Neuer Anhang der TRBS 1115-1: Unterstützung für Aufzugsbetreiber bei der Cybersicherheit

Autor: Philipp John, BGHM

Die Technische Regel für Betriebssicherheit (TRBS) 1115-1 „Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen“ konkretisiert die Betriebssicherheitsverordnung, wenn es darum geht, erforderliche Schutzmaßnahmen gegen Cyberbedrohungen an Arbeitsmitteln und überwachungsbedürftigen Anlagen zu ermitteln und festzulegen. Für Arbeitgeber und Aufzugsbetreiber bedeutet dies, dass sie im Rahmen ihrer Gefährdungsbeurteilung mögliche Bedrohungen identifizieren und angemessene Schutzmaßnahmen festlegen und umsetzen müssen. Eine unzureichende oder nicht durchgeführte Dokumentation dieses Vorgehens kann zu Mangeleinstufungen bei den wiederkehrenden Prüfungen durch die zugelassenen Überwachungsstellen (ZÜS) führen.

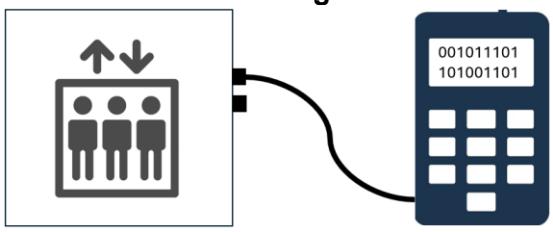
Der am 15. Januar 2026 veröffentlichte Anhang 2 soll die Forderungen der TRBS 1115-1 für Betreiber verständlicher machen und sie dabei unterstützen, die Gefährdungsbeurteilung entsprechend zu ergänzen. In dem Anhang finden sich Beispiele dafür, worauf je nach Grad der Vernetzung zu achten ist.

Folgende Beispiele werden betrachtet:

1) **Arbeitsmittel ohne externe Schnittstellen**

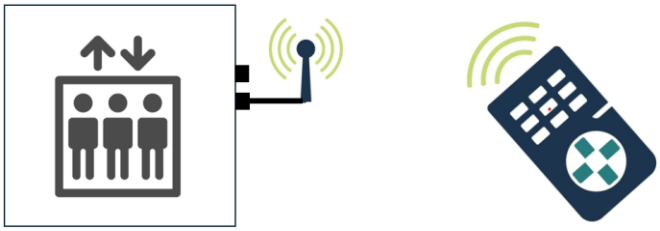
Bei dieser Ausführung sind keine externen Schnittstellen vorhanden oder nutzbar. Parameter können nur lokal an der Aufzugssteuerung verändert werden. Daher fällt dieser Anlagentyp nicht in den Anwendungsbereich der TRBS 1115-1. Eine Betrachtung der Cybersicherheit ist nicht notwendig. Dies muss anlagenspezifisch dokumentiert werden.

2) **Arbeitsmittel mit drahtgebundenen Schnittstellen ohne weitere Vernetzung**



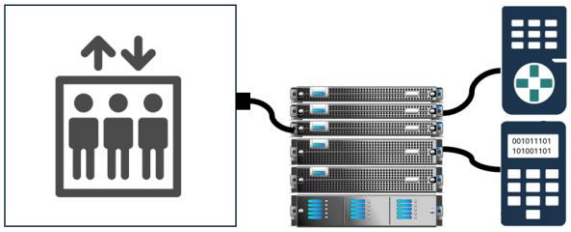
Die Schnittstellen werden nur drahtgebunden lokal genutzt (z.B. mit Konfigurationsgerät) und das Arbeitsmittel wird nicht vernetzt betrieben. Parameter können nur über die physische Schnittstelle geändert werden. Ab diesem Steuerungstyp fällt der Aufzug in den Anwendungsbereich der TRBS 1115-1 und muss gegen mögliche Cyberbedrohungen geschützt werden. Es empfiehlt sich, auch das Konfigurationsgerät zu betrachten.

3) **Arbeitsmittel mit drahtlosen Schnittstellen ohne weitere Vernetzung**



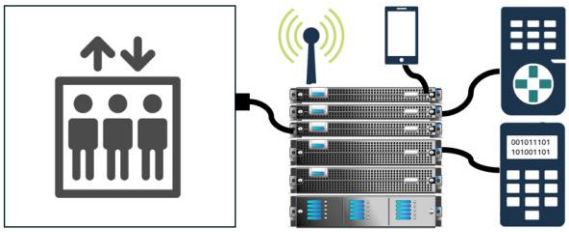
Bei diesem Beispiel ist lediglich im „Inselbetrieb“ eine Bedienung des Aufzuges, jedoch keine Parametrierung über die drahtlose Schnittstelle vorgesehen. In diesem Fall muss sowohl die Bedienstation als auch die drahtlose Verbindung betrachtet werden. Soll zusätzlich eine Programmierung über eine drahtgebundene Schnittstelle erfolgen, so ist das Beispiel 2 heranzuziehen.

4) **Arbeitsmittel mit drahtgebundenen Schnittstellen und Vernetzung im Inselbetrieb**



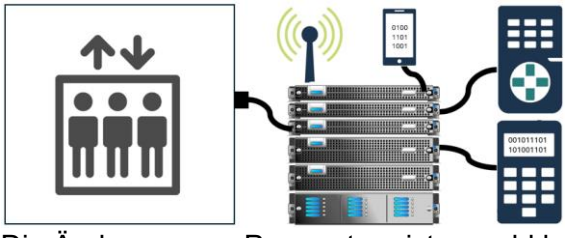
Der Aufzug ist an ein Netzwerk angeschlossen, arbeitet jedoch im „Inselbetrieb“. Das Netzwerk ist demnach nur zu Zwecken des Betriebes des Aufzuges vorgesehen. Eine Parametrierung ist lokal oder über das Netzwerk möglich, z.B. über angeschlossene Konfigurationsgeräte. Bei der Untersuchung auf Cyberbedrohungen muss das gesamte Netzwerk betrachtet werden.

5) **Arbeitsmittel mit drahtgebundener oder drahtloser Überwachung über OT-Netzwerk**



Der Aufzug wird dauerhaft über ein offenes Netzwerk betrieben, welches sowohl drahtgebunden als auch drahtlos mit Konfigurationsgeräten oder Bedienstationen verbunden ist. Außerdem können weitere Dienste (z.B. der Hersteller der Aufzugsanlage oder vernetzte Produktionsanlagen) Statusinformationen einsehen. Ein Ändern von Parametern ist nur lokal möglich. Auch bei diesem Beispiel muss das gesamte Netzwerk inklusive angeschlossener Geräte betrachtet werden.

6) **Arbeitsmittel mit drahtgebundener oder drahtloser Steuerung über OT-Netzwerk**



Die Änderung von Parametern ist sowohl lokal am Aufzug als auch über die drahtgebundene oder drahtlose externe Schnittstelle möglich. Einzelne weitere

Dienste haben Zugriff auf die Konfiguration oder Bedienung des Aufzuges. Eine Fernsteuerung z.B. durch den Hersteller ist möglich. In diesem Fall empfiehlt sich eine detaillierte systemspezifische Betrachtung aller einzelnen Komponenten.

Betreiber können den Anhang 2 der TRBS 1115-1 heranziehen, um Cyberbedrohungen zu ermitteln und zu bewerten als auch dafür, angemessene Schutzmaßnahmen gegen diese auszuwählen. Mögliche Schutzmaßnahmen sind unter anderem eine Segmentierung des Netzwerkes, Zugriffsbeschränkungen, Überwachungsmechanismen oder die Härtung von Schnittstellenkomponenten. Außerdem werden mögliche Prüfanforderungen an die Cybersicherheit vorgeschlagen, die im Rahmen der wiederkehrenden Prüfungen durch die ZÜS heranzuziehen sind.

Bei den regelmäßigen Kontrollen bei der Instandhaltung muss eine fachkundige Person feststellen, ob die Cybersicherheitsmaßnahmen im Betrieb weiterhin funktionstüchtig sind.

Unterstützung bei der Erstellung der Gefährdungsbeurteilung hinsichtlich Cybersicherheit erhalten Betreiber von ihrer Fachkraft für Arbeitssicherheit oder dem beauftragten Instandhaltungsunternehmen. Die Fachbereich AKTUELL FBHM-102 „Safety und Security in der vernetzten Produktion“ zeigt ein grundsätzlich auch für Aufzugsanlagen analog durchführbares Vorgehen auf. Für Aufzugsanlagen, die aus der Ferne gewartet werden können, bietet außerdem die Fachbereich AKTUELL FBHM-133 „Sichere Fernwartung von Maschinen“ den Betreibern hilfreiche Empfehlungen, wie sie die Verbindung mit der Fernwartungsstelle sicher gestalten können.