Herstellerklärung Cybersicherheit

NEWLIFT
NEUE ELEKTRONISCHE WEGE

Cybersicherheit NEW LIFT Produkte

Herausgeber: 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

Dokument-Version: 1.2

Herstellerklärung Cybersicherheit

NEWLIFT
NEUE ELEKTRONISCHE WEGE

Historie der Dokumentversionen

Dokument Version	Datum	Ersteller	Freigabe	Bemerkungen
1.1	08.03.24	Thomas Früchtl	Ja	Ersterstellung
1.2	27.06.24	Alexander Linke	Ja	Korrektur Kapitel 3, 5, 5.7.1, 8.4.1,8.6.1 & Gesamtübersicht

Freigabe durch:

Name	Datum	Funktion	Abteilung	E-Mail
Peter Zeitler	27.06.24	GF	GL	info@newlift.de
Alexander Linke	27.06.24	QMB	GL	info@newlift.de

Inhaltsverzeichnis

Herstellerklärung Cybersicherheit

NEW LIFT
NEUE ELEKTRONISCHE WEGE

1 Allgemein

Nach der TRBS 1115-1 müssen nach Stand der Technik MSR Systeme vor Cyberbedrohungen geschützt sein, so das Gefährdungen von Personen bei überwachungsbedürftigen Anlagen vermieden werden.

Zur Beurteilung der Gefährdungen durch Cyberangriffe werden für die NEW LIFT relevanten Produkte die ISO8102-20 als Richtlinie herangezogen. Dies verweist an vielen Stellen auf die IEC62433.

NEW LIFT sieht sich in erster Linie als Komponenten Hersteller und Entwickler
Daher wird die IEC62443 Teil 4 als relevant betrachtet.

2 Verwendete Standards und Normen

TRBS 1115-1
ISO8102-20
IEC62443-4

3 Begriffe und Abkürzungen

FST-(1) / FST-2 / FST-2XT* NEW LIFT Aufzugssteuerung Standard
FST-2XTs / FST-2s* NEW LIFT Aufzugssteuerung Modell zum Einbau in Zargen
FST-3 NEW LIFT Aufzugssteuerung mit Anbindung an Safety Modul S2
S1* Safetysystem 1. Generation
S2 Safetysystem 2. Generation
CBM (1 und 2) Contactorless Brake Modul
SST* NEW LIFT Aufzugsteuerung
KST* NEW LIFT Aufzugsteuerung
EST* NEW LIFT Aufzugsteuerung
SA3-S* NEW LIFT Safetysystem für UCM-A3 Funktion
EUC Geräte unter Kontrolle (Equipement under Control)
SL-C Security-Level Capability; Security-Level, den ein Gerät oder System erreichen kann, wenn es richtig eingesetzt und konfiguriert ist
SL-A Security-Level Achieved; Der im Gesamtsystem erreichte und messbare Security-Level
SL-T Security-Level Target; Dieser zu erzielende Security-Level ist ein Ergebnis der Bedrohungs-/Risikoanalyse (ISO 8102-20)
FR1 bis FR7 Basic Requirement, Grundlegende Anforderung siehe IEC62443-3-3 ab Punkt 5

*Produkt bereits abgekündigt oder ersetzt

4 Produkt Anforderungen

4.1 ISO8102-20 Domänen der EUC Funktionen

Domäne	Beschreibung
Safety Sicherheit	SIL bewertete elektronische Sicherheitseinrichtungen und elektrische Schutzeinrichtungen
Essential Notwendig	z.B. Normale Steuerung z.B. Kabinen und Aussenrufgeräte …
Alarm Alarm	Alarm und Gegensprechanlagen …

für weitere Geräte siehe ISO8102-20 Tabelle1

4.2 Grundsätzliche Anforderungen aus der ISO8102-20

Grundvoraussetzung FR	Domäne lt. ISO8102-20		
	Alarm	Notwendig	Safety
FR1- Identifikation und Authentifizierungskontrolle	2	2	3
FR2- Nutzungskontrolle	2	2	2
FR3- Systemintegrität	2	2	2
FR4- Datenvertraulichkeit	1	2	2
FR5- Eingeschränkter Datenfluss	1	1	1
FR6- Rechtzeitige Reaktion auf Ereignisse	1	1	1
FR-7- Ressourcenverfügbarkeit	1	2	2

4.3 Security Level

Level	Beschreibung
0	Keine besondere Anforderung oder Schutz erforderlich.
1	Schutz vor unbeabsichtigtem oder zufälligem Missbrauch.
2	Schutz vor vorsätzlichem Missbrauch mit einfachen Mitteln mit geringen Ressourcen, allgemeinen Fähigkeiten und geringer Motivation.
3	Schutz vor vorsätzlichem Missbrauch mit anspruchsvollen Mitteln mit moderaten Ressourcen, IACS-spezifischen Kenntnissen und moderater Motivation
4	Schutz vor vorsätzlichem Missbrauch unter Einsatz anspruchsvoller Mittel mit umfangreichen Ressourcen, IACS-spezifischen Kenntnissen und hoher Motivation

5 Aufzugssteuerungen FST-(1), FST-2(XT), FST-2(XT)s, FST-3 (FST Familie)

In Anlehnung an die ISO8102-20 Security Anforderungen wird die Aufzugssteuerung als Zugehörig zur Dömane „Notwendig“ betrachtet. Welche einen Security Level Vector von **SL-T** von {2,2,2,2,1,1,2} erfüllen soll.

5.1 FR1 Identifikation und Authentifizierungskontrolle SL-T 2

5.1.1 HMI

Die FST Familie besitzt eine mehrstufigen Passwortschutz über verschiedene Ebenen.

Zusätzlich muss der Zugang, zu den zu den Steuerungen durch geeignete Maßnahmen wie abgeschlossener Maschinenraum und oder abgeschlossener Schaltschrank, für Unbefugte verwehrt werden.

5.1.2 Netzwerk und RS232 Schnittstelle

Verbindungen über die oben genannten Schnittstellen werden ausschließlich durch die FST-Steuerung imitiert. Die Die Steuerung authentifiziert sich mittels einer Eindeutigen ID bei der Entsprechenden Applikation (z.B. PAM.E4 Gateway). Eine direkte Kommunikation von der Steuerung in das Internet findet nicht statt.

5.1.3 Ergebnis

Die FST besitzt, für FR1, den Security Level SL-C2

5.2 FR2 Nutzungskontrolle SL-T2

5.2.1 HMI

Es gelten die gleichen Regelungen wie in Punkt 5.1.1 Die FST- Steuerung wird in einem abschließbaren Maschineraum, Schaltschrank eingebaut welcher nur durch berechtigten Person betreten werden kann.

5.2.2 Netzwerk und RS232 Schnittstelle

Die Nutzungskontrolle unterliegt der Applikation auf die, die Steuerung zugreift.

5.2.3 Sonstige Schnittstellen wie LON und CAN

Der Zugang zu den Bussystemen ist ebenfalls für Unbefugte zu verwehren.

5.2.4 Ergebnis

Die FST besitzt, für FR2, den Security Level SL-C2.

5.3 FR3 Systemintegrität SL-T2

5.3.1 HMI

Änderungen an der FST-Steuerungssoftware wie z.B. Software Updates sind nur durch Zugangsberechtigtes Personal und eines entsprechend vorbereiteten Datenträgers möglich.

5.3.2 Netzwerk und RS232 Schnittstelle

Änderungen der FST Steuerungssoftware ist über diese Schnittstellen nicht möglich.

5.3.3 Ergebnis

Die FST besitzt, für FR3, den Security Level SL-C2.

5.4 FR4 Datenvertraulichkeit SL-T1

Die FST-Steuerungen speichern keine Personenbezogenen Daten.
Die Recording und Fehler-, Ereignislogs können nur durch Abfrage ausgelesen werden.

5.4.1 Ergebnis

Die FST besitzt, für FR4, den Security Level SL-C2.

5.5 FR5 Eingeschränkter Datenfluss SL-T1

Eine Manipulation der Daten z.B. über LON- oder CAN- Bus ist nur mit Expertenwissen und physischem Zugang möglich.

5.5.1 Ergebnis

Die FST besitzt, für FR5, den Security Level SL-C2.

5.6 FR6 Rechtzeitige Reaktion auf Ereignisse SL-T1

Die FST-Steuerung erzeugt bei Fehlern oder Betriebsstörungen einen Recording Eintrag.

5.6.1 Ergebnis

Die FST besitzt, für FR5, den Security Level SL-C2.

5.7 FR7 Ressourcenverfügbarkeit SL-T2

5.7.1 FST-2, FST-2XT und FST-2XTs

Sicherheitsfunktionen (Türüberbrückung) sind ausschließlich in Hardware abgebildet und somit unabhängig von der Kommunikation innerhalb der Steuerungssoftware.

5.7.2 FST-3

Sicherheitsfunktionen sind unabhängig von der Kommunikation innerhalb der Steuerung.
Das zugehörige Safe System S2 wird weiter unten gesondert betrachtet.

5.7.3 Ergebnis

Die FST besitzt, für FR5, den Security Level SL-C2.

5.8 Gesamtergebnis FST

Die FST kann, unter den oben genannten Bedingungen einen SL-C Vector von {2,2,2,2,2,2,2} erreichen.

6 Sicherheitssysteme S1,S2

In Anlehnung an die ISO8102-20 Security Anforderungen werden die Sicherheitsgeräte S1 und S2 als

Zugehörig zur Domäne „Safety“ betrachtet. Welche einen Security Level Vector von SL-T von {3,2,2,2,1,1,2} erfüllen soll.

6.1 FR1 Identifikation und Authentifizierungskontrolle SL-T 3

Die S1,S2 Module besitzen keine Authentifizierung.
Es wurden jedoch Maßnahmen getroffen um ein zufälliges Ändern von sicherheitsrelevanten Parametern zu verhindern.

Dazu zählen:
Lernen und verändern von Endschalter Positionen.
Lernen und verändern von Etagen Positionen.
Verändern von Auslösegeschwindigkeiten.
Die Konfiguration ist über eine Checksumme CRC abgesichert.

Eine Änderung der oben genannten Parameter ist nur durch vor einen vor Ort befindliche berechtigte Person möglich.

6.1.1 Ergebnis

Die S1, S2 besitzen, für FR1, den Security Level SL-C3 sofern sich die Module in einem abschließbaren Maschineraum bzw. Schaltschrank befinden.

6.2 FR2 Nutzungskontrolle SL-T2

Es gelten die gleichen Regelungen wie in Punkt 6.1 Die Module S1 und S1 werden in einem abschließbaren Maschineraum, Schaltschrank eingebaut welcher nur durch berechtigten Person betreten werden kann.

Sicherheitsmodule S1 und S2 sind in einem abschließbaren Maschineraum, Schaltschrank eingebaut welcher nur durch berechtigten Person betreten werden kann.

6.2.1 Ergebnis

Die S1, S2 besitzen, für FR2, den Security Level SL-C3 sofern sich die Module in einem abschließbaren Maschineraum bzw. Schaltschrank befinden.

6.3 FR3 Systemintegrität SL-T2

Die Software von S1, S2 kann weder in Teilen noch komplett geändert werden.
Die Module S1 und S2 überprüften die Korrektheit der Software anhand von Checksummen CRC.

6.3.1 Ergebnis

Die S1, S2 besitzen, für FR3, den Security Level SL-C2.

6.4 FR4 Datenvertraulichkeit SL-T2

Die Sicherheitsmodule S1 und S2 speichern keine Personenbezogenen Daten.
Die Fehler-, Ereignislogs werden auf dem CAN Bus zur Verfügung gestellt.
Eine Manipulation der Daten hat keinen Effekt auf die Sicherheit und ist nur mit Expertenwissen sowie physischen Zugang möglich.

6.4.1 Ergebnis

Die S1, S2 besitzen, für FR4, den Security Level SL-C2 sofern sich die Module in einem abschließbaren Maschineraum bzw. Schaltschrank befinden.

6.5 FR5 Eingeschränkter Datenfluss SL-T1

Eine Manipulation der Daten z.B. über LON- oder CAN- Bus ist nur mit Expertenwissen und physischem Zugang möglich.

6.5.1 Ergebnis

Die S1, S2 besitzen, für FR5, den Security Level SL-C2 sofern sich die Module in einem abschließbaren Maschineraum bzw. Schaltschrank befinden.

6.6 FR6 Rechtzeitige Reaktion auf Ereignisse SL-T1

Die Sicherheitsmodule S1 und S2 überprüfen unabhängig die RAM (Random Access Memory) und den Programmspeicher. Im Fehlerfall wir der „sichere“ Zustand eingenommen.

6.6.1 Ergebnis

Die S1, S2 besitzen, für FR6, den Security Level SL-C2.

6.7 FR7 Ressourcenverfügbarkeit SL-T2

Die Sicherheitsfunktionen in S1 und S2 sind unabhängig von der Kommunikation zu anderen Geräten (CAN BUS).
Bei Spannungseinbrüchen oder „Voltage Drops“ wechseln S1 und S2 automatisch in den sicheren Zustand.

6.7.1 Ergebnis

Die S1, S2 besitzen, für FR7, den Security Level SL-C2 sofern sich die Module in einem abschließbaren Maschineraum bzw. Schaltschrank befinden.

6.8 Gesamtergebnis S1,S2

Die S1, S2 können, unter den oben genannten Bedingungen einen SL-C Vector von {3,3,2,2,2,2,2} erreichen.

7 Contactorless Brake Module CBM1 / CBM2

In Anlehnung an die ISO8102-20 Security Anforderungen werden die CBM1 und CBM2 als Zugehörig zur Domäne „Safety“ betrachtet. Welche einen Security Level Vector von **SL-T** von {3,2,2,2,1,1,2} erfüllen soll.

7.1 FR1 Identifikation und Authentifizierungskontrolle SL-T 3

Die Module CBM1 und CBM2 besitzen keine Authentifizierung.
Alle Sicherheitsrelevanten Funktionen sind in Hardware ausgeführt.

Es können einige Parameter wie z.B. Bremsenspannung per (FST)Menü geändert werden.

Eine Änderung der oben genannten Parameter ist nur durch vor einen vor Ort befindliche berechtigte Person möglich.

7.1.1 Ergebnis

Die CBM1, CBM2 besitzen, für FR1, den Security Level SL-C3 sofern sich die Module in einem abschließbaren Maschineraum bzw. Schaltschrank befinden.

7.2 FR2 Nutzungskontrolle SL-T2

Es gelten die gleichen Regelungen wie in Punkt 6.1 Die Module CBM1 und CBM werden in einem abschließbaren Maschineraum, Schaltschrank eingebaut welcher nur durch berechtigten Person betreten werden kann.

Brake Module CBM1 und CBM2 sind in einem abschließbaren Maschineraum, Schaltschrank eingebaut welcher nur durch berechtigten Person betreten werden kann.

7.2.1 Ergebnis

Die CBM1, CBM2 besitzen, für FR2, den Security Level SL-C3 sofern sich die Module in einem abschließbaren Maschineraum bzw. Schaltschrank befinden.

7.3 FR3 Systemintegrität SL-T2

Die Software von CBM1 und CBM2 kann weder in Teilen noch komplett geändert werden.
Die Software hat keinen Einfluss auf die Sicherheitsfunktionalität.

7.3.1 Ergebnis

Die CBM1, CBM2 besitzen, für FR3, den Security Level SL-C3 sofern sich die Module in einem abschließbaren Maschineraum bzw. Schaltschrank befinden.

7.4 FR4 Datenvertraulichkeit SL-T2

Die Brake Module CBM1 und CBM2 speichern keine Personenbezogenen Daten.
Die Fehler-, Ereignislogs werden auf dem CAN Bus zur Verfügung gestellt.
Eine Manipulation der Daten hat keinen Effekt auf die Sicherheit und ist nur mit Expertenwissen sowie physischen Zugang möglich.

7.4.1 Ergebnis

Die CBM1, CBM2 besitzen, für FR4, den Security Level SL-C2 sofern sich die Module in einem abschließbaren Maschineraum bzw. Schaltschrank befinden.

7.5 FR5 Eingeschränkter Datenfluss SL-T1

Eine Manipulation der Daten z.B. über CAN- Bus ist nur mit Expertenwissen und physischem Zugang möglich.

7.5.1 Ergebnis

Die CBM1, CBM2 besitzen, für FR5, den Security Level SL-C2 sofern sich die Module in einem abschließbaren Maschineraum bzw. Schaltschrank befinden.

7.6 FR6 Rechtzeitige Reaktion auf Ereignisse SL-T1

Die Brake Module CBM1 und CBM2 übertragen Fehler und Ereignisse per CAN Bus.

Im Fehlerfall wir der „sichere“ Zustand eingenommen.

7.6.1 Ergebnis

Die CBM1, CBM2 besitzen, für FR6, den Security Level SL-C2 sofern sich die Module in einem abschließbaren Maschineraum bzw. Schaltschrank befinden.

7.7 FR7 Ressourcenverfügbarkeit SL-T2

Die Sicherheitsfunktionen in CBM1 und CBM2 sind unabhängig von der Kommunikation zu anderen Geräten (CAN BUS).
Bei Spannungseinbrüchen oder „Voltage Drops“ wechseln CBM1 und CBM2 automatisch in den sicheren Zustand.

7.7.1 Ergebnis

Die CBM1, CBM2 besitzen, für FR7, den Security Level SL-C2 sofern sich die Module in einem abschließbaren Maschineraum bzw. Schaltschrank befinden.

7.8 Gesamtergebnis CBM1, CBM2

Die CBM1, CBM2 können, unter den oben genannten Bedingungen einen SL-C Vector von {3,3,2,2,2,2,2} erreichen.

8 Aufzugssteuerungen SST, KST, EST

In Anlehnung an die ISO8102-20 Security Anforderungen wird die Aufzugssteuerung als Zugehörig zur Dömane „Notwendig“ betrachtet. Welche einen Security Level Vector von SL-T von {2,2,2,2,1,1,2} erfüllen soll.

8.1 FR1 Identifikation und Authentifizierungskontrolle SL-T 2

8.1.1 HMI

Die KST und EST besitzt einen mehrstufigen Passwortschutz über verschiedene Ebenen.
Die SST besitzt kein HMI.

Zusätzlich muss der Zugang, zu den zu den Steuerungen durch geeignete Maßnahmen wie abgeschlossener Maschinenraum und oder abgeschlossener Schaltschrank, für Unbefugte verwehrt werden.

8.1.2 RS232 Schnittstelle

Für eine Verbindung über die oben genannte Schnittstelle zu externen Geräten wird ein zusätzliches Modem benötigt welches ausschließlich eine „Peer to Peer“ Verbindung aufbauen kann.
Eine direkte Kommunikation von der Steuerung in das Internet findet nicht statt. Die SST Steuerung besitzt o.g. Schnittstelle nicht.

8.1.3 Ergebnis

Die SST, KST und EST besitzt, für FR1, den Security Level SL-C2.

8.2 FR2 Nutzungskontrolle SL-T2

8.2.1 HMI

Es gelten die gleichen Regelungen wie in Punkt 8.1.1 Die SST, KST und EST - Steuerung wird in einem abschließbaren Maschineraum, Schaltschrank eingebaut welcher nur durch berechtigten Person betreten werden kann.

8.2.2 RS232 Schnittstelle

Die Nutzungskontrolle unterliegt der Applikation auf die, die Steuerung zugreift.

8.2.3 Sonstige Schnittstellen

Keine.

8.2.4 Ergebnis

Die SST, KST und EST besitzt, für FR2, den Security Level SL-C2.

8.3 FR3 Systemintegrität SL-T2

8.3.1 HMI

Änderungen an der SST, KST und EST - Steuerungssoftware wie z.B. Software Updates sind nur durch Zugangsberechtigtes Personal und ein entsprechend vorbereiteten EEPROM möglich.

8.3.2 RS232 Schnittstelle

Änderungen der SST, KST und EST Steuerungssoftware ist über diese Schnittstellen nicht möglich.

8.3.3 Ergebnis

Die SST, KST und EST besitzt, für FR3, den Security Level SL-C2.

8.4 FR4 Datenvertraulichkeit SL-T1

Die SST, KST und EST - Steuerungen speichern keine Personenbezogenen Daten. Die Fehler-, Ereignislogs können nur durch Abfrage ausgelesen werden.

8.4.1 Ergebnis

Die SST, KST und EST besitzt, für FR4, den Security Level SL-C2.

8.5 FR5 Eingeschränkter Datenfluss SL-T1

Eine Manipulation der Daten z.B. über LON- oder CAN- Bus ist nicht möglich da serielle Bussysteme nicht vorhanden sind.

8.5.1 Ergebnis

Die SST, KST und EST besitzen für FR5, den Security Level SL-C2.

8.6 FR6 Rechtzeitige Reaktion auf Ereignisse SL-T1

Die SST, KST und EST -Steuerung erzeugt bei Fehlern oder Betriebsstörungen einen Fehlereintrag.

8.6.1 Ergebnis

Die SST, KST und EST besitzt, für FR5, den Security Level SL-C2.

8.7 FR7 Ressourcenverfügbarkeit SL-T2

8.7.1 SST,KST und EST – Steuerung

Sicherheitsfunktionen (Türüberbrückung) sind ausschließlich in der Hardware abgebildet und somit unabhängig von der Kommunikation innerhalb der Steuerungssoftware.

8.7.2 Ergebnis

Die SST,KST und EST -Steuerung besitzt, für FR5, den Security Level SL-C2.

8.8 Gesamtergebnis SST,KST und EST –Steuerung

Die SST, KST und EST -Steuerung kann, unter den oben genannten Bedingungen einen SL-C Vector von {2,2,2,2,2,2,2} erreichen.

9 Sicherheitssystem SA3-S

In Anlehnung an die ISO8102-20 Security Anforderungen wird das SA3-S als Zugehörig zur Domäne „Safety“ betrachtet. Welche einen Security Level Vector von SL-T von {3,2,2,2,1,1,2} erfüllen soll.

9.1 FR1 Identifikation und Authentifizierungskontrolle SL-T 3

Das SA3-S Module besitzen keine Authentifizierung, kein HMI und keine Parametereinstellmöglichkeit.

9.1.1 Ergebnis

Die SA3-S besitzen, für FR1, den Security Level SL-C3 sofern sich die Module in einem abschließbaren Maschineraum bzw. Schaltschrank befinden.

9.2 FR2 Nutzungskontrolle SL-T2

Es gelten die gleichen Regelungen wie in Punkt 9.1. Das Modul SA3-S wird in einem abschließbaren Maschineraum, Aufzugschacht oder Schaltschrank eingebaut welcher nur durch berechtigten Person betreten werden kann.

9.2.1 Ergebnis

Die SA3-S besitzen, für FR2, den Security Level SL-C3 sofern sich die Module in einem abschließbaren Maschineraum, Aufzugschacht bzw. Schaltschrank befindet.

9.3 FR3 Systemintegrität SL-T2

Die Software der SA3-S kann weder in Teilen noch komplett geändert werden. Das Gerät SA3-S überprüft die Korrektheit der Software anhand von Checksummen CRC.

9.3.1 Ergebnis

Die SA3-S besitzt, für FR3, den Security Level SL-C2.

9.4 FR4 Datenvertraulichkeit SL-T2

Die Sicherheitsmodule SA3-S speichert keine Personenbezogenen Daten. Die Fehler-, Ereignislogs werden auf eine USB-C Schnittstelle zur Verfügung gestellt. Eine Manipulation der Daten hat keinen Effekt auf die Sicherheit und ist nur mit Expertenwissen sowie physischen Zugang möglich.

9.4.1 Ergebnis

Die SA3-S besitzt, für FR4, den Security Level SL-C2 sofern sich die Module in einem abschließbaren Maschineraum, Aufzugschacht bzw. Schaltschrank befindet.

9.5 FR5 Eingeschränkter Datenfluss SL-T1

Eine Manipulation der Daten z.B. über USB-C ist nur mit Expertenwissen, Hersteller spezifischen Schnittstellenadapter und physischem Zugang möglich.

9.5.1 Ergebnis

Die SA3-S besitzt, für FR5, den Security Level SL-C2 sofern sich die Module in einem abschließbaren Maschineraum, Aufzugschacht bzw. Schaltschrank befindet.

9.6 FR6 Rechtzeitige Reaktion auf Ereignisse SL-T1

Das Sicherheitsmodule SA3-S überprüfen unabhängig die RAM (Random Access Memory) und den Programmspeicher. Im Fehlerfall wir der „sichere“ Zustand eingenommen.

9.6.1 Ergebnis

Die SA3-S besitzen, für FR6, den Security Level SL-C2.

9.7 FR7 Ressourcenverfügbarkeit SL-T2

Die Sicherheitsfunktionen der SA3-S ist unabhängig von der Kommunikation zu anderen Geräten, da keine Verbindung physisch besteht.
Bei Spannungseinbrüchen oder „Voltage Drops“ wechseln SA3-S automatisch in den sicheren Zustand.

9.7.1 Ergebnis

Die SA3-S besitzt, für FR7, den Security Level SL-C2 sofern sich das Modul in einem abschließbaren Maschineraum, Aufzugschacht bzw. Schaltschrank befindet.

9.8 Gesamtergebnis SA3-S

Die SA3-S kann, unter den oben genannten Bedingungen einen SL-C Vector von {3,3,2,2,2,2,2} erreichen.

Herstellerklärung Cybersicherheit

NEUE ELEKTRONISCHE WEGE

10 Gesamtübersicht

Herstellererklärung Cybersicherheit bezogen auf:

TRBS 1115-1
ISO8102-20
IEC62443-4

27.06.2024

Gesamtergebnisse:

Produkt	FR1 / SL-T	FR2 / SL-T	FR3 / SL-T	FR4 / SL-T	FR5 / SL-T	FR6 / SL-T	FR7 / SL-T	Grundsätzliche Anforderungen aus der ISO8102-20 erfüllt***
CBM**	3	3	2	2	2	2	2	**JA**
EST	2	2	2	2	2	2	2	**JA**
FST-(1)	2	2	2	2	2	2	2	**JA**
FST-2XT*	2	2	2	2	2	2	2	**JA**
FST-2XTs*	2	2	2	2	2	2	2	**JA**
FST-3	2	2	2	2	2	2	2	**JA**
KST	2	2	2	2	2	2	2	**JA**
S1	3	3	2	2	2	2	2	**JA**
S2	3	3	2	2	2	2	2	**JA**
SA3-S	3	3	2	2	2	2	2	**JA**
SST	2	2	2	2	2	2	2	**JA**

Die „Herstellerklärung Cybersicherheit – Produkte NEW LIFT“ ist unter dem Link https://www.newlift.de/downloads.html - „Bescheinigungen / Zertifikate“ abrufbar.

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

* FST-2/s inbegriffen
** CBM 1 und 2
*** Es sind die Voraussetzungen für die Teilergebnisse des jeweiligen Produktes zu beachten!