Manufacturer's Declaration Cybersecurity

NEUE ELEKTRONISCHE WEGE

Cybersecurity NEW LIFT Products

Publisher: NEW LIFT Neue elektronische Wege Steuerungsbau GmbH

Lochhamer Schlag 8
82166 Gräfelfing

Tel.: +49 (0) 89/89 866 – 0
Fax: +49 (0) 89/89 866 – 300
E-mail: info@newlift.de
Web: http://www.newlift.de

Document version: 1.2

Manufacturer's Declaration Cybersecurity

NEWLIFT
NEUE ELEKTRONISCHE WEGE

Document version history

Document version	Date	Author	Approved	Remarks
1.1	08.03.24	Thomas Früchtl	Yes	Initial version
1.2	27.06.24	Alexander Linke	Yes	Correction of sections 3, 5, 5.7.1, 8.4.1, 8.6.1 & overall summary

Approved by:

Name	Date	Function	Dept.	E-mail
Peter Zeitler	27.06.24	MD	Mgmt.	info@newlift.de
Alexander Linke	27.06.24	QMB	Mgmt.	info@newlift.de

Table of contents

1 General 6
2 Applied standards 6
3 Terms and abbreviations 6
4 Product requirements 7
4.1 ISO 8102-20 domains of EUC functions 7
4.2 Basic requirements of ISO 8102-20 7
4.3 Security Level 7
5 Lift controllers 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 Use 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
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 SL-T1 9
5.6.1 Result 9
5.7 FR7 Resource availability SL-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 10
6 Safety systems S1, S2 10
6.1 FR1 Identification and authentication control SL-T 3 10
6.1.1 Result 10
6.2 FR2 Use 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 Contactorless Brake Module CBM1 / CBM2 11
7.1 FR1 Identification and authentication control SL-T 3 11
7.1.1 Result 12
7.2 FR2 Use 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
7.5 FR5 Restricted data flow SL-T1 12
7.5.1 Result 12

7.6 FR6 Timely response to events SL-T1 13
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 controllers 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 Use control SL-T2 14
8.2.1 HMI 14
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 15
8.6.1 Result 15
8.7 FR7 Resource availability SL-T2 15
8.7.1 SST, KST and EST controllers 15
8.7.2 Result 15
8.8 Overall result SST, KST and EST controllers 15
9 Safety system SA3-S 15
9.1 FR1 Identification and authentication control SL-T 3 15
9.1.1 Result 15
9.2 FR2 Use control SL-T2 15
9.2.1 Result 15
9.3 FR3 System integrity SL-T2 15
9.3.1 Result 16
9.4 FR4 Data confidentiality SL-T2 16
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 Overall summary 17

1 General

According to TRBS 1115-1, measurement, control and regulation (MCR) systems must be protected against cyber threats in line with the state of the art, so that hazards to persons at installations requiring monitoring are avoided.

To assess the hazards posed by cyberattacks, ISO 8102-20 is used as the guideline for the relevant NEW LIFT products. This standard refers to IEC 62443 in many places.

NEW LIFT sees itself primarily as a component manufacturer and developer.
Therefore, IEC 62443 Part 4 is considered relevant.

2 Applied standards

TRBS 1115-1
ISO8102-20
IEC62443-4

3 Terms and abbreviations

FST-(1) / FST-2 / FST-2XT* NEW LIFT lift controller, standard
FST-2XTs / FST-2s* NEW LIFT lift controller, model for installation in door frames
FST-3 NEW LIFT lift controller 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 controller
KST* NEW LIFT lift controller
EST* NEW LIFT lift controller
SA3-S* NEW LIFT safety system for UCM-A3 function
EUC Equipment under control
SL-C Security Level Capability; the security level that a device or system can achieve when properly used and configured
SL-A Security Level Achieved; the security level actually achieved and measurable in the overall system
SL-T Security Level Target; the security level to be achieved, resulting from the threat/risk analysis (ISO 8102-20)
FR1 to FR7 Foundational requirements, see IEC 62443-3-3 from section 5

*Product already discontinued or replaced

4 Product requirements

4.1 ISO 8102-20 domains of EUC functions

Domain	Description
Safety	SIL-rated electronic safety devices and electrical protective devices
Essential	e.g. standard controller e.g. car and landing call devices …
Alarm	Alarm and intercom systems …

for further devices see ISO 8102-20 Table 1

4.2 Basic requirements of ISO 8102-20

Foundational requirement FR	Domain acc. to ISO 8102-20		
	Alarm	Essential	Safety
FR1 - Identification and authentication control	2	2	3
FR2 - Use 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 specific requirement or protection necessary.
1	Protection against unintentional or accidental misuse.
2	Protection against intentional misuse using simple means with low resources, generic skills and low motivation.
3	Protection against intentional misuse using sophisticated means with moderate resources, IACS-specific skills and moderate motivation.
4	Protection against intentional misuse using sophisticated means with extended resources, IACS-specific skills and high motivation.

5 Lift controllers FST-(1), FST-2(XT), FST-2(XT)s, FST-3 (FST family)

Based on the security requirements of ISO 8102-20, the lift controller is considered to belong to the “Essential” domain, which is to meet an SL-T security level vector 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 several levels.

In addition, access to the controllers must be denied to unauthorised persons by suitable measures such as a locked machine room and/or a locked control cabinet.

5.1.2 Network and RS232 interface

Connections via the interfaces mentioned above are initiated exclusively by the FST controller. The controller authenticates itself to the respective application (e.g. PAM.E4 gateway) by means of a unique ID. There is no direct communication from the controller to the internet.

5.1.3 Result

For FR1, the FST has security level SL-C2.

5.2 FR2 Use control SL-T2

5.2.1 HMI

The same provisions as in section 5.1.1 apply. The FST controller is installed in a lockable machine room or control cabinet that can only be accessed by authorised persons.

5.2.2 Network and RS232 interface

Use control is the responsibility of the application that the controller accesses.

5.2.3 Other interfaces such as LON and CAN

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

5.2.4 Result

For FR2, the FST has security level SL-C2.

5.3 FR3 System integrity SL-T2

5.3.1 HMI

Changes to the FST controller software, such as software updates, are only possible by authorised personnel using a suitably prepared data carrier.

5.3.2 Network and RS232 interface

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

5.3.3 Result

For FR3, the FST has security level SL-C2.

5.4 FR4 Data confidentiality SL-T1

The FST controllers do not store any personal data.
The recording and the error and event logs can only be read out on request.

5.4.1 Result

For FR4, the FST has security level SL-C2.

5.5 FR5 Restricted data flow SL-T1

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

5.5.1 Result

For FR5, the FST has security level SL-C2.

5.6 FR6 Timely response to events SL-T1

The FST controller creates a recording entry in the event of errors or malfunctions.

5.6.1 Result

For FR6, the FST has security level SL-C2.

5.7 FR7 Resource availability SL-T2

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

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

5.7.2 FST-3

Safety functions are independent of communication within the controller.
The associated safety system S2 is considered separately below.

5.7.3 Result

For FR7, the FST has security level SL-C2.

5.8 Overall result FST

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

6 Safety systems S1, S2

Based on the security requirements of ISO 8102-20, the safety devices S1 and S2 are considered to belong to the “Safety” domain, which is to meet an SL-T security level vector of {3,2,2,2,1,1,2}.

6.1 FR1 Identification and authentication control SL-T 3

The S1 and S2 modules have no authentication.
However, measures have been taken to prevent accidental changes to safety-relevant parameters.

These include:
Teaching and changing limit switch positions.
Teaching and changing floor positions.
Changing tripping speeds.
The configuration is protected by a CRC checksum.

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

6.1.1 Result

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

6.2 FR2 Use control SL-T2

The same provisions as in section 6.1 apply. The S1 and S2 modules are installed in a lockable machine room or control cabinet that can only be accessed by authorised persons.

Safety modules S1 and S2 are installed in a lockable machine room or control cabinet that can only be accessed by authorised persons.

6.2.1 Result

For FR2, S1 and S2 have security level SL-C3, provided 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 changed, either partially or completely.
The S1 and S2 modules verify the correctness of the software using CRC checksums.

6.3.1 Result

For FR3, S1 and S2 have security level SL-C2.

6.4 FR4 Data confidentiality SL-T2

The safety modules S1 and S2 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.

6.4.1 Result

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

6.5 FR5 Restricted data flow SL-T1

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

6.5.1 Result

For FR5, S1 and S2 have security level SL-C2, provided 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 program memory. In the event of a fault, the “safe” state is assumed.

6.6.1 Result

For FR6, S1 and S2 have security level SL-C2.

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

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

6.8 Overall result S1, S2

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

7 Contactorless Brake Module CBM1 / CBM2

Based on the security requirements of ISO 8102-20, CBM1 and CBM2 are considered to belong to the “Safety” domain, which is to meet an SL-T security level vector of {3,2,2,2,1,1,2}.

7.1 FR1 Identification and authentication control SL-T 3

The CBM1 and CBM2 modules have no authentication.
All safety-relevant functions are implemented in hardware.

Some parameters, e.g. brake voltage, can be changed via the (FST) menu.

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

7.1.1 Result

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

7.2 FR2 Use control SL-T2

The same provisions as in section 7.1 apply. The CBM1 and CBM2 modules are installed in a lockable machine room or control cabinet that can only be accessed by authorised persons.

Brake modules CBM1 and CBM2 are installed in a lockable machine room or control cabinet that can only be accessed by authorised persons.

7.2.1 Result

For FR2, CBM1 and CBM2 have security level SL-C3, provided 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 changed, either partially or completely.
The software has no influence on the safety functionality.

7.3.1 Result

For FR3, CBM1 and CBM2 have security level SL-C3, provided 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

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

7.5 FR5 Restricted data flow SL-T1

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

7.5.1 Result

For FR5, CBM1 and CBM2 have security level SL-C2, provided 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 errors and events via the CAN bus.
In the event of a fault, the “safe” state is assumed.

7.6.1 Result

For FR6, CBM1 and CBM2 have security level SL-C2, provided 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 dips or voltage drops, CBM1 and CBM2 automatically switch to the safe state.

7.7.1 Result

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

7.8 Overall result CBM1, CBM2

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

8 Lift controllers SST, KST, EST

Based on the security requirements of ISO 8102-20, the lift controller is considered to belong to the “Essential” domain, which is to meet an SL-T security level vector 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 several levels.
The SST has no HMI.

In addition, access to the controllers must be denied to unauthorised persons by suitable measures such as a locked machine room and/or a locked control cabinet.

8.1.2 RS232 interface

A connection to external devices via the interface mentioned above requires an additional modem, which can only establish a peer-to-peer connection.
There is no direct communication from the controller to the internet. The SST controller does not have the interface mentioned above.

8.1.3 Result

For FR1, the SST, KST and EST have security level SL-C2.

8.2 FR2 Use control SL-T2

8.2.1 HMI

The same provisions as in section 8.1.1 apply. The SST, KST and EST controllers are installed in a lockable machine room or control cabinet that can only be accessed by authorised persons.

8.2.2 RS232 interface

Use control is the responsibility of the application that the controller accesses.

8.2.3 Other interfaces

None.

8.2.4 Result

For FR2, the SST, KST and EST have security level SL-C2.

8.3 FR3 System integrity SL-T2

8.3.1 HMI

Changes to the SST, KST and EST controller software, such as software updates, are only possible by authorised personnel using a suitably prepared EEPROM.

8.3.2 RS232 interface

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

8.3.3 Result

For FR3, the SST, KST and EST have security level SL-C2.

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 on request.

8.4.1 Result

For FR4, the SST, KST and EST have security level SL-C2.

8.5 FR5 Restricted data flow SL-T1

Manipulation of the data, e.g. via the LON or CAN bus, is not possible, as no serial bus systems are present.

8.5.1 Result

For FR5, the SST, KST and EST have security level SL-C2.

8.6 FR6 Timely response to events SL-T1

The SST, KST and EST controllers create an error entry in the event of errors or malfunctions.

8.6.1 Result

For FR6, the SST, KST and EST have security level SL-C2.

8.7 FR7 Resource availability SL-T2

8.7.1 SST, KST and EST controllers

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

8.7.2 Result

For FR7, the SST, KST and EST controllers have security level SL-C2.

8.8 Overall result SST, KST and EST controllers

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

9 Safety system SA3-S

Based on the security requirements of ISO 8102-20, the SA3-S is considered to belong to the “Safety” domain, which is to meet an SL-T security level vector of {3,2,2,2,1,1,2}.

9.1 FR1 Identification and authentication control SL-T 3

The SA3-S module has no authentication, no HMI and no means of setting parameters.

9.1.1 Result

For FR1, the SA3-S has security level SL-C3, provided the module is located in a lockable machine room or control cabinet.

9.2 FR2 Use control SL-T2

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

9.2.1 Result

For FR2, the SA3-S has security level SL-C3, provided the module is located in a lockable machine room, lift shaft or control cabinet.

9.3 FR3 System integrity SL-T2

The software of the SA3-S cannot be changed, either partially or completely. The SA3-S device verifies the correctness of the software using CRC checksums.

9.3.1 Result

For FR3, the SA3-S has security level SL-C2.

9.4 FR4 Data confidentiality SL-T2

The SA3-S safety module does 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.

9.4.1 Result

For FR4, the SA3-S has security level SL-C2, provided the module is located in a lockable machine room, lift shaft or control cabinet.

9.5 FR5 Restricted data flow SL-T1

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

9.5.1 Result

For FR5, the SA3-S has security level SL-C2, provided the module is located in a lockable machine room, lift shaft or control cabinet.

9.6 FR6 Timely response to events SL-T1

The SA3-S safety module independently checks the RAM (random access memory) and the program memory. In the event of a fault, the “safe” state is assumed.

9.6.1 Result

For FR6, the SA3-S has security level SL-C2.

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 dips or voltage drops, the SA3-S automatically switches to the safe state.

9.7.1 Result

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

9.8 Overall result SA3-S

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

10 Overall summary

Manufacturer's declaration on cybersecurity with reference 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	Basic requirements of ISO 8102-20 met***
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 on Cybersecurity – NEW LIFT Products” is available at https://www.newlift.de/downloads.html under “Bescheinigungen / Zertifikate” (certificates).

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

* FST-2/s included
** CBM 1 and 2
*** The conditions for the partial results of the respective product must be observed!