Cybersecurity: Normenentwurf mit massiven Folgen

Cyber security: draft standard with massive consequences

Vor kurzem ist der Entwurf des Teils 20 der ISO 8102-Reihe zur Cybersecurity von Aufzügen und Fahrtreppen (Electrical requirements for lifts, escalators and moving walks) erschienen. Tim Ebeling, Geschäftsführer des Aufzugmessgeräteherstellers Henning, ist Vertreter des VFA-Interlift im Komitee „Digitalization and Cyber Security" des europäischen Aufzugsverbands ELA. Wir haben ihn um seine Einschätzung des Entwurfs gebeten.

Ist der Inhalt ISO/DIS 8102-20 für Sie überraschend?
Ebeling: Die ISO/DIS 8102-20 wurde für eine ISO-Norm in bemerkenswert kurzer Zeit erarbeitet. Viele der beteiligten Parteien scheinen ein großes Interesse an dieser Norm zu haben. Und selbstverständlich ist Cybersecurity auch ein wichtiges Thema in unserer Branche, da immer mehr Aufzuganlagen z. B. über das Internet vernetzt werden. Der Inhalt an sich hat mich nicht wirklich überrascht. Der Normentwurf referenziert zu großen Teilen auf die IEC 62443, eine internationale Normenreihe über „Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme". Überraschend waren allerdings einige Ausprägungen, die es vielen Marktteilnehmern sehr schwer machen dürften, auch zukünftig ihre Dienste in gewohnter Weise anzubieten.

Was meinen Sie damit?
Ebeling: Nun, der Schwerpunkt dieses Normentwurfs liegt im Kapitel zur „Secure development life cycle for lifts, escalators and moving walks", also dem sicheren Entwicklungs-Lebenszyklus der Komponenten eines Aufzuges. Dabei richtet sich dieses Kapitel an Komponentenhersteller und Systemintegratoren, wobei mit letzteren wohl die Errichter, bzw. Instandhaltungsunternehmen gemeint sind.

Fangen wir mit den Komponentenherstellern an. Ich traue es fast allen zu, nach der bereits angesprochenen Normenreihe IEC 62443 zukünftig ihre Komponenten zu entwickeln – auch wenn das vermutlich bereits während der Entwicklung viele Zertifizierungsnotwendigkeiten durch entsprechende Stellen nach sich ziehen wird.

Das eigentliche Problem ist aber, dass diese Komponentenhersteller in der Regel in die Errichtung einer Anlage und deren Betrieb nicht involviert sind. Dadurch können sie viele der

„Der Entwurf der ISO/DIS 8102-20 wurde für eine ISO-Norm in bemerkenswert kurzer Zeit erarbeitet."
"The draft of ISO/DIS 8102-20 was prepared in a remarkably short time for an ISO standard."

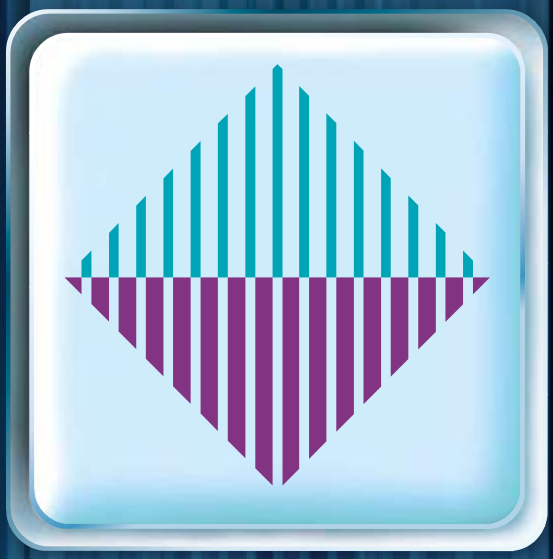
Fotos: ©jeshoots, unsplash.com / berya113, 123rf.com / Collage okapidesign

The draft of section 20 of ISO 8102 on cyber security in lifts and escalators (Electrical requirements for lifts, escalators and moving walks) was published recently. Tim Ebeling, managing director of the lift measurement equipment manufacturer Henning, is the representative of the VFA-Interlift in the committee "Digitalization and Cyber Security" of the European Lift Association ELA. We asked him for his assessment of the draft.

Are you surprised by the contents of ISO/DIS 8102-20?
Ebeling: *The ISO/DIS 8102-20 was prepared in a remarkably short time for an ISO standard. Many of the parties involved appear to be very interested in this standard. And cyber security is of course also an important subject in our sector, since increasing numbers of lifts are networked, e. g. via the Internet. The contents did not really surprise me. To a large extent, the draft standard referenced IEC 62443, an international standard series on "Industrial communication networks – IT security for networks and systems". However, there were several variations, which will probably make it very difficult for many market participants to offer their services in the future in the way they're accustomed to.*

What do you mean by that?
Ebeling: *Well, the main thrust of this draft standard can be found in the chapter on "Secure development life cycle for lifts, escalators and moving walks", i.e. the secure development life cycle of the components of a lift. This chapter is intended for component manufacturers and system integrators, though the latter really refers to the erectors or maintenance companies.*
Let's get started with the component manufacturers. I can see almost all of them in future being able to develop their components according to the already mentioned standard series IEC 62443 – even if this will probably result in having to acquire many certifications during development from the corresponding bodies.

WELCOME TO



interlift

THE HOME OF ELEVATORS

26. – 29. April 2022

Messe Augsburg | Germany

Alle Informationen unter www.interlift.de

Veranstalter: AFAG Messen und Ausstellungen GmbH
Am Messezentrum 5, 86159 Augsburg I www.interlift.de

AFAG WE MAKE FAIRS

Fachlicher Träger: VFA-Interlift e.V.
Süderstraße 282, 20537 Hamburg I www.vfa-interlift.de

VFA INTERLIFT VERBAND FÜR AUFZUGS-TECHNIK

Anforderungen gar nicht erfüllen – gerade in Bezug auf Softwareupdates, Zertifikats-, bzw. Schlüsselhandling und dem geforderten Informationsaustausch zwischen Anlagenbesitzer, Systemintegrator (Instandhaltungs-, bzw. Errichterbetrieb) und Komponentenhersteller.

Dies ist wohl nur möglich, wenn Hersteller, Errichter und Instandhaltungsbetrieb ein und dieselbe Firma sind. Die Cybersecurity-Anforderungen sollten meiner Ansicht nach vor allem technischer Natur sein und nicht organisatorischer und sich auch auf die fertige Anlage beziehen und nicht so sehr den Fokus auf die Arbeitsorganisation der beteiligten Firmen setzen.

Wenn der Normenentwurf in dieser Form bestehen bleibt, scheinen auf die Komponentenhersteller große Anforderungen zuzukommen. Wie sieht es mit den Errichtern und Instandhaltungsfirmen aus?
Ebeling: Schon die Wortwahl Systemintegrator sagt einiges über die Anforderungen aus, die beim Errichten von Anlagen und deren Instandhaltung unter der Berücksichtigung des Normenentwurfs der ISO 8102-20 zu erwarten sind. Die Inbetriebnahme der Anlage oder der spätere Austausch einer Komponente kann dann durchaus auch den Austausch von Softwarezertifikaten und ähnlichem bedeuten. Damit dürften die meisten kleinen und mittelständischen Wartungsunternehmen momentan überfordert sein. Entweder müssen neue Anforderungsprofile an Monteure erstellt werden oder es wird sich vielleicht eine neue Nische für reine Systemintegrator-Firmen im Aufzugbau auftun.

„Eine spezielle Schwierigkeit sehe ich bei modular aufgebauten Anlagen, bei denen sich der Errichter selbst die notwendigen Komponenten zusammenstellt. Gerade dafür würde wohl IT-Systemintegrator-Wissen benötigt werden."

Eine spezielle Schwierigkeit sehe ich bei modular aufgebauten Anlagen, bei denen sich der Errichter selbst die notwendigen Komponenten zusammenstellt. Gerade dafür würde wohl IT-Systemintegrator-Wissen benötigt werden. Wenn die Anlage unter dem Normenentwurf ISO 8102-20 errichtet werden müsste, würde es sich für KMUs wohl anbieten, stattdessen Aufzug-Komplettpakete zu benutzen.


Tim Ebeling

Foto: © Henning

Provokant gefragt – Sie scheinen große Bedenken gegenüber dieses Normentwurfs zu haben. Meinen Sie nicht, dass das Thema Cybersecurity wichtig ist?
Ebeling: Selbstverständlich ist das Thema extrem wichtig. Gerade als Branche, die sich der funktionalen Sicherheit besonders verschrieben hat, können wir solch ein wichtiges Thema nicht einfach ignorieren.

Cybersecurity ist auch für die Fördertechnik immens wichtig und wir müssen alles tun, um IT-Attacken auf unsere Anlagen zu verhindern. Ich habe aber Bedenken über die möglichen Auswirkungen dieses Normentwurfs und hätte mir mehr Praktikabilität gewünscht.

Nehmen Sie das Positionspapier, dass der Verband der Aufzug- und Fahrtreppenbranche in Nordamerika, die National Elevator & Escalator Industry Association (NEII) vor einiger Zeit zum Thema Cybersecurity veröffentlicht hat. Dort wurde ein meiner Ansicht nach sehr einleuchtender Ansatz vorgestellt. Die Kommunikation der Aufzugkomponenten untereinander wurde als sichere Zone definiert, genauso sicher wie die Kabelverbindung zwischen den elektronischen Aufzugkomponenten.

Natürlich ist dieses Kabel auch nicht wirklich sicher, mit einem einfachen Dreikant kann man sich Zugang zum Kabinendach verschaffen, das Kabel durchschneiden oder sonstige gefährliche Zustände herstellen. Die NEII hat aber den Fernzugang zu dieser „sicheren Zone" als besonders schützenswert herausgearbeitet. Das bedeutet, dass die Maßnahmen zur Cybersecurity an dieser Stelle ansetzen müssen, also an der Schnittstelle zur Außenwelt. Diese entsprechende Komponente muss besonders gesichert und geschützt werden. Meiner Ansicht nach ist das sinnvoll und auch praktikabel.

Wen der Entwurf der ISO/DIS 8102-20 unverändert übernommen wird, müssen sich dann die von Ihnen angesprochenen Marktteilnehmer darauf einstellen, neue

However, the actual problem is that these component manufacturers normally aren't involved in setting up a system and its operation. As a result, they cannot meet many of the requirements at all – particularly regarding software updates, certificates or key handling and the information exchange required between lift owners, system integrators (maintenance or erector operation) and component manufacturers.

This is only possible if manufacturers, erectors and the maintenance firm are one and the same company. In my view, the cyber security requirements should above all be of a technical and not an organisational nature and not be too much focused on the work organisation of the companies involved.

If the draft standard continues to exist in this form, major demands appear to be in store for the component manufacturers. What about the erectors and maintenance companies?
Ebeling: *The term system integrator in itself says a lot about the requirements to be expected in erecting lifts and their maintenance, taking the draft standard ISO 8102 into account. Start-up of the lift or later replacement of a component could then certainly also mean replacing software certificates and similar measures. At the moment, this would probably be beyond most of the small and medium-sized maintenance companies. Either new job profiles will have to be set for fitters or a new niche for pure system integrator companies may emerge in lift building.*

I see a special difficulty in modular construction lifts where the erector itself puts together the components needed. This in particular would require IT system integrator knowledge. If the lift has to be erected under the draft standard ISO/DIS 8102-20, it makes sense for SMEs to use complete lift packages instead.

Not to be provocative, but you appear to have great reservations about this draft standard. Don't you think that cyber security is important?
Ebeling: *Of course, it's extremely important. Particularly as a sector that is especially devoted to functional safety, we cannot simply ignore such a crucial subject.*

Cyber security is also immensely important for conveyance technology, and we have to do everything to prevent attacks on our installations. But I do have reservations about the possible

Foto: ©davooda, shutterstock.com/ berya113, 123rf.com/Collage ekapidesign

access to this "secure zone" as particularly worthy of protection. This means that the measures for cyber security have to start at this point, i.e. at the interface to the outside world. These corresponding components have to be specially secured and protected. In my opinion, this makes sense and is also practicable.

Qualifikationen, Arbeitsprozesse etc. einzuführen?

Ebeling: Das heißt es nicht unmittelbar. Solange diese Norm nicht in der EU harmonisiert wird, muss sie auch von keinem Marktteilnehmer zur Anwendung gebracht werden, außer sie ist z. B. in einer Ausschreibung explizit gefordert. Das finde ich insofern bedauerlich, als dass wir uns mit dem Thema Cybersecurity tatsächlich auseinandersetzen und auch sichere Fernzugriffe ermöglichen müssen. Aus diesem Grund würde ich mir eine praktikable, technische und funktionale Lösung wünschen, die auch wirklich durch jeden Marktteilnehmer angewendet werden kann.

effects of this draft standard and would have welcomed more practicability.

Take the paper that the North American National Elevator & Escalator Industry Association (NEII) recently published about cyber security. In my view, it presented a very reasonable approach. Communication of the lift components with each other was defined as a secure zone, just as secure as the cable connection between the electronic lift components.

Of course, this cable is not really secure either. You can gain access to the car roof with a simple triangle, cut the cable or create other dangerous conditions. However, the NEII established remote

If the draft of ISO/DIS 8102-20 is adopted unamended, will the market participants you mentioned have to be prepared to introduce new qualifications, work processes, etc.?

Ebeling: *It doesn't mean this immediately. As long as this standard has not been harmonised in the EU, it does not have to be applied by any market participant unless it is explicitly required, e. g. in a call for tenders. I find this is regrettable, since we actually have to get to grips with cyber security and also facilitate secure remote access. On these grounds, I would welcome a practicable, technical and functional solution, which can also really be applied by every market participant.*