

# Manufacturer's declaration of cybersecurity



## Cybersecurity Elevision 4.0

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: 1.1

Created:	TF	Date :	08.03.2024	Page: 1 of 6
Reviewed:	QMB	Date :	10.03.2024	FB_Manufacturer's declaration of cybersecurity.dot
Approved:	AL	Date :	10.03.2024	Status 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

## Approved by:

Name	Date	Function	Department	E-mail
Peter Zeitler	16.03.24	GF	GL	<a href="mailto:info@newlift.de">info@newlift.de</a>

## Table of contents

1	General .....	<b>Fehler! Textmarke nicht definiert.</b>
2	Standards and norms used .....	<b>Fehler! Textmarke nicht definiert.</b>
3	Terms and abbreviations .....	<b>Fehler! Textmarke nicht definiert.</b>
4	Product requirements .....	4
4.1	Basic requirements from ISO62443 .....	4
4.2	Security level .....	4
5	Elevison 4.0 .....	4
5.1	FR1 Identification and authentication control .....	4
5.1.1	Result .....	<b>Fehler! Textmarke nicht definiert.</b>
5.2	FR2 Usage control .....	4
5.2.1	Result .....	<b>Fehler! Textmarke nicht definiert.</b>
5.3	FR3 System integrity .....	5
5.3.1	Result .....	<b>Fehler! Textmarke nicht definiert.</b>
5.4	FR4 Data confidentiality SL-T1 .....	5
5.4.1	Result .....	<b>Fehler! Textmarke nicht definiert.</b>
5.5	FR5 Restricted data flow SL-T1 .....	5
5.5.1	Result .....	<b>Fehler! Textmarke nicht definiert.</b>
5.6	FR6 Timely response to events SL-T1 .....	5
5.6.1	Result .....	<b>Fehler! Textmarke nicht definiert.</b>
5.7	FR7 Resource availability SL-T2 .....	5
5.7.1	Result .....	<b>Fehler! Textmarke nicht definiert.</b>

Created:	TF	Date :	08.03.2024	<b>Page: 2 of 6</b>
Reviewed:	QMB	Date :	10.03.2024	FB_Manufacturer's declaration of cybersecurity.dot
Approved:	AL	Date :	10.03.2024	Status 02/2024

# Manufacturer's declaration of cybersecurity



6 Overview ..... Fehler! Textmarke nicht definiert.

## 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 potential hazards arising from cyberattacks, the ISO 8102-20 standard is used as a guideline for the NEW LIFT FST product family. This standard makes numerous references to IEC 62443.

NEW LIFT considers itself primarily 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

E4 Elevision 4.0 cloud platform

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

Created:	TF	Date :	08.03.2024	Page: 3 of 6
Reviewed:	QMB	Date :	10.03.2024	FB_Manufacturer's declaration of cybersecurity.dot
Approved:	AL	Date :	10.03.2024	Status 02/2024

# Manufacturer's declaration of cybersecurity



## 4 Product requirements

### 4.1 Basic requirements from ISO62443

#### Basic requirements FR

FR1- Identification and authentication control

FR2- Usage control

FR3- System integrity

FR4- Data confidentiality

FR5- Restricted data flow

FR6- Timely response to events

FR7- Resource availability

### 4.2 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 misuse 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.

## 5 Elevision 4.0

### 5.1 FR1 Identification and authentication control

The Elevision 4.0 system has various authentication and identification procedures so that different security levels can be achieved.

#### 5.1.1 Result

With Elevision 4.0, activating two-factor authentication allows you to achieve **at least SL-C3** (attainable security level).

### 5.2 FR2 Usage control

E4 offers different user roles. Accesses and changes are logged in the system log, can be viewed by the administrator at any time, and can be archived as PDF files.

Created:	TF	Date :	08.03.2024	Page: 4 of 6
Reviewed:	QMB	Date :	10.03.2024	FB_Manufacturer's declaration of cybersecurity.dot
Approved:	AL	Date :	10.03.2024	Status 02/2024

# Manufacturer's declaration of cybersecurity



## 5.2.1 Result

The E4 has at least the SL-C3 for the FR2.

## 5.3 FR3 System integrity

The E4 is hosted by a hosting provider (server farm) that is ISO 27001 certified. The data is regularly backed up to an external drive.

### 5.3.1 Result

Elevison 4.0 achieves security level SL-C2 for FR3 .

## 5.4 FR4 Data confidentiality SL-T1

Elevison 4.0 does not store any personal data other than your E-mail address.

### 5.4.1 Result

Elevison 4.0 achieves at least security level SL-C2 for FR4.

## 5.5 FR5 Restricted data flow SL-T1

The data connection to the lift control system is established via a VPN channel in the case of GSM. The connection from the web browser to the web server is TSL-encrypted.

### 5.5.1 Result

Elevison 4.0 achieves at least security level SL-C2 for FR5.

## 5.6 FR6 Timely response to events SL-T1

Elevison 4.0 is monitored and controlled via 'Grafana'. In addition, events are recorded in the system log.

### 5.6.1 Result

Elevison 4.0 achieves at least security level SL-C2 for FR6.

## 5.7 FR7 Resource availability SL-T2

Elevison 4.0 is monitored and controlled via Grafana. The server is monitored for memory availability and upgraded as necessary.

### 5.7.1 Result

Elevison 4.0 achieves at least security level SL-C2 for FR7.

Created:	TF	Date :	08.03.2024	Page: 5 of 6
Reviewed:	QMB	Date :	10.03.2024	FB_Manufacturer's declaration of cybersecurity.dot
Approved:	AL	Date :	10.03.2024	Status 02/2024

# Manufacturer's declaration of cybersecurity



## 6 Overview

Manufacturer's declaration on cybersecurity relating to:

TRBS 1115-1  
ISO8102-20  
IEC62443-4

17.03.2024

Overall result:

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*
Elevision 4.0	3	3	2	2	2	2	2	YES

The 'Manufacturer's declaration of cybersecurity – Elevision 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

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

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