

Herstellererklärung-Cybersicherheit ISO 8102-20 & IEC 62443

1.0 Prolog

Die Cybersecurity bedeutet festgelegte Steuerungsfunktionen an Aufzugsanlagen mit digital veränderbaren Elementen vor Cyberangriffen zu schützen. Die **ISO 8102-20**, in Verbindung mit der Industrienorm **IEC 62443**, sowie den Vorgaben aus der Betriebssicherheit **EmpBS 1115** „Cyber-Sicherheit von sicherheitsrelevanten MSR-Einrichtungen“ und der **preTRBS 15-1** verpflichtet zur Definition von Schutzzielen, um mit Hilfe von erforderlichen Maßnahmen ein Schutzniveau zu erreichen.

1.1 Die ISO 8102-20

1.1.1 Definition der Schutzziele

Laut Definition des Council of the European Union sollten Steuerungssysteme in der folgenden Art und Weise entwickelt und konstruiert werden:

Control systems shall be designed and constructed in such a way that:

(a) they can withstand, where appropriate to the circumstances and the risks, the intended operating stresses and intended and unintended external influences, including reasonably foreseeable malicious attempts from third parties leading to a hazardous situation:

Dies bedeutet, dass die EU-Kommission davon ausgeht, dass Manipulationsversuche zu erwarten sind, die als "allgemeinen Umweltfaktor" betrachtet werden können. Jedoch sind terroristische Angriffe, grenzüberschreitende Verbrechen von Organisationen und Handlungen kriegführender Nationen hiervon ausgenommen.

Die potentiellen Gefahren werden in zwei Kategorien eingeteilt, nämlich in die der Wirtschaftlichkeit und in die der Sicherheit.

Wirtschaftlichkeit:

- Verschlechterung der Wirtschaftlichkeit durch Manipulation resultierend in höhere Fahrintensität und Verschleiß.
- Einschränkung des Betriebs, Verminderung der Zuverlässigkeit und Verfügbarkeit.

Sicherheit:

- Manipulation der passiven Sicherheit, z.B. Verfügbarkeit des Notrufsystems.
- Manipulation von Sicherheitskomponenten, wie z.B. Gefahren durch Stufenbildung bei Schachtkopierungssystemen.

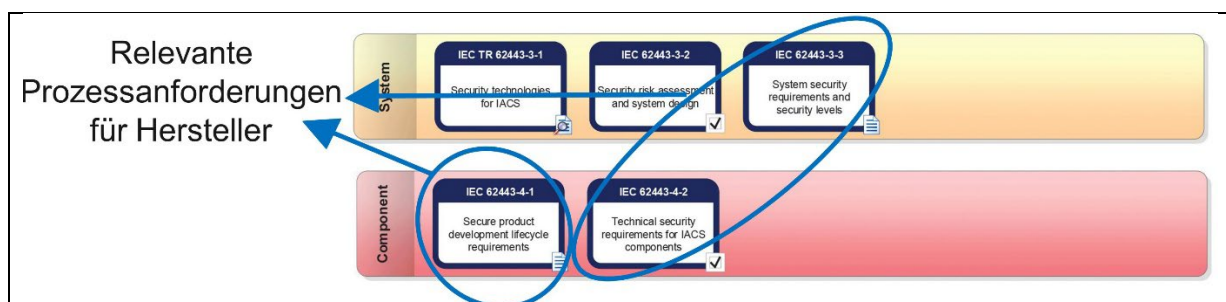
Die Vermeidung dieser Gefahren sind die Schutzziele, die zu erreichen sind.

1.1.2 Anwendung der ISO 8102-20 in Verbindung mit der IEC 62443

Um die gesetzten Schutzziele zu erreichen, ist die Norm ISO 8102-20 erschaffen worden. Beim Studium des Inhaltes erkennt man, dass die ISO sich auf die weithin akzeptierte Industrienorm für operative Technologie (OT), der IEC 62443 stützt. Die IEC 62443 ist der Industriestandard für industrielle Automatisierungs- und Steuerungssysteme. Sie deckt folgende Ziele ab:

- Definition der Prozessanforderungen (Secure Development Lifecycle) und dem Reifegrad
- Definition der Produkthanforderungen (System- und Komponentenanforderungen) und der Sicherheitsstufen.

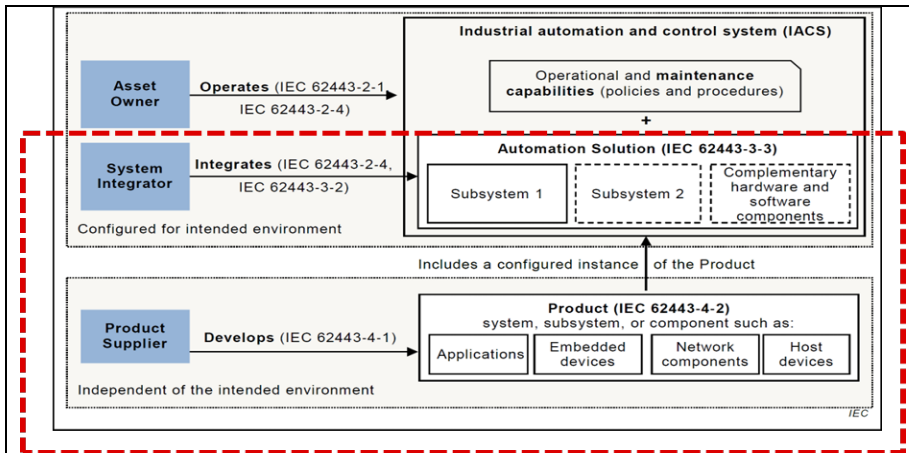
Die Definition der Sicherheitsstufen für die Funktionen und deren Schnittstellen erfolgt in der ISO 8102-20. Da die IEC 62443 auch den Asset Owner mit einbezieht, kann für die Hersteller der Kreis der wichtigen Normen eingegrenzt werden:



Quellenverweis: | © Schindler 2023 | We Elevate |

1.2 ISO 8102-20 Kapitel 1 Anwendungsbereich

Beim Kapitel 1 müssen wir als Komponenten-Hersteller ganz klar den Anwendungsbereich abgrenzen. Hierbei hilft uns wieder die Norm der ISO 62443:



Unser Anwendungsbereich:	Außerhalb des Anwendungsbereiches:
Sicherheits-, Essentiell- und Alarmfunktionen Lebenszyklus der Installation Permanente oder temporäre Konnektivität Rolle des Produktlieferanten Informationen für den Eigentümer/Betreiber	Weiterführende Funktionen am Aufzug Rolle des Systemsintegrators Rolle des Eigentümers / Betreibers Externe Systeme

1.3 ISO 8102-20 Kapitel 2 Normative Referenzen

Für Aufzüge wird der Kontext der ISO 8100-1:2019 (identisch mit der EN 81-20:2020) referenziert.

1.4 ISO 8102-20 Kapitel 3 Begriffe und Definitionen

Kapitel 3 listet die verwendeten Begriffe und ihre Definitionen. Für uns entscheidend ist die Definition des Begriffes der Cybersicherheit und deren Verweis auf die IEC 62443:

Cybersecurity	Measures taken to protect a computer or computer system against unauthorized access or attack (aus IEC 62443-3-2)
---------------	---

1.5 ISO 8102-20 Kapitel 4 Prozessanforderungen

In der IEC 62443, welche der Industriestandard für industrielle Automatisierungs- und Steuerungssysteme (OT) darstellt, sind die Prozessanforderungen der ISO 8102-20 Kapitel 4 definiert. Es handelt sich hierbei um den Lebenszyklus der Prozesse (Secure Development Lifecycle) und dem Prozess-Reifegrad.

1.5.1 Reifegrad für Prozesse IEC 62443

Stufe	Definition
1 Initial	Produktlieferanten führen die Produktentwicklung in der Regel ad hoc und oft undokumentiert (oder nicht vollständig dokumentiert) durch.
2 Managed	Produktlieferant ist in der Lage die Entwicklung eines Produkts gemäß den schriftlichen Richtlinien (einschließlich Zielen) zu verwalten. Der Produktlieferant verfügt auch über Nachweise dafür, dass das Personal geschult ist, über das Fachwissen verfügt und die Prozess befolgt. Die Prozesse sind wiederholbar.
3 Defined (Practiced)	Der Prozess ist in der gesamten Organisation des Lieferanten wiederholbar. Die Prozesse wurden praktiziert, und es gibt Beweise, die zeigen, dass dies geschehen ist.
4 Improving	Anhand geeigneter Prozessmetriken kontrollieren Produktlieferanten die Wirksamkeit des Prozesses und zeigen eine kontinuierliche Verbesserung in diesen Bereichen.

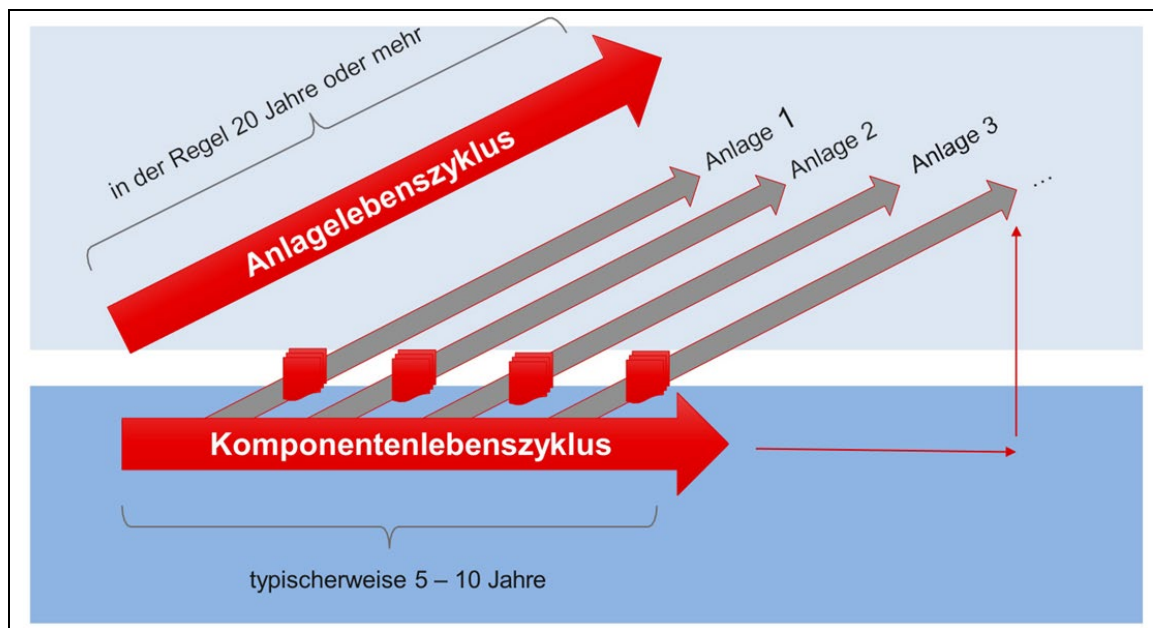
Quellenverweis: | © Schindler 2023 | We Elevate |

Fazit: Die KW Aufzugstechnik GmbH ist seit Jahrzehnten nach dem Qualitätsstandard ISO 9001:1996 bzw. ISO 9001:2015 zertifiziert. Alle Bereiche des Unternehmens, wie auch die Entwicklung werden jährlich auditiert. Alle Prozesse sind in dem PBs (Prozessbeschreibungen), beschrieben, kontrollierbar, multizierbar und der KV (Kontinuierlichen Verbesserung) unterworfen. Laut der Tabelle der IEC 62443 befinden wir uns auf der Stufe 4, dem Improved Process.

Siehe auch Anhang A – Zertifikat ISO 9001:2015 – KW Aufzugstechnik GmbH

1.5.2 Lebenszyklus der Prozesse

Sowohl der Anlage-, als auch der Komponentenlebenszyklus müssen bei der Umsetzung der Cybersicherheitsanforderungen berücksichtigt werden. Für uns als Komponentenhersteller ist der Lebenszyklus der Komponenten entscheidend. Dank der Datenanalyse der Firma Schindler stehen uns verlässliche Aussagen zum Komponentenlebenszyklus zur Verfügung:



Quellenverweis: | © Schindler 2023 | We Elevate |

Fazit: Die KW Aufzugstechnik GmbH ist als Hersteller von Sicherheitsbauteilen verpflichtet, einen Random Check (Stichprobenprüfung) durch einen Notified Body (Zertifizierte Prüforganisation) durchführen zu lassen. Da wir als einer der wenigen Hersteller Steuerungs- und Regelgeräte mit funktionaler Sicherheit herstellen, haben wir erhöhte Anforderungen an unsere Fertigungsprozesse. Dieser Qualitätsvorsprung manifestiert sich in unseren Produkten und den jährlichen Prüfungsergebnissen.

Siehe auch Anhang B – Zertifikat Random Check – KW Aufzugstechnik GmbH

1.6 ISO 8102-20 Kapitel 5 Produktanforderungen

Die IEC 62443-3-3:2013 und IEC 62443-4-2:2019 stellen die Basis dar für die Sicherheitsanforderungen an das Produkt. Die ISO 8102-20 wiederum schafft die Verbindung zur Aufzugswelt und stellt anhand von Tabellen die Einteilung von Funktionen und Sicherheitsstufen und deren Gewichtung in Bezug zu den technischen Grundanforderungen dar.

1.6.1 Funktionsbereiche und Sicherheitsstufen IEC 62443

In der ISO 8102-20 finden wir unter Kapitel 5.3 die Klassifizierung der einzelnen Aufzugsfunktionen nach ihrer Wichtigkeit (Sicherheitsstufe). Alle elektrischen und softwarebasierten Sil-Funktionen fallen in die wichtigste Kategorie Safety (Sicherheit).

Bereich	Beschreibung	Beispiele
Safety Sicherheit	SIL-rated control functions.	SIL-rated electric safety devices and electrical protective devices, SIL-rated motor and brake control functions
Essential Essentiell	Function or capability that is required to ensure the availability of the lift , escalator or moving walk, and its compliance to safety regulations , and which do not belong to Safety or Alarm function domains.	Normal control, Car and landing call devices and indicators, Access control, Energy saving (car light, ventilation, etc.) Hoisting machine motor control Door control including its protective devices, Load control, Run time limiter Fire service operation, Return to normal operation of the lift, Re-opening of the door Remote monitoring and interaction
Alarm	Devices used to verify entrapment, to call for help and to rescue passengers in case of entrapment.	Alarm, intercom and video devices Emergency supply Evacuation device Displays and voice announcements used for rescue

Tabelle 1 – ISO 8102-10 Kap.5.3 Domains of the EUC functions

Diese Funktionen, welche den drei Sicherheitsstufen zugeordnet wurden, werden nun nochmal gewichtet in drei Stufen

Gewichtung	
Stufe 1	Normale Anforderungen
Stufe 2	Höhere Anforderungen, die ein Fachwissen erfordern
Stufe 3	Höchste Anforderungen, die eine Verschlüsselung von Hard- und Software erforderlich machen

in Bezug auf 7 grundlegende technische Grundanforderungen:

Foundational requirement	Security level		
	Alarm	Essential	Safety
FR 1 – Identification and authentication control	1	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

Tabelle 2 – ISO 8102-10 Kap.5.4 Security level vectors for EUC function domains

Wie wir unschwer erkennen können haben die Sicherheitsfunktionen in Bezug auf die technische Anforderung FR 1- Identifikation und Authentifizierungs-Kontrolle die höchsten Anforderungen. Im folgendem haben wir die Remote- und die Geräte der Funktionalen-Sicherheit im einzelnen untersucht.

1.6.2 Bewertung der Sicherheitsanforderungen – Remote Control - Fernzugriff über KWeb

KWEB ist ein von KW entwickeltes Cloud-System zur Fernüberwachung von Aufzugsanlagen. Da es sich bei KWEB um eine eigene Entwicklung handelt, kann die Sicherheit von der Hardware, bis zur Software komplett von uns gewährleistet werden. In diesem Dokument werden die wichtigsten Aspekte der Cyber-Sicherheit von KWEB erläutert und wie die KW Aufzugstechnik GmbH sicherstellt, dass ihre Daten und Systeme geschützt sind.

Schutz vor Injection und Request Forgery Angriffen

Das Cloud-System KWEB wird durch Content Security Policy (CSP) vor Data-Injection und Cross-Site Scripting Angriffen geschützt. Die CSP verhindern unter anderem, dass Skripte und andere Inhalte aus nicht vorgesehenen Quellen geladen werden können. Ebenso lässt sich damit sicherstellen, dass alle Inhalt und Verbindungen über verschlüsselte Protokolle (HTTPS) abgerufen werden.

Durch XSRF Tokens werden Cross-Site Request Forgery Angriffe verhindert. Dies ist essentiell um ungewollte unautorisierte Befehle zu verhindern, die jedoch von autorisierten Benutzern kommen. Ohne die Verwendung von XSRF Tokens, bzw. anderen Techniken zur Minimierung von XSRF Angriffen, könnte beispielsweise durch das versehentlich anklicken eines Links, Befehle im Cloud Service ausgeführt werden. Solche Angriffe werden hierbei vollständig abgefangen.

Verbindungsverschlüsselung

Ein weiterer wichtiger Aspekt der Cyber-Sicherheit ist die Verschlüsselung der übertragenen Daten. KWEB verwendet TLS 1.3 sowohl für die Verschlüsselung des Datenverkehrs zwischen dem Benutzer (Webbrowser) und dem Webserver via HTTPS, sowie für die Verbindung zwischen Gateway und Cloud-System. TLS 1.3 ist hierbei die aktuellste und sicherste Version des verbreiteten Protokolls zur Absicherung der Transportschicht. Unterstützte Algorithmen zur Authentifizierung, Schlüsselaustausch und Verschlüsselung beschränken sich hierbei ausschließlich auf moderne und sichere Verfahren wie RSA, ECDHE, ECDSA, AES, CHACHA20 mit Schlüssellängen von mindestens 128 Bit für symmetrische, sowie 2048 Bit für asymmetrische Verschlüsselung. Dies schützt sämtliche Daten zuverlässig vor unautorisiertem Zugriff während der Übertragung und verhindert durch die bei TLS verwendeten Zertifikate Man-in-the-Middle Angriffe. Damit ist FR 1 (Identification and authentication control) erfüllt.

Zugangskontrolle

Zugriffskontrollen sind auch von entscheidender Bedeutung für die Sicherheit von Cloud-Systemen. KWEB verwendet eine rollenbasierte Zugriffskontrolle, um sicherzustellen, dass Benutzer nur auf die zugewiesenen Anlagen zugreifen können, die für ihre Rolle relevant sind. Jeder Benutzer erhält nur die notwendigen Berechtigungen, um seine Arbeit zu erledigen, wodurch hier das Minimalprinzip umgesetzt wird.

Systemdesign

Der Verbindung des Gateways zum Cloud-Server erfolgt ausschließlich von Gateway zum Server. Das Gateway bietet keine Möglichkeit um eingehende Verbindung anzunehmen. Das Ausführen von Befehlen auf dem Gateway ist vom Cloud-Server aus und somit nur durch die KWEB -Oberfläche möglich. Es erfolgt bei jeder Eingabe bei KWEB eine Überprüfung auf Plausibilität und Zugriffsberechtigung.

Backup und Recovery

Ein weiterer wichtiger Aspekt der Cyber-Sicherheit ist die Datensicherung und Wiederherstellung. KW Aufzugstechnik GmbH sichert regelmäßig alle Daten auf KWEB und stellt sicher, dass eine Wiederherstellung im Falle eines Ausfalls möglich ist. Durch regelmäßige Backups werden Datenverluste minimiert, falls ein Fehler auftritt.

Datenschutz

Von KWEB werden ausschließlich Maschinendaten erfasst, welche nicht zu einzelnen Personen zugeordnet sind. Im Bezug auf Nutzerdaten speichert KWEB ausschließlich die benötigten Daten zur Authentifizierung wie Anmeldename, Email-Adresse und Passwort. Die Passwörter werden zu keinem Zeitpunkt im Klartext gespeichert, sondern es werden lediglich die dazugehörigen Hashwerte abgelegt. Hierbei kommt die das bewährte Bcrypt Verfahren zum Einsatz, das eine speziell auf das sichere Speichern von Passwörtern ausgelegte Hashfunktion bietet. Dabei wird neben dem reinen Hashen, wie bei Bcrypt vorgesehen, auch ein zufälliger Salt verwendet. Dies verhindert offline Angriffe auf die gespeicherten Passwörter mittels Rainbow Tables und erhöht die Sicherheit auch in weiteren Aspekten.

1.6.3 Bewertung der Sicherheitsanforderungen – SIL Brake Control Function BG-90

Unser schützloses Bremsgerät BG-90 ist eine Komponente der Funktionalen-Sicherheit. Es stellt so zu sagen die höchste Sicherheitsform dar, nämlich die Eigensicherheit. Der Sicherheitskreis stellt den Energiefluß ohne dazwischen liegende Schaltglieder zum Öffnen der Bremse zur Verfügung. Eine Unterbrechung der Sicherheitskette an irgend einer Stelle führt zwangsläufig zum Abfall der Bremseinrichtung. Aus der Ferne ist der Prozess nicht manipulierbar, sondern erfordert vor Ort, im Schacht oder im Schaltschrank eine manuelle Zerstörung. Damit ist FR 1 (Identification and authentication control) erfüllt.

1.6.4 Bewertung der Sicherheitsanforderungen – SIL Motor Control Function GOLIATH-90

Unser schützloser Frequenzumrichter GOLIATG-90 ist eine Komponente der Funktionalen-Sicherheit. Es stellt so zu sagen die höchste Sicherheitsform dar, nämlich die Eigensicherheit. Der Sicherheitskreis stellt den Energiefluß ohne dazwischen liegende Schaltglieder zum Betrieb der Treiberstufe der Leistungshalbleiter zur Verfügung. Eine Unterbrechung der Sicherheitskette an irgend einer Stelle führt zwangsläufig zum Abfall der Bestromung des Antriebsmotors. Aus der Ferne ist der Prozess nicht manipulierbar, sondern erfordert vor Ort, im Schacht oder im Schaltschrank eine manuelle Zerstörung. Damit ist FR 1 (Identification and authentication control) erfüllt.

1.6.5 Bewertung der Sicherheitsanforderungen – SIL Shaft-Copy ELGO LIMAX CP-33

Das SIL-3 Schachtkopierungssystem LIMAX CP33 der Firma ELGO wird von uns hauptsächlich als Kopierung eingesetzt. Da es sich um eine Komponente der Funktionalen-Sicherheit handelt, muss sie im Rahmen einer Sicherheitsbewertung untersucht werden. Die Lage der Haltestellen Und Sicherheitsschalter erfolgt bei der Inbetriebnahme des Aufzuges vor Ort im Schacht. Auch eine Änderung dieser Werte kann nur vor Ort durch einen erneuten Teach-In-Vorgang erfolgen Eine Manipulation der Sicherheitsfunktion aus der Ferne ist daher auszuschließen. Theoretisch wäre es möglich, die Schachtkopierung durch andauerndes Senden von Anfragen auf dem CANOpen-Bus zu stören. Dies ist aber nahezu auszuschließen, da der CANOpen-Bus für die Kopierung nur auf dem Fahrkorb zur Verfügung steht. Eine **Injection** mit Schadprogrammen auf dem Fahrkorbrechners, bzw. dem Zentralrechner ist zu 100% auszuschließen, da das Steuersystem keine Betriebssystemebene hat, sondern sehr systemnah als Maschinensprache im Mikroprozessor verankert ist. Damit ist FR 1 (Identification and authentication control) erfüllt.

1.6.6 Kompensierende Gegenmaßnahmen laut ISO 8102-20 Annex A

Die im Anhang Annex A 3.9 der ISO 8102-20 definierten Maßnahmen können für das in 4.3.2 geforderte Bedrohungsmodell berücksichtigt werden, wie z.B. physische Zugangsbeschränkung, Zugang nur für autorisierte Personen, Spezialschlüssel zur Notentriegelung, verriegelte Schrank- oder Revisionstüren...

Die Abschwächung der kompensierender Gegenmaßnahmen werden in den folgenden Beispiele veranschaulicht:

A.3.9.2 Nummer zum Fern-Notruf / WLAN Zugriff

Aufzüge, die nach ISO 8100-1:2019, 5.12.3.1 konstruiert sind, müssen über ein Fernnotrufsystem verfügen. Ein unkontrollierter Zugang zur Änderung der Alarmrufnummer ist nicht akzeptabel. Ein verschlossener Maschinenraum oder verschlossener Schrank, zu dem nur befugte Personen Zugang haben, reicht aus, um SL1 für FR 1 (Identifizierungs- und Authentifizierungskontrolle) zu erreichen.

Für den WLAN-Zugriff auf unsere Steuerungen gilt die gleiche Verfahrensweise. Es gibt kein Master Codewort zum Zugriff auf die Steuerungen. Jede Steuerung hat ihr eigenes einzigartiges Codewort, welches in den Unterlagen im verschlossenen Schaltschrank zu finden ist.

A.3.9.3 Sicherheitskreis

Aufzüge, die nach ISO 8100-1 konstruiert sind, haben einen Sicherheitskreis. Ein verschlossener Schrank oder verschlossener Maschinenraum verhindert einen direkten Zugriff auf die Sicherheitskreiskette. Dies reicht aus, um SL2 für FR 3 (Systemintegrität) und die Erfüllung von FR 4 (Datenvertraulichkeit).

A.3.9.4 Firmware update

Die Fähigkeit, die Software oder Firmware sicher zu aktualisieren, ist eine wichtige Funktion und für alle EUC-Funktionsbereiche von Bedeutung. Kompensierende Gegenmaßnahmen, wie z. B. ein verschlossener Schrank oder verschlossener Maschinenraum, können das Risiko weiter verringern und können daher verwendet werden, um gleichwertige Sicherheitskontrollen zu ersetzen, die erforderlich sind, um die den verschiedenen Sicherheitsstufen entsprechenden Sicherheitsanforderungen zu erfüllen.

1.7 ISO 8102-20 Kapitel 6 Benutzerinformation - Cloudanforderungen

Der Zweck der Benutzerinformation ist es, den Betreibern, Eigentümern, Instandhaltern und anderen Beteiligten die Informationen zur Verfügung zu stellen, die für die Erreichung und Aufrechterhaltung der Sicherheit nötig sind. In Bezug auf unser Cloud-System KWEB geben wir die Benutzerinformationen weiter, mit dem Ziel die Sicherheit zu gewährleisten.

Das Cloud-System KWEB wird bei der Firma Hetzner, einem Webhosting Unternehmen mit Standort Deutschland gehostet. Die Maßnahmen für die Sicherheit, wie Firewall-Systeme, automatisierter DDoS-Schutz und Sicherheitsupdates sichern den Server vor Angriffen aus dem Internet ab. Das Unternehmen ist zertifiziert nach ISO / IEC 27001:2013

Siehe auch Anhang C – Zertifikat IEC 27001:2013 – Hetzner Online GmbH



Management Service

ZERTIFIKAT

Die Zertifizierungsstelle
der TÜV SÜD Management Service GmbH

bescheinigt, dass das Unternehmen

KW Aufzugstechnik GmbH
Zimmersmühlenweg 69
61440 Oberursel
Deutschland

für den Geltungsbereich

**Beratung, Projektierung, Entwicklung und Fertigung von
Aufzugssteuerungen, Frequenzumrichtern und
elektronischen Aufzugskomponenten**

ein Qualitätsmanagementsystem
eingeführt hat und anwendet.

Durch ein Audit, Auftrags-Nr. **70772354**,
wurde der Nachweis erbracht, dass die Forderungen der

DIN EN ISO 9001:2015

erfüllt sind.

Dieses Zertifikat ist gültig vom **19.12.2022** bis **18.12.2025**.

Zertifikat-Registrier-Nr.: **12 100 39815 TMS**.

Leiter der Zertifizierungsstelle
München, 25.11.2022



ZERTIFIKAT ◆ CERTIFICATE ◆ 認證書 ◆ CERTIFICADO ◆ CERTIFICAT



Report of random check

Lifts Directive 2014/33/EU

Report belonging to certificate of conformity to type number : NL22-400-1002-170-RC01
Date of issue : 17-10-2022
Revision number / date : -
Subject : Random check of safety component
Requirements : Lifts Directive 2014/33/EU
Date of random check : 13-09-2022
Random check performed by : A. Santoe & W. Bijlsma
Project number : P220176

1. Related EU-type examination certificates

Name and address certificate holder : KW-Aufzugstechnik GmbH
Zimmersmühlenweg 69
61440 Oberursel, Germany
Name and address of manufacturer : KW-Aufzugstechnik GmbH
Zimmersmühlenweg 69
61440 Oberursel, Germany

Product description	Type	EU-type examination certificate no.	Rev. no.	Date of issue
Frequency inverters for elevator drives without contactors	SAS16 + GOLIATH-90	NL16-400-1002-170-03	1	25-10-2021



2. Description of safety component

To provide state of the art stopping accuracy for lifts, inverters are more and more used. Today drive manufacturers provide inverters with safe torque off (STO) functionality. This means basically that the safety circuit of the lift is directly controlling the information to the drive if torque to the motor is allowed. Motor power contactors are not necessary anymore.

To be able to do this the drive manufacturer have to follow a process to prove that the safety and the reliability of this function is in accordance with the current state of the art.

With the SAS function (safe off output) the GOLIATH-90 inverter series can be used in lift applications without the need of main contactors. The device can drive synchronous and asynchronous motors with nominal current from 12 Ampere to 162 Ampere. The SAS function provides the power to the semi-conductors controlling the frequency generator for the AC supply to the motor. The energy for powering the IGBT's is provided by the safety circuit of the lift. This allows an inherent safe circuit; when the safety circuit of the lift is opened the IGBT's cannot be powered anymore.

The safety circuit SAS16-102 replaces the main contactors at the end of the safety circuit. The safety circuit powers the primary winding of the transformer TR4 (J1a, J1b). The secondary winding of the transformer (J3a, J3b) provides with 400 VAC the control power of the IGBT's of the inverter.

Since the galvanic isolated drive stage of the inverter needs a voltage of 400 VAC at the terminals LSAS1 and LSAS2 to control the drive stages of the IGBT's, it is ensured that the voltage supply for gate control of the IGBTs T1 / T2 / T3 of the inverter is switched off and T1 / T2 / T3 cannot be controlled if the safety circuit is interrupted. In that case no torque can be generated for the motor.

The inputs of the drive are monitored to check if the power is removed at standstill of the lift. From SAS16 a monitoring output is provided for the controller.

Further properties and conditions are given in the EU-type examination certificate.



3. Examinations and Tests

A sample of ready safety components was randomly taken at the manufacturers premises. The following examinations and tests (where applicable) were carried out:

1. Examination of the measures carried out by the manufacturer, to ensure the continuous conformity of the ready safety component with the applicable EU-type examination certificate in the following areas:
 - Material procurement
 - Receipt of goods
 - Production
 - Assembly
 - Finish adjustment and functional tests
 - Documentation
2. Inspection of quality records and test records
3. Comparison of the current drawings – especially drawings for the production – with the EU-type certified documentation.
4. Comparison of a safety component randomly taken out of the production with the EU-type certified documentation, to check validity of material specification, drawings and parts list.
5. Comparison of components with the basis of examination.
6. Performance of a functional test.

4. Results of the random check

The checked safety component mentioned under chapter 1 was found in compliance with the technical documentation. The safety component passed the performed tests.

5. Conclusions

Liftinstituut BV declares, based on the results of the random check, that the examined safety component is in conformity with the EU-type certified safety component and issues the certificate of conformity to type.



liftinstituut
SINCE 1933



6. CE marking

Each safety component that is in conformity with the EU-type certified safety component mentioned under chapter 1 shall be CE-marked according to annex IX pt. 5 of the Lifts Directive 2014/33/EU under consideration that conformity with eventually other applicable Directives is proven.

Following annex IX pt.5 of the Directive, the CE-marking shall be accompanied by the Notified Body identification number no. 0400 of Liftinstituut B.V.

7. Intervals of the random check

The next random check shall be carried out within the applicable interval, with the aim to keep the right to apply the Notified Body identification number 0400 of Liftinstituut BV. Unless otherwise agreed the interval of the random checks is yearly.

Prepared by:

Azaad Santoe
Product specialist Certification

Certification decision by:



Annex

Annex 1. Revision of the certificate and its report

Rev.:	Date	Summary of revision
-	17-10-2022	Original



ZERTIFIKAT

HETZNER

SOCOTEC Certification Deutschland GmbH bescheinigt hiermit, dass das Informationssicherheitsmanagementsystem des Antragstellers

**Hetzner Online GmbH
Industriestraße 25
D-91710 Gunzenhausen**

im Geltungsbereich

"Der Anwendungsbereich des Informationssicherheitsmanagementsystems umfasst alle Hosting-Dienstleistungen und die Rechenzentren der Hetzner Online GmbH."

auf Grundlage des Statement of Applicability in der Version 4.1 die Anforderungen des folgenden Regelwerks erfüllt:

ISO/IEC 27001:2022

Im Zertifizierungsaudit konnten Nachweise vorgelegt werden, die die Erfüllung der Anforderungen belegten.

Statement of Applicability(SoA):	Version 4.1 datiert 09.07.2025
Zertifizierungsentscheidung:	18.09.2025
Ausgestellt am:	18.09.2025
Gültigkeit Zertifikat:	27.09.2025 - 26.09.2028
Zertifikatsnummer:	ZN-2025-35 v1.0

SOCOTEC Certification
Deutschland GmbH
Graf-Dürkheim-Straße 3
87642 Halblech

Zertifizierungsstelle





ZERTIFIKATSANHANG

Standort 1:

Hetzner Online GmbH
Sigmundstraße 135 90431
Nürnberg
Deutschland

Standort 2:

Hetzner Online GmbH
Am Datacenter-Park 1 08223
Falkenstein/Vogtland
Deutschland

Standort 3:

Hetzner Online GmbH
Huurrekuja 10
04360 Tuusula
Finnland