7	FR7 Resource availability SL-T2 .....	16
9.7.1	Result .....	16
9.8	Overall result SA3-S .....	16
10	Overview .....	17

Created:	TF	Date :	08.03.2024	Page: 5 of 17
Reviewed:	QMB	Date:	10.03.2024	FB_Manufacturer's declaration of cybersecurity.dot
Approved:	AL	Date:	10.03.2024	Stauts 02/2024

# Manufacturer's declaration of cybersecurity



## 1 General

According to TRBS 1115-1, control and safety systems (MSR systems) must be protected against cyber threats in accordance with the state of the art, in order to prevent hazards to persons in systems requiring monitoring.

To assess the risks arising from cyberattacks, the ISO 8102-20 standard is used as a guideline for products relevant to NEW LIFT. This standard makes numerous references to IEC 62443.

NEW LIFT primarily considers itself a manufacturer and developer of components. Therefore, IEC 62443 Part 4 is regarded as the relevant standard.

## 2 Standards and norms used

TRBS 1115-1  
ISO8102-20  
IEC62443-4

## 3 Terms and abbreviations

FST-(1) / FST-2 / FST-2XT\* NEW LIFT lift control system standard  
FST-2XTs / FST-2s\* NEW LIFT lift control system model for installation in frames  
FST-3 NEW LIFT lift control system with connection to safety module S2  
S1\* Safety System 1st generation  
S2 Safety system 2nd generation  
CBM (1 and 2) Contactorless brake module  
SST\* NEW LIFT Lift control  
KST\* NEW LIFT Lift control  
EST\* NEW LIFT Lift control  
SA3-S\* NEW LIFT Safety system for UCM-A3 function  
EUC Equipment Under Control  
SL-C Security Level Capability; security level that a device or system can achieve when used and configured correctly  
SL-A Security Level Achieved; the measurable security level achieved in the overall system  
SL-T Security Level Target; this target security level is the result of a threat/risk analysis (ISO 8102-20)  
FR1 to FR7 Basic Requirement, see IEC62443-3-3 from point 5 onwards

\*Product already discontinued or replaced

Created:	TF	Date :	08.03.2024	Page: 6 of 17
Reviewed:	QMB	Date:	10.03.2024	FB_Manufacturer's declaration of cybersecurity.dot
Approved:	AL	Date:	10.03.2024	Stauts 02/2024

# Manufacturer's declaration of cybersecurity



## 4 Product requirements

### 4.1 ISO8102-20 Domains of EUC functions

Domain	Description
Safety	SIL-rated electronic safety devices and electrical protective devices
Essential	e.g. Normal control e.g. Cabins and external call devices ...
Alarm	Alarm and intercom systems ...

for further devices, see ISO 8102-20 table 1

### 4.2 Basic requirements from ISO 8102-20

Basic requirement FR	Domain according to ISO8102-20		
	Alarm	Essential	Safety
FR1- Identification and authentication control	2	2	3
FR2- Usage control	2	2	2
FR3- System integrity	2	2	2
FR4- Data confidentiality	1	2	2
FR5- Restricted data flow	1	1	1
FR6- Timely response to events	1	1	1
FR7- Resource availability	1	2	2

### 4.3 Security level

Level	Description
0	No special requirements or protection necessary.
1	Protection against unintentional or accidental misuse.
2	Protection against deliberate misuse using simple means with limited resources, general skills and low motivation.
3	Protection against deliberate abuse using sophisticated means with moderate resources, IACS-specific knowledge and moderate motivation.
4	Protection against deliberate misuse using sophisticated means with extensive resources, IACS-specific knowledge and high motivation.

Created:	TF	Date :	08.03.2024	Page: 7 of 17
Reviewed:	QMB	Date:	10.03.2024	FB_Manufacturer's declaration of cybersecurity.dot
Approved:	AL	Date:	10.03.2024	Stauts 02/2024

# Manufacturer's declaration of cybersecurity



## 5 Lift controls FST-(1), FST-2(XT), FST-2(XT)s, FST-3 (FST Family)

In accordance with ISO8102-20 security requirements, the lift control system is considered to belong to the 'necessary' domain. This must meet a security level vector of **SL-T** of {2,2,2,2,1,1,2}.

### 5.1 FR1 Identification and authentication control SL-T 2

#### 5.1.1 HMI

The FST family has multi-level password protection across various levels.

In addition, access to the controls must be prevented for unauthorised persons by appropriate measures such as a locked machine room and/or locked switch cabinet.

#### 5.1.2 Network and RS232 interface

Connections via the above-mentioned interfaces are simulated exclusively by the FST control system. The control system authenticates itself to the corresponding application (e.g. PAM.E4 Gateway) using a unique ID. There is no direct communication from the control system to the Internet.

#### 5.1.3 Result

The FST has security level SL-C2 for FR1.

### 5.2 FR2 Usage control SL-T2

#### 5.2.1 HMI

The same regulations apply as in point 5.1.1. The FST control system is installed in a lockable machine room, switch cabinet, which can only be accessed by authorised persons.

#### 5.2.2 Network and RS232 interface

Usage control is subject to the application that accesses the controller.

#### 5.2.3 Other interfaces such as LON and CAN

Access to the bus systems must also be denied to unauthorised persons.

#### 5.2.4 Result

The FST has security level SL-C2 for FR2.

### 5.3 FR3 System integrity SL-T2

#### 5.3.1 HMI

Changes to the FST control software, such as software updates, may only be made by authorised personnel using a suitably prepared data carrier.

Created:	TF	Date :	08.03.2024	Page: 8 of 17
Reviewed:	QMB	Date:	10.03.2024	FB_Manufacturer's declaration of cybersecurity.dot
Approved:	AL	Date:	10.03.2024	Stauts 02/2024

# Manufacturer's declaration of cybersecurity



## 5.3.2 Network and RS232 interface

Changes to the FST control software are not possible via these interfaces.

## 5.3.3 Result

The FST has security level SL-C2 for FR3.

## 5.4 FR4 Data confidentiality SL-T1

The FST controllers do not store any personal data.

The recording and error/event logs can only be read out by query.

## 5.4.1 Result

The FST has security level SL-C2 for FR4.

## 5.5 FR5 Restricted data flow SL-T1

Manipulation of data, e.g. via LON or CAN bus, is only possible with expert knowledge and physical access.

## 5.5.1 Result

The FST has security level SL-C2 for FR5.

## 5.6 FR6 Timely response to events -T1

The FST control system generates a recording entry in the event of errors or malfunctions.

## 5.6.1 Result

The FST has security level SL-C2 for FR5.

## 5.7 FR7 Resource availability SL-T2

### 5.7.1 FST-2, FST-2XT and FST-2XTs

Safety functions (door override) are implemented exclusively in hardware and are therefore independent of communication within the control software.

### 5.7.2 FST-3

Safety functions are independent of communication within the control system.

The associated safe system S2 is discussed separately below.

### 5.7.3 Result

The FST has security level SL-C2 for FR5.

## 5.8 Overall result FST

Under the above conditions, the FST can achieve an SL-C Vector of {2,2,2,2,2,2,2}.

Created:	TF	Date :	08.03.2024	Page: 9 of 17
Reviewed:	QMB	Date:	10.03.2024	FB_Manufacturer's declaration of cybersecurity.dot
Approved:	AL	Date:	10.03.2024	Stauts 02/2024

# Manufacturer's declaration of cybersecurity



## 6 Security systems S1,S2

In accordance with ISO8102-20 security requirements, security devices S1 and S2 are considered to belong to the 'Safety' domain. These must fulfil a security level vector of SL-T of {3,2,2,2,1,1,2}.

### 6.1 FR1 Identification and authentication control SL-T 3

The S1 and S2 modules do not have authentication.

However, measures have been taken to prevent accidental changes to security-related parameters.

These include:

Learning and changing limit switch positions.

Learning and changing floor positions.

Changing trigger speeds.

The configuration is secured by a CRC checksum.

The above parameters can only be changed by an authorised person on site.

#### 6.1.1 Result

The S1 and S2 have security level SL-C3 for FR1, provided that the modules are located in a lockable machine room or control cabinet.

### 6.2 FR2 Usage control SL-T2

The same regulations apply as in point 6.1. modules S1 and S1 are installed in a lockable machine room, switch cabinet, which can only be accessed by authorised persons.

Safety modules S1 and S2 are installed in a lockable machine room, switch cabinet, which can only be accessed by authorised persons.

#### 6.2.1 Result

The S1 and S2 have security level SL-C3 for FR2, provided that the modules are located in a lockable machine room or control cabinet.

### 6.3 FR3 System integrity SL-T2

The software of S1 and S2 cannot be modified either in part or in whole.

The S1 and S2 modules verified the correctness of the software using CRC checksums.

#### 6.3.1 Result

The S1 and S2 have security level SL-C2 for FR3.

### 6.4 FR4 Data confidentiality SL-T2

The S1 and S2 safety modules do not store any personal data.

The error and event logs are made available on the CAN bus.

Manipulation of the data has no effect on safety and is only possible with expert knowledge and physical access.

Created:	TF	Date :	08.03.2024	Page: 10 of 17
Reviewed:	QMB	Date:	10.03.2024	FB_Manufacturer's declaration of cybersecurity.dot
Approved:	AL	Date:	10.03.2024	Stauts 02/2024

# Manufacturer's declaration of cybersecurity



## 6.4.1 Result

The S1 and S2 have security level SL-C2 for FR4, provided that the modules are located in a lockable machine room or control cabinet.

## 6.5 FR5 Restricted data flow SL-T1

Manipulation of data, e.g. via LON or CAN bus, is only possible with expert knowledge and physical access.

### 6.5.1 Result

The S1 and S2 have security level SL-C2 for FR5, provided that the modules are located in a lockable machine room or control cabinet.

## 6.6 FR6 Timely response to events SL-T1

The safety modules S1 and S2 independently check the RAM (Random Access Memory) and the programme memory. In the event of a fault, the 'safe' state is assumed.

### 6.6.1 Result

The S1 and S2 have security level SL-C2 for FR6.

## 6.7 FR7 Resource availability SL-T2

The safety functions in S1 and S2 are independent of communication with other devices (CAN BUS).

In the event of voltage dips or voltage drops, S1 and S2 automatically switch to the safe state.

### 6.7.1 Result

The S1 and S2 have security level SL-C2 for FR7, provided that the modules are located in a lockable machine room or control cabinet.

## 6.8 Overall result S1,S2

Under the above conditions, S1 and S2 can achieve an SL-C vector of {3,3,2,2,2,2,2}.

## 7 Contactorless brake module CBM1 / CBM2

In accordance with ISO8102-20 security requirements, CBM1 and CBM2 are considered to belong to the 'Safety' domain. This domain must fulfil a security level vector of **SL-T** of {3,2,2,2,1,1,2}.

### 7.1 FR1 Identification and authentication control SL-T 3

The CBM1 and CBM2 modules do not have authentication.  
All security-related functions are performed in hardware.

Some parameters, such as brake voltage, can be changed via the (FST) menu.

The above parameters can only be changed by an authorised person on site.

Created:	TF	Date :	08.03.2024	Page: 11 of 17
Reviewed:	QMB	Date:	10.03.2024	FB_Manufacturer's declaration of cybersecurity.dot
Approved:	AL	Date:	10.03.2024	Stauts 02/2024

# Manufacturer's declaration of cybersecurity



## 7.1.1 Result

The CBM1 and CBM2 have security level SL-C3 for FR1, provided that the modules are located in a lockable machine room or control cabinet.

## 7.2 FR2 Usage control SL-T2

The same regulations apply as in point 6.1. The CBM1 and CBM modules are installed in a lockable machine room, switch cabinet, which can only be accessed by authorised persons.

Brake modules CBM1 and CBM2 are installed in a lockable machine room, switch cabinet, which can only be accessed by authorised persons.

## 7.2.1 Result

The CBM1 and CBM2 have security level SL-C3 for FR2, provided that the modules are located in a lockable machine room or control cabinet.

## 7.3 FR3 System integrity SL-T2

The software of CBM1 and CBM2 cannot be modified either in part or in whole.  
The software has no influence on safety functionality.

## 7.3.1 Result

The CBM1 and CBM2 have security level SL-C3 for FR3, provided that the modules are located in a lockable machine room or control cabinet.

## 7.4 FR4 Data confidentiality SL-T2

The brake modules CBM1 and CBM2 do not store any personal data.  
The error and event logs are made available on the CAN bus.  
Manipulation of the data has no effect on safety and is only possible with expert knowledge and physical access.

## 7.4.1 Result

The CBM1 and CBM2 have security level SL-C2 for FR4, provided that the modules are located in a lockable machine room or control cabinet.

## 7.5 FR5 Restricted data flow SL-T1

Manipulation of data, e.g. via CAN bus, is only possible with expert knowledge and physical access.

## 7.5.1 Result

The CBM1 and CBM2 have security level SL-C2 for FR5, provided that the modules are located in a lockable machine room or control cabinet.

## 7.6 FR6 Timely response to events SL-T1

The brake modules CBM1 and CBM2 transmit faults and events via CAN bus.  
In the event of a fault, the 'safe' state is assumed.

Created:	TF	Date :	08.03.2024	Page: 12 of 17
Reviewed:	QMB	Date:	10.03.2024	FB_Manufacturer's declaration of cybersecurity.dot
Approved:	AL	Date:	10.03.2024	Stauts 02/2024

# Manufacturer's declaration of cybersecurity



## 7.6.1 Result

The CBM1 and CBM2 have security level SL-C2 for FR6, provided that the modules are located in a lockable machine room or control cabinet.

## 7.7 FR7 Resource availability SL-T2

The safety functions in CBM1 and CBM2 are independent of communication with other devices (CAN BUS).

In the event of voltage drops, CBM1 and CBM2 automatically switch to the safe state.

### 7.7.1 Result

The CBM1 and CBM2 have security level SL-C2 for FR7, provided that the modules are located in a lockable machine room or control cabinet.

## 7.8 Overall result CBM1, CBM2

Under the above conditions, CBM1 and CBM2 can achieve an SL-C vector of {3,3,2,2,2,2,2}.

## 8 Lift controls SST, KST, EST

In accordance with ISO8102-20 security requirements, the lift control system is considered to belong to the 'necessary' domain.

This must meet a security level vector of SL-T of {2,2,2,2,1,1,2}.

## 8.1 FR1 Identification and authentication control SL-T 2

### 8.1.1 HMI

The KST and EST have multi-level password protection across various levels.  
The SST does not have an HMI.

In addition, access to the control systems must be prevented for unauthorised persons by means of suitable measures such as a locked machine room and/or locked control cabinet.

### 8.1.2 RS232 Interface

An additional modem that can only establish a peer-to-peer connection is required for connecting to external devices via the above-mentioned interface. There is no direct communication from the control system to the Internet. The SST control system does not have the above-mentioned interface.

### 8.1.3 Result

The SST, KST and EST have security level SL-C2 for FR1.

## 8.2 FR2 Usage control SL-T2

### 8.2.1 HMI

The same regulations apply as in point 8.1.1. The SST, KST and EST control system is installed in a lockable machine room, switch cabinet, which can only be accessed by authorised persons.

Created:	TF	Date :	08.03.2024	Page: 13 of 17
Reviewed:	QMB	Date:	10.03.2024	FB_Manufacturer's declaration of cybersecurity.dot
Approved:	AL	Date:	10.03.2024	Stauts 02/2024

# Manufacturer's declaration of cybersecurity



## 8.2.2 RS232 Interface

Usage control is subject to the application that accesses the controller.

## 8.2.3 Other Interfaces

None.

## 8.2.4 Result

The SST, KST and EST have security level SL-C2 for FR2.

## 8.3 FR3 System integrity SL-T2

### 8.3.1 HMI

Changes to the SST, KST and EST control software, such as software updates, may only be carried out by authorised personnel and with a suitably prepared EEPROM.

### 8.3.2 RS232 Interface

Changes to the SST, KST and EST control software are not possible via these interfaces.

### 8.3.3 Result

The SST, KST and EST have security level SL-C2 for FR3.

## 8.4 FR4 Data confidentiality SL-T1

The SST, KST and EST controllers do not store any personal data. The error and event logs can only be read out by query.

### 8.4.1 Result

The SST, KST and EST have security level SL-C2 for FR4.

## 8.5 FR5 Restricted data flow SL-T1

Manipulation of the data, e.g. via LON or CAN bus, is not possible as serial bus systems are not available.

### 8.5.1 Result

The SST, KST and EST have security level SL-C2 for FR5.

## 8.6 FR6 Timely response to events SL-T1

The SST, KST and EST control systems generate an error entry in the event of errors or malfunctions.

### 8.6.1 Result

The SST, KST and EST have security level SL-C2 for FR5.

Created:	TF	Date :	08.03.2024	Page: 14 of 17
Reviewed:	QMB	Date:	10.03.2024	FB_Manufacturer's declaration of cybersecurity.dot
Approved:	AL	Date:	10.03.2024	Stauts 02/2024

# Manufacturer's declaration of cybersecurity



## 8.7 FR7 Resource availability SL-T2

### 8.7.1 SST,KST and EST – control

Safety functions (door override) are implemented exclusively in the hardware and are therefore independent of communication within the control software.

### 8.7.2 Result

The SST, KST and EST control systems have security level SL-C2 for FR5.

## 8.8 Overall result SST,KST and EST – control

Under the above conditions, the SST, KST and EST control can achieve an SL-C vector of {2,2,2,2,2,2,2}.

## 9 Security system SA3-S

In accordance with ISO8102-20 security requirements, the SA3-S is considered to belong to the 'Safety' domain, which must meet a security level vector of SL-T of {3,2,2,2,1,1,2}.

### 9.1 FR1 Identification and authentication control SL-T 3

The SA3-S modules do not have authentication, HMI or parameter setting options.

#### 9.1.1 Result

The SA3-S has security level SL-C3 for FR1, provided that the modules are located in a lockable machine room or control cabinet.

### 9.2 FR2 Usage control SL-T2

The same regulations apply as in section 9.1. The SA3-S module is installed in a lockable machine room, lift shaft or control cabinet which can only be accessed by authorised persons.

#### 9.2.1 Result

The SA3-S has security level SL-C3 for FR2, provided that the modules are located in a lockable machine room, lift shaft or control cabinet.

### 9.3 FR3 System integrity SL-T2

The SA3-S software cannot be modified, either in part or in whole. The SA3-S device verifies the correctness of the software using CRC checksums.

#### 9.3.1 Result

The SA3-S has security level SL-C2 for FR3.

### 9.4 FR4 Data confidentiality SL-T2

The SA3-S safety modules do not store any personal data. The error and event logs are made available via a USB-C interface. Manipulation of the data has no effect on safety and is only possible with expert knowledge and physical access.

Created:	TF	Date :	08.03.2024	Page: 15 of 17
Reviewed:	QMB	Date:	10.03.2024	FB_Manufacturer's declaration of cybersecurity.dot
Approved:	AL	Date:	10.03.2024	Stauts 02/2024

# Manufacturer's declaration of cybersecurity



## 9.4.1 Result

The SA3-S has security level SL-C2 for FR4, provided that the modules are located in a lockable machine room, lift shaft or control cabinet.

## 9.5 FR5 Restricted data flow SL-T1

Manipulation of data, e.g. via USB-C, is only possible with expert knowledge, manufacturer-specific interface adapters and physical access.

## 9.5.1 Result

The SA3-S has security level SL-C2 for FR5, provided that the modules are located in a lockable machine room, lift shaft or control cabinet.

## 9.6 FR6 Timely response to events SL-T1

The SA3-S safety modules independently check the RAM (Random Access Memory) and the programme memory. In the event of a fault, the 'safe' state is assumed.

## 9.6.1 Result

The SA3-S has security level SL-C2 for FR6.

## 9.7 FR7 Resource availability SL-T2

The safety functions of the SA3-S are independent of communication with other devices, as there is no physical connection.

In the event of voltage drops, SA3-S devices automatically switch to a safe state.

## 9.7.1 Result

The SA3-S has security level SL-C2 for FR7, provided that the module is located in a lockable machine room, lift shaft or control cabinet.

## 9.8 Overall result SA3-S

Under the above conditions, the SA3-S can achieve an SL-C vector of {3,3,2,2,2,2,2}.

Created:	TF	Date :	08.03.2024	Page: 16 of 17
Reviewed:	QMB	Date:	10.03.2024	FB_Manufacturer's declaration of cybersecurity.dot
Approved:	AL	Date:	10.03.2024	Stauts 02/2024

# Manufacturer's declaration of cybersecurity



## 10 Overview

Manufacturer's declaration of cybersecurity relating to:

TRBS 1115-1  
ISO8102-20  
IEC62443-4

27.06.2024

Overall results:

Product	FR1 / SL-T	FR2 / SL-T	FR3 / SL-T	FR4 / SL-T	FR5 / SL-T	FR6 / SL-T	FR7 / SL-T	Fundamental requirements of ISO 8102-20 fulfilled***
CBM**	3	3	2	2	2	2	2	YES
EST	2	2	2	2	2	2	2	YES
FST-(1)	2	2	2	2	2	2	2	YES
FST-2XT*	2	2	2	2	2	2	2	YES
FST-2XTs*	2	2	2	2	2	2	2	YES
FST-3	2	2	2	2	2	2	2	YES
KST	2	2	2	2	2	2	2	YES
S1	3	3	2	2	2	2	2	YES
S2	3	3	2	2	2	2	2	YES
SA3-S	3	3	2	2	2	2	2	YES
SST	2	2	2	2	2	2	2	YES

The 'Manufacturer's declaration of cybersecurity – Elevison 4.0 NEW LIFT' is available at <https://www.newlift.de/downloads-311.html> - 'Certificate'.

NEW LIFT Neue elektronische Wege Steuerungsbau GmbH  
Lochhamer Schlag 8  
82166 Gräfelfing

\* FST-2/s included

\*\* CBM 1 and 2

\*\*\* The requirements for the partial results of the respective product must be observed!

Created:	TF	Date :	08.03.2024	Page: 17 of 17
Reviewed:	QMB	Date:	10.03.2024	FB_Manufacturer's declaration of cybersecurity.dot
Approved:	AL	Date:	10.03.2024	Stauts 02/2024