
KONE
Cybersecurity
Wie real ist die
Bedrohung für Aufzüge
Referierende: Andreas Backer, Thomas Lipphardt
Im Chat: Stephan Hindemith
Dedicated to
People Flow™

# Mit mir haben Sie es heute zu tun

ANDREAS BACKER

- Seit September 2022 bei KONE
- Produktmanagement Digital Solutions (APIs, People Flow, Monitoring)
- Einführung und Betreuung digitaler Lösungen
- Vor KONE:
  Softwareentwicklung, IT-Administration, Beauftragter Informationssicherheit

# Mit mir haben Sie es heute zu tun

## THOMAS LIPPHARDT

- Manager Technische Regelwerke bei KONE
- Mitglied in folgenden Gremien
  - Deutscher Ausschuss für Aufzugstechnik (DAfA)
  - Deutsches Institut für Normung (DIN)
  - Verein Deutscher Ingenieure (VDI)
  - Verband der Maschinen und Anlagenbauer (VDMA)
  - Fachausschuss und Fachbeirat des VDI
- Mitglied bei folgenden Richtlinien-Ausschüssen
  - DIN 8989 / VDI 2566 Schallschutz
  - VDI 2168 Qualifizierung von Personal
  - VDI 3809 Prüfung von Feuerwehraufzügen
  - VDI 3810 Blatt 6 Wartung von gebäudetechnischen Anlagen "Aufzüge"
  - VDI 4068 Befähigte Personen
  - VDI 4705 Notrufmanagement (Obmann)
  - VDI 4707 1+2 Energieeffizienz
  - VDI 6004 Vandalismus
  - VDI 6017 Brandfallsteuerung von Aufzügen
  - VDI 6022 Entrauchung und Be- und Entlüftung von Aufzugsschächten

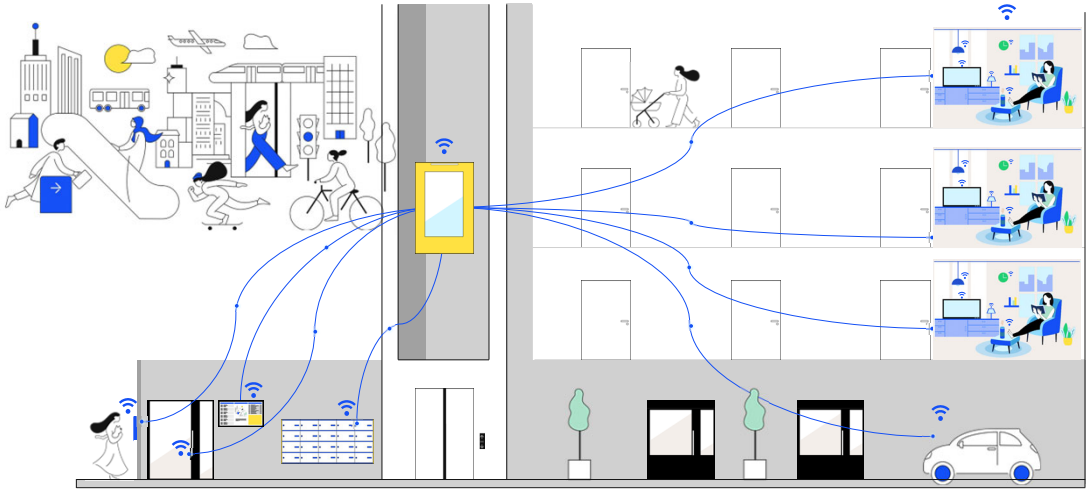
## Unsere heutigen Themen

1. Warum ist Cybersecurity bei Aufzügen wichtig?
2. Sicherheit: Safety vs. Security
3. TRBS 1115 und 1115-1 (Deutschland)
4. Angreifbare Komponenten
5. Aktuelle und kommende Normen
6. Was sollte ich tun?

KONE

# Warum ist Cybersecurity bei Aufzügen wichtig?

## Aufzug im Smart Building



Gebäude werden zunehmend digitaler – Stichwort „Smart Building“
Moderne Aufzüge sind mittlerweile Teil dieser smarten Gebäude-Infrastruktur und mit anderen Systemen vernetzt. Sie sind quasi auch ein IoT-System.
Dieser Trend der Vernetzung von Systemen wird sich in Zukunft fortsetzen.

## Aufzugsanlagen werden digitaler

Aufzugsanlagen werden digitaler. Damit kann Mehrwert für die Anwender erzeugt werden
Mit einem einfachen Aufzug kann ich nur hoch und runter fahren. Wenn ich ihn mit Drittsystemen koppele, entstehen Anwendungsfälle, die so vorher nicht möglich waren.
Hier einige Beispiele:

- Prädiktive Wartung
  - Betriebsdaten der Aufzüge werden gesammelt und auf Unregelmäßigkeiten analysiert
  - Dadurch kann frühzeitig der Ausfall eines Bauteils prognostiziert werden und ein Austausch vorgenommen werden, ohne dass eine Störung auftritt

- Informationssysteme für Facility Management und Bewohner
  - Informationen über den Status (z.B. in Betrieb oder Störung/Wartung) werden transparent zur Verfügung gestellt
  - Für Bewohner z.B. über Bildschirme im Haus oder Gebäude-App
  - Für Facility Management z.b. über zentrale Systeme und Dashboards

- Smartphone App zur Aufzugssteuerung
  - Aufzug schon in der Wohnung oder im Büro rufen und keine Zeit beim Warten verlieren

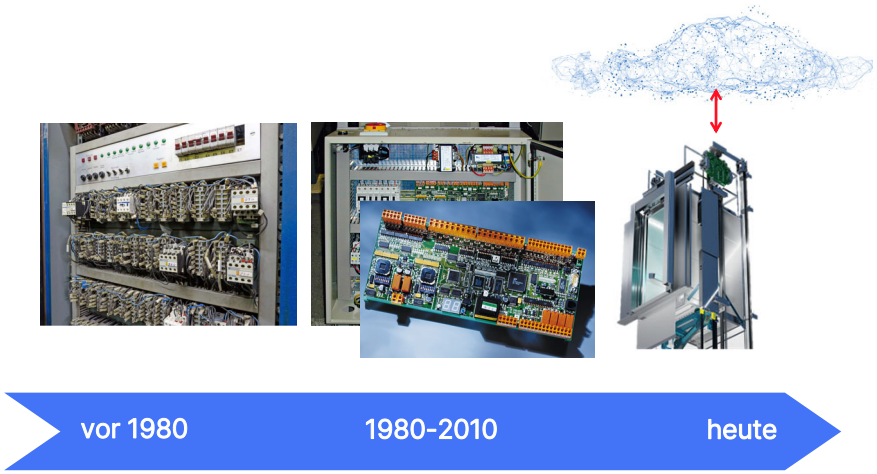
- Sprachsteuerung
  - Aufzüge per Sprachbefehl rufen, komplett berührungslos

- Anbindung Smarthome Systeme
  - Sammlung und Auswertung von Betriebsdaten des Aufzugs
  - Anwendungsfall Gästesteuerung (Aufzug vorprogrammiert nach unten senden, um einen Gast abzuholen)

- (Video-) Intercom und Zutrittssysteme
  - Wenn ich die Haustür für mich selber oder aus der Wohnung heraus für Besucher öffne, weiß der Aufzug schon Bescheid und holt mich/den Besucher ab
  - Wartezeiten werden so reduziert

- Serviceroboter
  - Serviceroboter, die sich in mehrstöckigen Gebäuden bewegen sollen, müssen dafür Aufzug fahren
  - Dafür benötigen sie eine Schnittstelle zum Aufzug, um die entsprechenden Befehle senden zu können
  - Interessant z.B. für
    - Zimmerservice in Hotels
    - Lieferroboter
    - Reinigungsroboter

## Aufzugsanlagen werden digitaler




Bei der Digitalisierung und bei der Frage nach der Cybersicherheit spiel die Steuerung eine besondere Rolle.
Wie haben sich die Steuerungen über die Jahre entwickelt?

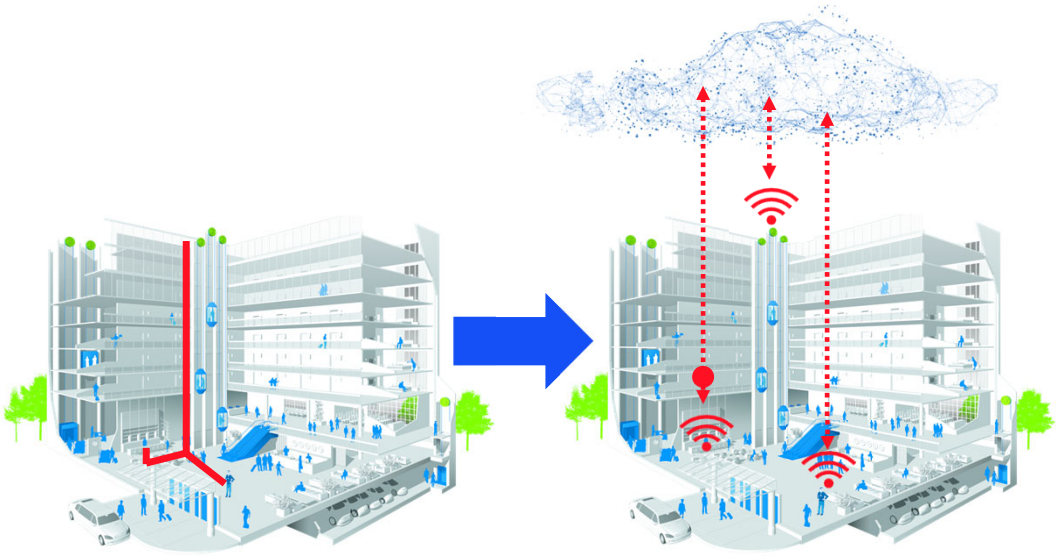
Vor 1980:
- Überwiegend Relaissteuerungen
- Man hat den Strom, der dort fließt regelrecht gehört
- Daher auch nicht ganz ungefährlich
- Cybersecurity war noch kein Thema. Die Steuerungen waren nicht vernetzt und es gab ja auch noch gar kein Internet

Nach 1980:
- Steuerungen wurden zunehmend in Form von Controllerboards gebaut
- Anfangs auch noch mit fest eingebrannter Software
- Steuerungen wurden dadurch kleiner und sicherer (keine offenen Relais mehr)
- Cybersecurity war immer noch kein Thema, da die Anlagen keine Schnittstellen nach außen hatten
- Der physische Schutz musste damals wie heute gewährleistet werden, da mit direktem Zugriff auf die Anlagenbauteile auch Manipulationen möglich gewesen wären.

Das war früher so und gilt heute noch genauso

Heute:
- Die Steuerungen sind heute mehr oder weniger kleine Computer und haben Schnittstellen zu externen Systemen (z.B. Cloud)
- Das ermöglicht die gerade vorgestellten Anwendungsfälle und die Erzeugung von Mehrwert
- Hier müssen wir uns dann auch mit dem Thema Cybersicherheit beschäftigen

## Vom Kabel zur Cloud



Früher: lokale Verkabelung

Für jeden Anwendungsfall mussten Kabel gezogen werden
- Z.B. von der Rezeption zur Aufzugssteuerung, um den Aufzug zu rufen
- Ein Knopf an der Rezeption kann dann genau eine Aktion ausführen: Aufzug ins Erdgeschoss rufen

Für komplexere Anwendungsfälle brauchte man ggf. noch zusätzliche Hardware (z.B. Server) vor Ort

Der Trend geht heute vermehrt zu Cloudlösungen.

Vorteile:
- Keine Server vor Ort
  - Kein eigenes IT-Personal erforderlich für Wartung
- Automatische Updates
  - Software immer up-to-date, Sicherheitslücken werden schnell geschlossen
- Sicherheit
  - Fachpersonal, die sich wirklich mit IT-Sicherheit auskennen
  - Vergangene Ransomware Attacken: immer lokale IT betroffen statt großen Clouddienstleister
- Von überall erreichbar

    - Smartphones/Tablets können von überall mit den Diensten kommunizieren
    - Kein extra einloggen ins WLAN nötig
- Skalierbarkeit
    - Serverkapazitäten können sehr schnell und einfach erweitert werden

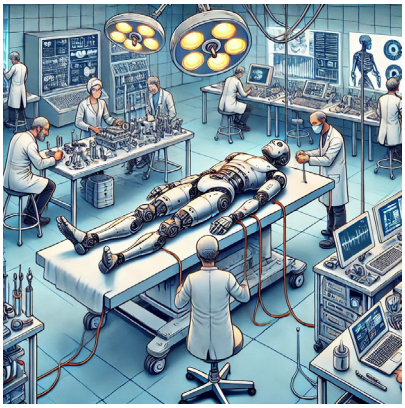
KONE

# Sicherheit:

# Safety vs. Security

## Sicherheit: Safety vs. Security

**Safety**
„Schütze den Menschen vor der Maschine“



**Security**
„Schütze die Maschine vor dem Menschen“

*Bilder KI-generiert

Das Wort „Sicherheit“ kann verschiedene Bedeutungen haben.
Im Englischen gibt es hier eine schöne Unterscheidung: Safety und Security

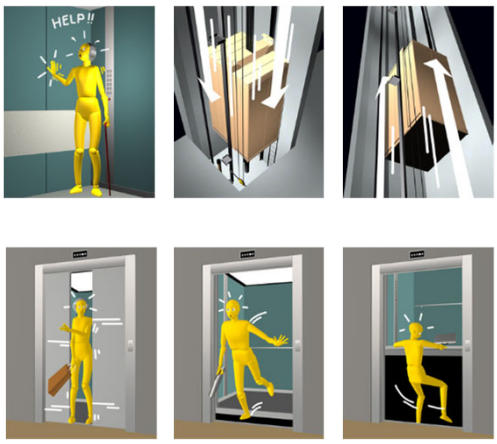
Safety: Schutz von Menschen vor Gefährdungen durch Maschinen > Betriebssicherheit
Security: Schutz von Maschinen/Informationen auf Systemen vor den Menschen (z.B. Hackern) > Informationssicherheit

Früher wurden diese beiden Bereiche getrennt betrachtet.
„Saftey“ spielt in der Aufzugsbranche schon immer eine sehr große Rolle.
Bei der (Cyber-)“Secutrity“ ging es darum Informationen auf IT-Systemen zu schützen.

Mit der zunehmenden Vernetzung von Systemen (Stichwort IoT/Industrie 4.0) kann die (Cyber-)Secutrity jetzt ggf. auch Einfluss auf die „Safety“ von Maschinen haben.

Daher müssen wir uns auch für Aufzüge um das Thema kümmern.

## Mögliche Gefährdungen?




Gibt es denn mögliche gefährliche Situationen, die durch solche Cyberangriffe verursacht werden könnten?

- Der Aufzug fährt hoch und runter und macht die Tür nicht auf, ich komme nicht raus
  -> Unangenehm, aber nicht gefährlich -> Notruf verwenden
- Der Aufzug bleibt stecken
  -> Unangenehm, aber nicht gefährlich -> Notruf verwenden
- Der Notruf funktioniert nicht
  -> Auch keine gefährliche Situation. Allerspätestens alle 72 Stunden (nach Norm) muss die Funktionsfähigkeit des Notrufs geprüft werden und es fällt auf.
  Bei KONE passiert das alle 24 Stunden automatisch (Routine Call)
- Aufzug fährt zu schnell (hoch oder runter)
  -> Dafür gibt es spezielle unabhängige Sicherheitseinrichtungen im Aufzug. Bei Übergeschwindigkeit würde der Geschwindigkeitsbegrenzer die Bremse und Fangvorrichtung auslösen
- Tür läuft zu schnell oder mit zu viel Kraft zu
  -> Auch dafür gibt es Sicherheitseinrichtungen
- Stolperkante durch unbündiges Anhalten in der Etage
  -> Sicherheitseinrichtung vorhanden
- Aufzug fährt bei geöffneter Tür weg
  -> Sicherheitseinrichtung vorhanden (USM), die das verhindert

## Sicherheitseinrichtungen eines Aufzugs

| | |
|---|---|
| Mechanische Sicherheitseinrichtungen | Beispiel: Fangvorrichtung |
| Elektrische Sicherheitseinrichtungen | Sicherheitskreis |
| Elektronische/ programmierbare Sicherheitseinrichtungen | PESSRAL ("Programmable Electronic System in Safety-Related Applications for Lifts") |

Sicherheitseinrichtungen an Aufzügen:

- Mechanische Sicherheitseinrichtungen
  - Rein mechanische, unabhängige Sicherheitseinrichtungen. Z.B. Fangvorrichtung

- elektrische Sicherheitseinrichtungen
  - Elektrische Sicherheitssysteme, die in Reihe geschaltet sind. Wenn eines auslöst wird der Stromkreis unterbrochen und die Bremsen aktiviert

- Elektronische/Programmierbare Sicherheitseinrichtungen
  - Das sind die so genannten PESSRAL-Systeme (Programmable Electronic System in Safety-Related Applications for Lifts)
  - Separate, von der Steuerung unabhängige Sicherheitsplatinen
  - Sind besonders vor Veränderungen geschützt (z.B. per Siegel, das bei Wiederkehrenden Prüfungen auf Beschädigungen geprüft warden muss)
  - Software auf diesen Platinen kann nicht verändert werden (es muss die ganze Platine getauscht werden)
  - PESSRAL Systeme sind geschlossene Komponenten und haben eine eigene Baumusterprüfbescheinigung
  - PESSRAL Systeme kommen in neueren Aufzugsgenerationen zum Einsatz

Um diese Elektronische/Programmierbare Sicherheitseinrichtungen geht es im Folgenden.
Der Stand der Technik hat sich hier weiterentwickelt. Es werden in modernen Aufzügen zunehmend auf solche digitalen Sicherheitssysteme eingesetzt.
Da sie programmierbar sind, d.h. eine Software einsetzen, muss sichergestellt werden, dass hier (auch durch Cyberangriffe) nichts verändert werden kann.

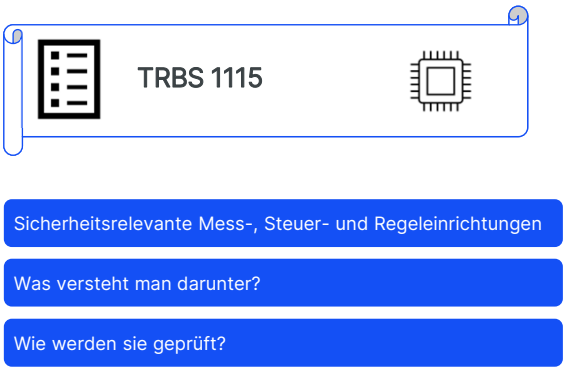
# TRBS 1115 und 1115-1 (Deutschland)

## Betreiber sind verantwortlich für ihre Aufzüge


Die Betriebssicherheitsverordnung (deutsches Gesetz) regelt in die Bereitstellung und Benutzung von Arbeitsmitteln sowie Errichtung und Betrieb von überwachungsbedürftigen Anlagen im Sinne des Arbeitsschutzes.
Quasi alle Aufzüge gelten nach der BetrSichV als Arbeitsmittel.
Daher sind Sie als Betreiber grundsätzlich einem Arbeitgeber gleichgestellt und unterliegen den Pflichten der BetrSichV.
Arbeitgeber im Sinne der Betriebssicherheitsverordnung ist, wer die wirtschaftliche Macht über den Aufzug hat und entscheidet, was mit dem Aufzug passiert.
Arbeitgeber ist für die Aufzugssicherheit verantwortlich und steht in der Haftung.
TRBS (Technische Regeln für Betriebssicherheit) konkretisieren die BetrSichV hinsichtlich des Standes der Technik und beschreiben, wie ein Arbeitgeber die Anforderungen aus der BetrSichV erfüllen kann.
TRBS sind nicht spezifisch für Aufzugssysteme, sondern gelten vor allem auch für große Industrieanlagen.
Ein Arbeitgeber ist nach der BetrSichV verpflichtet eine Gefährdungsbeurteilung für seinen Aufzug zu erstellen.

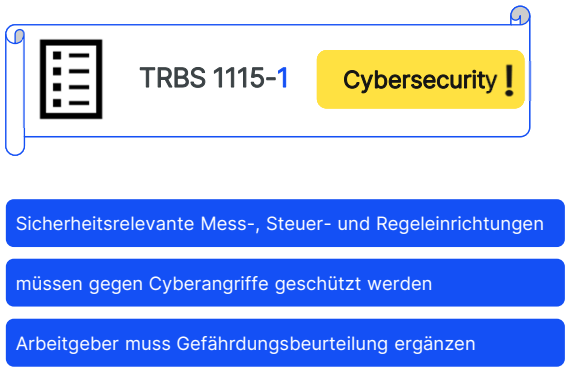

Betriebssicherheitsverordnung und Technische Regeln für Betriebssicherheit haben hauptsächlich große Industrieanlagen im Fokus.
Aufzüge gelten auch als überwachungsbedürftige Anlagen und fallen daher auch unter die Betriebssicherheitsverordnung.

## Sicherheitsrelevante MSR-Einrichtungen und deren Prüfung




Die TRBS 1115 behandelt den Umgang mit so genannten sicherheitsrelevanten Mess- Steuer- und Regeleinrichtungen.
Wir erinnern uns an die vorhin erwähnten elektronische/programmierbare Sicherheitseinrichtungen in Aufzügen (PESSRAL).
Genau diese Sicherheitseinrichtungen und deren Prüfung werden in dieser TRBS behandelt.

## Sicherheitsrelevante MSR-Einrichtungen Cybersicherheit




Die TRBS 1115-1 behandelt das Thema Cybersicherheit für die sicherheitsrelevanten Mess- Steuer- und Regeleinrichtungen (sicherheitsrelevante MSR-Einrichtungen) aus der TRBS 1115

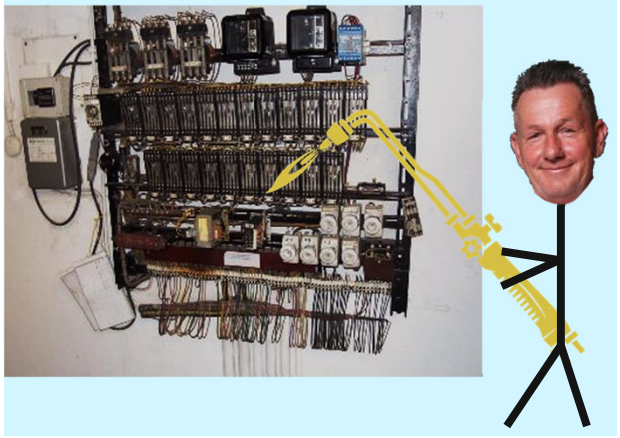
- Sicherheitsrelevante MSR-Einrichtungen müssen gegen Cyberangriffe geschützt werden
- Der Arbeitgeber muss seine Gefährdungsbeurteilung dahingehend ergänzen

- Hier geht es nur um das Thema „Safety“
- Es geht nicht um die Abwehr von wirtschaftlichen Schäden oder um Datenschutz
  - z.B. auch nicht um die Frage: Wie sicher sind meine Daten in einer Cloud
- Diese TRBS behandelt keine Arbeitsmittel oder sicherheitsrelevante MSR-Einrichtungen, die keine Schnittstellen (kabelgebunden oder kabellos) haben und daher nicht kompromittiert werden können

## Physische Sicherheit

**BEKANNT**

Schutz vor physischer Manipulation

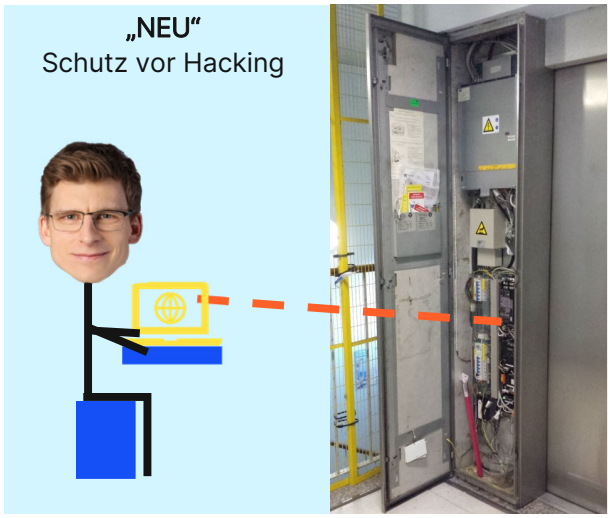


**TYPISCHES SCHUTZMITTEL:**

Technik hinter verschlossenen Bereichen

Der Schutz der physischen Sicherheit von (insbesondere sicherheitsrelevanten) Anlagenteilen ist nicht neu.
Typisches Schutzmittel hierfür ist: Technik hinter verschlossenen Bereichen halten.
So ist sie vor Manipulation geschützt.
D.h. dieser Aspekt ist auch nicht neu für sicherheitsrelevante MSR-Einrichtungen.

## Cyber- Sicherheit




**Neu:**

Wie sind vorhandene (Fern-) Zugriffs-Schnittstellen gesichert?

Neu ist der Schutz von Angriffen aus der Ferne durch evtl. vorhandene (Fern-) Zugriffsschnittstellen.

Ein Angreifer könnte somit unbemerkt aus der Ferne versuchen, eine Anlage zu kompromittieren.
Vor solchen Angriffsszenarien müssen insbesondere sicherheitsrelevante Komponenten geschützt werden.

KONE

# Angreifbare Komponenten

Welche Komponenten eines Aufzugs sind denn potenziell angreifbar?

## Wann ist eine Komponente potenziell angreifbar?


Komponenten sind nur potentiell angreifbar, wenn sie eine digitale Schnittstelle haben.

Das können sein:
- Physische Schnittstellen (USB, Netzwerk/RJ45, etc.)
- Lokale drahtlose Schnittstellen (z.B. Bluetooth, WLAN)
- Externe Schnittstellen (z.B. Internetanbindung)

➔ Lokale Schnittstellen müssen physisch gesichert werden
➔ Lokale Drahtlose Schnittstellen können z.B. passwortgeschützt oder verschlüsselt werden (Stichwort: sicheres WLAN-Passwort)
➔ Externe Schnittstellen können z.B. verschlüsselt und mit sicheren Authentifizierungsmechanismen versehen werden
Cloudlösungen können entsprechend zertifiziert werden und so die Cybersicherheit nachgewiesen werden

## Sichtweise der Prüforganisationen

**Beispiele betroffener Komponenten**

- Sicherheitsrelevante MSR-Einrichtungen
- Zwei Wege-Kommunikationssysteme („Notrufsystem“)
- Schutzbedürftige IT/OT-Umgebung
- Weitere Bauteile gem. ISO 8102-20, sofern digital und cyberrelevant/schutzbedürftig
- PESSRAL-Komponenten
- Frequenzumrichter (FU) mit sicherheitsrelevanter Funktion

Bewertung durch den Sachverständigen

Die Prüforganisationen sehen eine etwas größere Anzahl an potenziell betroffenen Komponenten als in der TRBS 1115 und 1115-1 genannt sind.

## Sicherheitseinrichtungen eines Aufzugs

| | |
|---|---|
| Mechanische Sicherheitseinrichtungen | Beispiel: Fangvorrichtung |
| Elektrische Sicherheitseinrichtungen | Sicherheitskreis |
| Elektronische/ programmierbare Sicherheitseinrichtungen | PESSRAL ("Programmable E… …in Safety-Relat… …or Lifts") |

Gemäß TRBS 1115-1

Wir erinnern uns nochmal an die Sicherheitseinrichtungen eines Aufzugs.
Die elektronischen/programmierbaren Sicherheitseinrichtungen fallen unter die TRBS 1115-1.

## Laut Prüforganisationen zu prüfen

Elektronische/ programmierbare Sicherheitseinrichtungen

PESSRAL

("Programmable E… in Safety-Relat… …or Lifts")

Gemäß TRBS 1115-1

Laut Prüforgani-sationen meist gefordert

Steuerung
Notrufsystem

Frequenzumrichter
Türantrieb

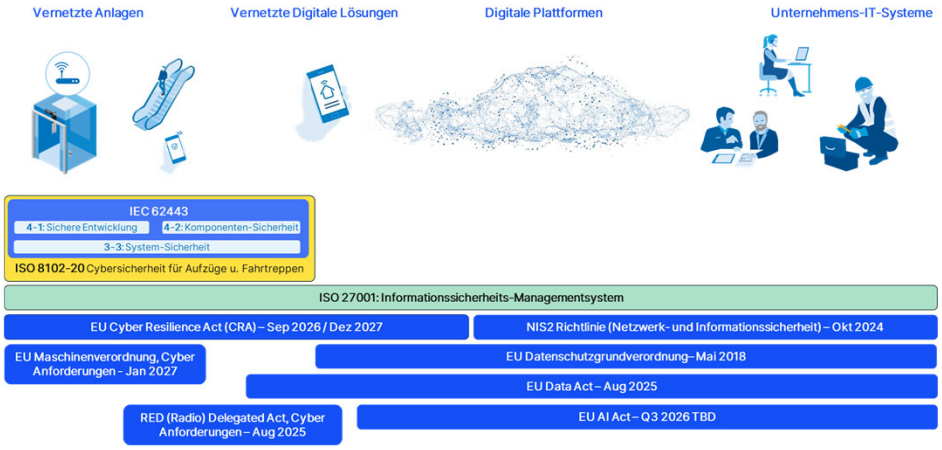
Diese sind auf jeden Fall zu betrachten und bzgl. Cybersicherheit zu schützen

Aus unserer Erfahrung der letzten 1,5 Jahre bestehen die Prüforganisationen mindestens auf die Betrachtung der folgenden Komponenten eines Aufzugs

- Steuerung
- Notrufsystem
- Frequenzumrichter
- Türantrieb

# Aktuelle und kommende Normen

## Aktuelle und kommende Cyber-Vorschriften




Es sind bereits viele neue Vorschriften zum Thema Cybersicherheit auf dem Weg bzw. Zum Teil schon umgesetzt

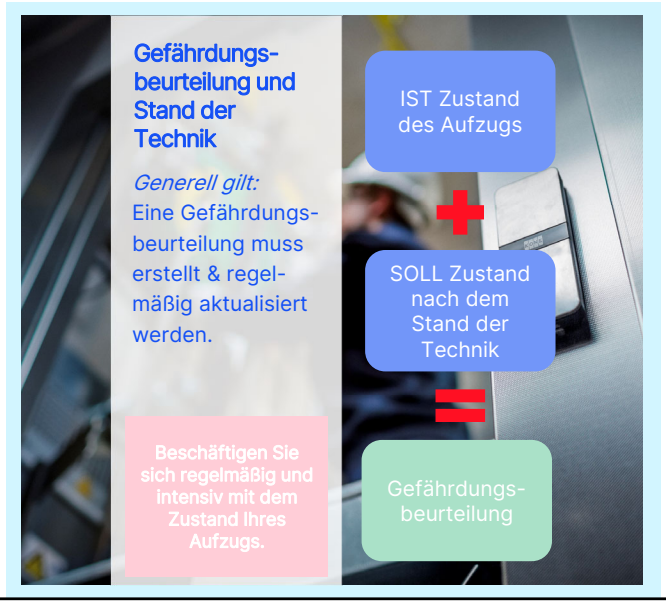
Hervorzuheben sind hier vor allem:

- Die ISO 8100er Normenreihe
  - Hier speziell die ISO 8102-20, die sich explizit mit der Cybersicherheit von Aufzügen befasst
  - Sie verweist sehr stark auf die IEC 62443 (eine Normenreihe für industrielle Cybersicherheit und zum Schutz kritischer industrieller Steuerungssysteme)
  - Damit wird es auch für die Hersteller eine Vorgabe geben, sich mit dem Thema Cybersicherheit auseinanderzusetzen
  - Hinweis: Die Steuerungen neuer KONE Aufzüge werden bereits nach der IEC 62443 zertifiziert
- ISO 27001
  - Internationale Norm zur Informationssicherheit
  - Sie wird verwendet zur Zertifizierung von Informationssicherheitsmanagementsystemen und -prozessen in Unternehmen.
  - Kunden können anhand einer Zertifizierunge nach dieser Norm die Informationssicherheit eines Unternehmens bzw. deren Angebotener (Cloud-) Dienste beurteilen.

KONE

Was sollte ich tun?

## Gefährdungsbeurteilung

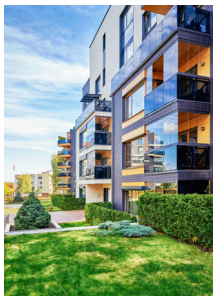



Erstellen sie eine Gefährdungsbeurteilung für ihre Aufzüge. Sie sind als Arbeitgeber im Sinne der Betriebssicherheitsverordnung dazu verpflichtet.
Betrachten sie darin auch das Thema Cybersicherheit.

- Grundlage ist die Betrachtung des IST-Zustandes Ihrer Anlage
- Dagegen wird der Sollzustand nach dem Stand der Technik gehalten
- Aus den Abweichungen und der Behandlung der sich daraus ergebenden Risiken ergibt sich die Gefährdungsbeurteilung

## Umfeldbetrachtung

Wo wird mein Aufzug eingesetzt?



Kleines Wohngebäude

VS

Krankenhaus, Bank, etc.

Das Umfeld des Aufzugs spielt eine Rolle bei der Erstellung der Gefährdungsbeurteilung und bei der Betrachtung der Cybersicherheit

Ein Aufzug in einem einfachen/mittleren Wohngebäude wird kein lohnendes Ziel für einen Hacker sein.
Wenn ein Aufzug hier durch einen Angriff ausfallen würde, würde das erstmal keinen massiven Schaden verursachen.

Anders sieht es hingegen z.B. bei Krankenhäusern aus.
Wenn hier ein Aufzug vom Heli-Pad zum Operationsaal ausfällt stehen ggf. Menschenleben auf dem Spiel.
Hier muss das Risiko ganz anders betrachtet werden, als in Wohngebäuden.

Solch ein hohes Risiko besteht aber nur beim kleinsten Teil aller Aufzugsanlagen.

Daher: Immer das tatsächliche Risiko mitbetrachten bei der Bewertung von Cybersecurity-Anforderungen und –Maßnahmen.

## Das haben wir heute gelernt

1. Aufzüge werden digitaler
2. Cybersecurity spielt daher eine größere Rolle
3. Digitale Komponenten mit Schnittstellen nach außen müssen geschützt werden
4. Betreiber sind für ihre Anlagen verantwortlich
5. Erstellen Sie eine Gefährdungsbeurteilung
6. Der Aufzug ist und bleibt das sicherste Verkehrsmittel

# Weitere Informationen

## AUF UNSEREN WEBSITES

Unsere Cyber-Security-Prinzipien

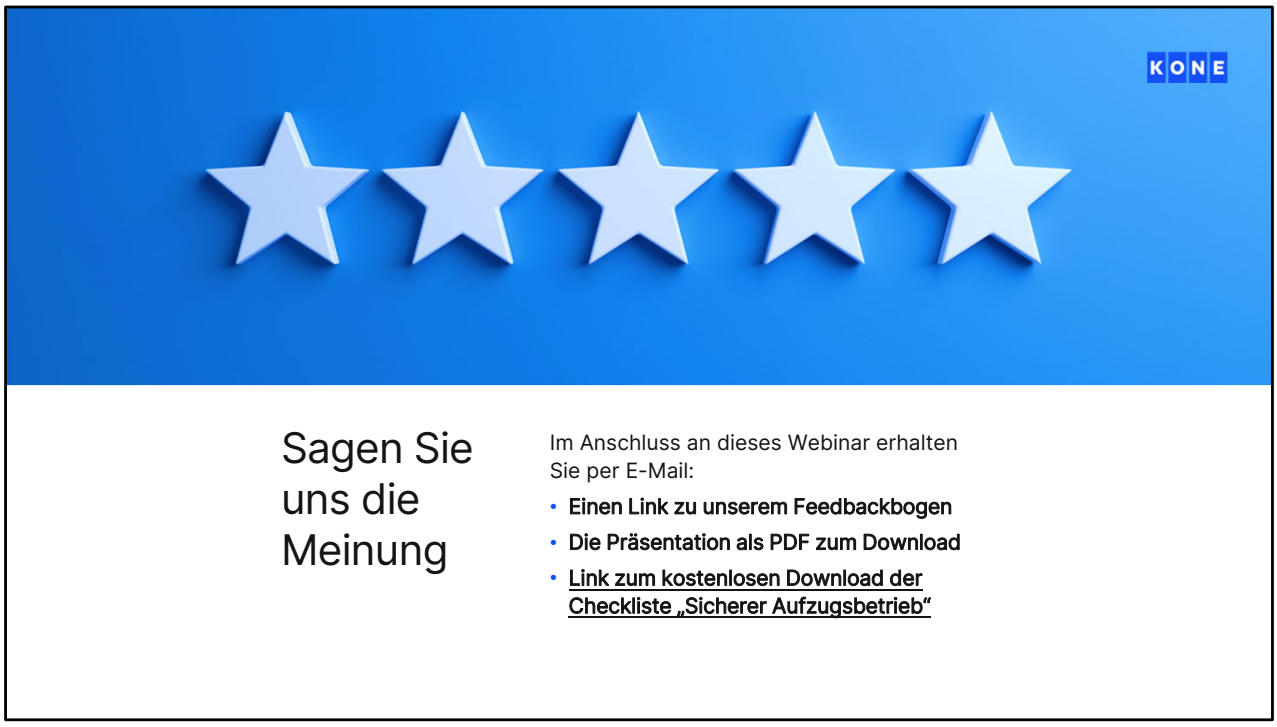
- https://www.kone.de
- https://www.kone.at
- https://www.kone.ch

## IM NÄCHSTEN LIVE-ONLINETRAINING

Donnerstag, 8. Mai 2025, 15-16 Uhr

**„Ausfallzeiten, Aufwand und Kosten älterer Aufzüge reduzieren – Ihre Mieter danken es Ihnen" mit Matthias Meiner und Rüdiger Scheidt**

Jetzt anmelden




Checkliste: Sicherer Aufzugsbetrieb
Beim Betrieb von Aufzügen sind eine Vielzahl von Normen und Vorschriften zu beachten, Cybersecurity war heute im Fokus. Die Checkliste: Sicherer Aufzugsbetrieb fasst zusammen, an was Sie beim Aufzugsbetrieb denken müssen und wo Sie Unterstützung finden.


KONE
Vielen Dank.
Wie lauten Ihre Fragen?
Thomas Lipphardt
Manager Technische Regelwerke
E-Mail: thomas.lipphardt@kone.com
Andreas Backer
Produktmanagement Digital Solutions
E-Mail: andreas.backer@kone.com
Dedicated to
People Flow™