

Herstellerklärung-Cybersecurity

ISO 8102-20 & IEC 62443


LIMAX Safe

LIMAX Safe besteht aus der Auswerteeinheit "Safe Box" und dem sicheren Positionssensor "LIMAX33 RED" oder "LIMAX44 RED"

Herausgeber ELGO Batscale AG

Föhrenweg 20
FL-9496 Balzers

Technischer Support  +423 380 02 22

 +423 380 02 24

 support@elgo.li

Dokumenten- Nr. D-109855

Dokumenten- Name D-109855_51-23

Artikelnummer

Dokumenten- Revision Rev. 0

Ausgabedatum 19.12.2023

1 Präambel

Die ISO 8102-20 beschreibt die Umsetzung der IEC 62443 - Industrielle Kommunikationsnetze - IT-Sicherheit für Netze und Systeme auf Aufzüge, Rolltreppen und Fahrsteige.

Als Hersteller von Sicherheitskomponenten beschränkt sich unser Anwendungsbereich auf die IEC 62443-4. Dieses Dokument soll eine Hilfestellung für den System Integrator nach IEC 62443-3 darstellen.

2 Produktanforderungen

2.1 Funktionsbereiche IEC 62443

Die Funktionsbereiche werden nach IEC 62443 in vier Bereiche eingeteilt:

Bereich	Beschreibung	Beispiele
Essential	Essentielle Bereiche die die Verfügbarkeit der Anlage sicherstellen	Stockwerksindikator, Kabinenposition, Fahrriichtungserkennung
Safety	SIL gerichtete Sicherheitsfunktionen	Endschalter, Türüberbrückung
Alarm	Notfallfunktionen	Evakuierung, Notruf
Other	Andere Funktionen	Musik, Werbung, Infotainment

Table 1 Funktionsbereiche

2.2 Sicherheitslevel

Jeder Funktionsbereich hat einen Sicherheitslevel der mindestens erreicht werden muss (SL-T). Die IEC 62443 unterscheidet fünf Level:

Level	Beschreibung
0	Kein besonderer Schutz
1	Schutz vor unbeabsichtigten oder zufälligem Missbrauch
2	Schutz vor vorsätzlichem Missbrauch, ohne besondere Kenntnisse des Systems
3	Schutz vor vorsätzlichem Missbrauch, mit Fachkenntnissen und moderaten Ressourcen
4	Wie Level 3, jedoch mit umfangreichen Ressourcen und hoher Motivation

Table 2 Sicherheitslevel

Produkte die einen geringeren Sicherheitslevel (SL-C) implementieren, müssen durch geeignete Maßnahmen auf den Mindestlevel angehoben werden.

2.3 Grundanforderungen

Jeder Grundanforderung ist ein Mindestsicherheitslevel in Abhängigkeit des Funktionsbereiches zugeordnet.

Grundanforderung	Security level		
	Alarm	Essential	Safety
FR 1 – Identification and authentication	2	2	3
FR 2 – Use control	1	2	2
FR 3 – System integrity	1	2	2
FR 4 – Data confidentiality	1	2	2
FR 5 – Restricted data flow	1	1	1
FR 6 – Timely response to events	1	1	1
FR 7 – Resource availability	1	2	2

Table 3 Grundanforderungen

Im Folgenden werden die Sicherheitslevel im in IEC 62443-3-3:2013, A.3.3 beschriebenen Vektorformat dargestellt.

3 Schachtkopiersystem LIMAX Safe

Nach ISO 8102-20 hat der SIL-Bereich des Gerätes folgenden Sicherheitslevelvektor $SL-T(\text{Safety}) = \{3\ 2\ 2\ 2\ 1\ 1\ 2\}$, LIMAX Safe implementiert dabei einen $SL-C(\text{Safety}) = \{1\ 1\ 4\ 4\ 1\ 4\ 1\}$. Es müssen dementsprechend geeignete Maßnahmen getroffen werden.

3.1 FR1 – Identification and authentication – SL-T 3

LIMAX Safe unterstützt keine Authentifikationsmechanismen, jedoch verhindern mehrere Mechanismen das zufällige Verstellen der Parameter.

- Stockwerke lassen sich nicht im normalen Betriebsmodus lernen oder verändern
- Geschwindigkeitsparameter lassen sich nur während der Fertigung einstellen.
- Zur Türüberbrückung muss neben dem Stockwerk auch die passende Position übertragen werden.

Fazit: LIMAX Safe hat für FR1 einen SL-C von 1. Der Zugang zum CAN-Bus des LIMAX Safe muss durch geeignete Maßnahmen (z.B. verschlossener Schacht/Schaltschrank) verwehrt werden.

3.2 FR2 – Use control – SL-T 2

Da LIMAX Safe keine Authentifikationsmechanismen für Benutzer unterstützt, wird nicht weiter unterschieden und es gelten die gleichen Einschränkungen wie von FR1.

3.3 FR3 – System integrity – SL-T 2

Die Software in LIMAX Safe bietet keine Möglichkeit die Software als Ganzes oder in Teilen zu ändern. Sollten sich durch geeignete Maßnahmen doch Teile der Software (zufällig) ändern, erkennt die Systemsoftware von LIMAX Safe die Veränderung durch Prüfsummenchecks und quittiert die Funktion durch Öffnen aller zur Verfügung stehenden Aktoren (Safe Box) oder durch anfordern des sicheren Zustandes von über das Protokoll (LIMAX33/44 RED).

Fazit: LIMAX Safe hat für FR3 einen SL-C von 4. Eine Änderung ist nur mit Expertenwissen über die Interna des Gerätes in Kombination mit physischem Zugang zum Sensor möglich.

3.4 FR4 – Data confidentiality – SL-T 2

Die Sicherheitsparameter und Etagenpositionen sind durch eine Prüfsumme geschützt. Eine Änderung der Parameter ist nur während der Fertigung möglich. Die Etagenpositionen werden intern aus der physikalischen Position ermittelt und können nicht von außen eingestellt werden.

Zusätzlich speichert LIMAX Safe Fehlerereignisse in einem internen Log. Dieser Log ist über den CAN-Bus verfügbar. Die Daten werden selbst nicht weiter verarbeitet und nur auf Anfrage auf den Bus gesendet. Neben dem Löschen des kompletten Ereignislogs ist eine Manipulation der Daten nicht vorgesehen und hätte keinen Effekt außer der Datenkorruption. LIMAX Safe speichert weiterhin keine Komponenten- oder Personenbezogenen Daten.

Fazit: LIMAX Safe hat für FR4 einen SL-C von 4. Eine Änderung der Daten ist nur mit Expertenwissen über die Interna und einem physischen Zugang zum den Geräten möglich.

3.5 FR5 – Restricted data flow – SL-T 1

Der Datenfluss unterliegt keinen Einschränkungen. Es gelten die gleichen Einschränkungen wie von FR1.

3.6 FR6 – Timely response to events – SL-T 1

LIMAX Safe überwacht selbstständig den Arbeitsspeicher und den Programmspeicher. Bei Fehlern wird ein Log-Eintrag (siehe FR4) generiert.

Fazit: LIMAX Safe hat für FR6 einen SL-C von 4. Die Überwachung der Integrität wird innerhalb des Systems durchgeführt und kann von außen nicht manipuliert werden.

3.7 FR7 – Resource availability – SL-T 2

Die Sicherheitsfunktionen laufen unabhängig der Kommunikation zwischen Safe Box und Steuerung ab. Eine Busüberlastung schränkt die Systemfunktionalität nicht ein, lediglich die Position und Statusinformationen können für andere Busteilnehmer verloren gehen, bleiben aber intern erhalten. Die sichere Position zwischen Positionssensor und Safe Box wird über eine dedizierte Punkt-zu-Punkt-Verbindung ohne weitere Teilnehmer übertragen und kann nicht direkt beeinflusst werden.

Sollte die Systemspannung auf Notfallstromversorgung abfallen, so bleibt das System weiterhin ansprechbar und die Position wird weiterhin errechnet und auf dem Bus verfügbar gemacht. Lediglich die Aktorik wird abgeschaltet.

Fazit: Durch gezieltes Umschalten auf Notfallstromversorgung kann die Anlage lahmgelegt werden. LIMAX Safe erreicht somit für FR7 einen SL-C von 1. Für einen reibungslosen Betrieb muss der Zugang zur Stromversorgung durch geeignete Maßnahmen (z.B. verschlossener Schacht/Schaltschrank) verhindert werden.

4 Zusammenfassung

LIMAX Safe erreicht für sich alleine einen SL-C von {1 1 4 4 1 4 1}, kann aber mit einfachen Maßnahmen (kontrollierter Zugang zum CAN-Bus und der Stromversorgung) den geforderten SL-T von {3 2 2 2 1 1 2} problemlos erreichen. Somit kann zusammengefasst werden, dass von dem LIMAX Safe keine Gefährdung bezüglich Cybersecurity zu erwarten ist.

Document- No.: D-109855 / Rev. 0

Document- Name: D-109855_51-23

Änderungen und Irrtümer vorbehalten

© 2023, ELGO Batscale AG

ELGO Batscale AG

Messen | Steuern | Positionieren

Föhrenweg 20, FL-9496 Balzers

Tel.: +423 (0) 380 02 22, Fax.: +423 (0) 380 02 24

Internet: www.elgo.li, Mail: info@elgo.li

