Herstellererklärung Cybersecurity

Schneider Steuerungstechnik

Allgemeine Anforderungen, Normen:

Durch den Einsatz von IT-basierten Technologien und steigendem Vernetzungsgrad können sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen zum Ziel von Manipulationen werden, soweit deren Informationstechnik durch Cyber-Bedrohungen kompromittiert werden kann.

Sicherheitsrelevante MSR-Einrichtungen müssen gemäß TRBS 1115-1 nach dem Stand der Technik vor Cyber-Bedrohungen geschützt sein, so dass Gefährdungen von Personen bei überwachungsbedürftigen Anlagen vermieden werden.

Zur Abwehr der Gefährdung durch Cyber-Bedrohungen werden für die LiSA-Aufzugssteuerungen der Firma Schneider Steuerungstechnik die Richtlinen der ISO 8102-20 herangezogen.

Dabei sind für die Firma Schneider Steuerungstechnik als Komponentenhersteller insbesondere die IEC 62443 Teil 4-1 und 4-2 relevant.

Grundanforderungen:

In folgender Tabelle sind die Grundanforderungen FR 1 - FR 7 dargestellt, welchen jeweils die Sicherheitsrelevanten Funktionsbereiche mit dem erforderlichen Mindest-Sicherheitslevel zugeordnet sind.

Grundanforderungen	Mindest-Sicherheitslevel		
	Alarm	Essential	Safety
FR 1 - Identification and authentication control / Identifizierung und Authentifikation	1	2	3
FR 2 - Use control / Nutzungskontrolle	1	2	2
FR 3 - System integrity / Systemintegrität	1	2	2
FR 4 - Data confidentiality / Vertraulichkeit der Daten	1	2	2
FR 5 - Restricted data flow / Eingeschränkter Datenfluss	1	1	1
FR 6 - Timely response to events / Rechtzeitige Reaktion	1	1	1
FR 7 - Resource availability / Verfügbarkeit der Ressourcen	1	2	2

Sicherheitslevel:

Level	Beschreibung
0	Kein besonderer Schutz
1	Schutz vor unbeabsichtigtem oder zufälligem Missbrauch
2	Schutz vor vorsätzlichem Missbrauch, ohne besondere Kenntnisse des Systems
3	Schutz vor vorsätzlichem Missbrauch, mit Fachkenntnissen und moderaten Ressourcen

Sicherheitsrelevante Funktionsbereiche:

Die Sicherheitsrelevanten Teile einer Aufzugssteuerung werden nach IEC 62443 in verschiedene Bereiche eingeteilt.

Safety: Umfasst Einrichtungen die für die Auslösung der Sicherheitsfunktion zwingend erforderlich sind.

- Steuerrechner (LiSA)
- Sicherheitsschaltung zur Türüberbrückung
- Aktoren und Sensoren zur Schachtkopierung.

Essential: Ist die erweiterte Sicherheitsrelevante Einrichtung. Diese umfasst die Komponenten die nicht zur Auslösung der Sicherheitsfunktion notwendig sind, aber die Verfügbarkeit der Anlage sicherstellen.

- Bedien und Visualisierungseinrichtungen (Handterminal)
- Ein- und Ausgabebaugruppen (I/O-Module)

Alarm: Umfasst weitere Einrichtungen welche nicht zur Auslösung der Sicherheitsfunktion notwendig sind, aber unter Umständen diese Einrichtungen beeinflussen können.

- Notbefreiungseinrichtung
- Notruf
- Fernwartungseinrichtungen

Die Umgebung umfasst noch weitere Komponenten die in Verbindung mit der Steuerung stehen aber weder direkt noch indirekt der Sicherheitsrelevanten Einrichtung zuzuordnen sind (Other).

Schutzmassnahmen:

Zu den Grundanforderungen FR 1 - FR-7 zur Sicherheit vor Manipulationen durch Cyber-Bedrohungen an den Sicherheitsrelevanten Teilen der Steuerung sind im Folgenden die Gegebenheiten und die Schutzmassnahmen ausgeführt.

FR 1 - Identifizierung und Authentifikation

Die LiSA-Steuerung unterstützt keine Authentifikationsmechanismen. Änderungen an der Software und den Betriebsparametern sind nur direkt an der Steuerung möglich

- Der Zugang zu Steuerung muss durch geeignete Maßnahmen (z.B. verschlossener Maschinenraum, abgeschlossenern Schaltschrank) für Unbefugte verwehrt werden.
- Der Zugang zum CAN-BUS muss ebenfalls für Unbefugte verwehrt werden.

FR 2 - Nutzungskontrolle

Es gelten die gleichen Einschränkungen wie bei FR 1

- Die LiSA-Steuerung wird in einem abschließbaren Schaltschrank eingebaut welcher nur für Berechtigte Personen zugänglich ist.

FR 3 - Systemintegrität

- Änderungen an der Betriebssoftware wie z.B. updates sind nur durch Zugangsberechtigtes Fachpersonal und nur direkt an der Steuerung unter Anschluss eines entsprechend vorbereiteten Speichermediums möglichmöglich.

FR 4 - Vertraulichkeit der Daten

- Die LiSA-Steuerung speichert keine personenbezogenen Daten
- Die von der LiSA-Steuerung gespeicherten Log-Dateien für Betriebs- und Fehlerzustände werden von der Steuerung nicht weiterverarbeitet und können nur durch Abfrage ausgelesen werden.

FR 5 - Eingeschränkter Datenfluss

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

FR 6 - Rechtzeitige Reaktion auf Ereignisse

- Die LiSA-Steuerung generiert bei Fehlern oder Betriebsstörungen einen Log-Eintrag.

FR 7 - Verfügbarkeit der Ressourcen

- Die Sicherheitsfunktionen sind unabhängig von der Kommunikation innerhalb der Steuerung.
- Einsatz von Komponenten in sicherheitsrelevanten Bereichen (z.B. Schachtkopierung) welche selbst eine entsprechende Cybersicherheit aufweisen.

Aktualisierung:

Die LiSA-Software wird ständig weiterentwickelt um auch unter sich ändernden Gegebenheiten auf dem Stand der Technik zu bleiben.

Schneider Steuerungstechnik GmbH
Gewerbestrasse 7
D-83558 Maitenbeth

http: //www.lisa-lift.de

Telefon: + 49 (0)8076 / 91 87 - 0
Telefax: + 49 (0)8076 / 91 87 - 117

E-Mail: info@lisa-lift.de