Foto: © Dall·e/okapidesign

CANopen-Lift, CRA und Cybersecurity

CANopen Lift, CRA and cyber security

VON HOLGER ZELTWANGER

Cyber-Kriminalität ist die drittgrößte Wirtschaft nach den USA und China: Sie beträgt nach Schätzungen rund 10,5 Trillionen US-Dollar im nächsten Jahr. Deshalb ist Cybersecurity ein heißes Thema – auch für CAN-Netzwerke, die in vielen Aufzügen eingesetzt werden. Die Befürchtung ist, dass jemand ein Gerät an das Netzwerk anschließt, das die Kommunikation korrumpiert und zu fehlerhaftem Verhalten des Aufzugs führt. Es gibt sicherlich noch weitere Szenarien, die aber nicht das Thema dieses Artikels sind.

Nationale, regionale und internationale Institutionen haben bereits Gesetze und Vorschriften zur Cybersecurity erlassen. Eines davon ist der europäische Cyber-Resilienz-Act (CRA): Dabei handelt es sich um ein Rahmenwerk, das die Anforderungen an die Cybersicherheit von Hard- und Software beschreibt, die in Europa erfüllt werden müssen. Hersteller sind verpflichtet, Maßnahmen gegen Cyberangriffe während des gesamten Lebenszyklus eines digitalen Produkts zu ergreifen (das LIFTjournal berichtete in der vergangenen Ausgabe darüber). Was Hersteller und Anwender im Einzelnen

Cybercrime is the world's third-largest economy after the U.S. and China: estimates put it at $ 10.5 trillion next year. Therefore, cybersecurity is a hot topic - also for CAN-networked systems as used in many lift control systems. The fear is that someone may connect a device to the network, which corrupts the communication functionality and causes malfunctions in the lift's behaviour. There are other scenarios, but this is not the topic of this article.

BY HOLGER ZELTWANGER

National, regional, and international authorities have already released regulations on cyber security. One of them is the European Cyber Resilience Act (CRA): This is a legal framework that describes the cybersecurity requirements for hardware and software products,

tun müssen, ist jedoch noch unklar. Es gibt viele Fragen und Unsicherheiten. CAN-Netzwerke bestehen aus Hardware und Software, sie fallen also unter den europäischen Cyber-Resilienz-Act.

CAN-Netzwerke sind nicht per se gegen Cyber-Angriffe geschützt. Dies muss hinzugefügt werden. Mit anderen Worten: CAN ist wie eine Tür ohne Schloss. Abhängig von der Anwendung und den zu erwartenden Risiken, muss man entsprechende Maßnahmen ergreifen. Das international genormte OSI-Modell (Open Systems Interconnection) beschreibt entsprechende Security-Maßnahmen (ISO 7498-2:1998). Es modelliert die sichere Kommunikation zwischen den vernetzten Geräten. Theoretisch kann jede der sieben Kommunikationsschichten Security-Maßnahmen implementieren.

CYBERSECURITY BEI CIA

CANopen-Lift ist in der CiA-Dokumentenreihe CiA 417 spezifiziert. Danach entwickelte Geräte brauchen eventuell zusätzlich Funktionen, um vor Cyberangriffen geschützt zu werden. Im eingetragenen Verein CiA (CAN in Automation) gibt es derzeit zwei Gruppen, die sich mit Cybersecurity beschäftigen:

- Die **Special Interest Group (SIG) 01 der Interest Group (IG) 04** entwickelt den CANsec-Sublayer für CAN XL. Es ist vorgesehen, ihn in den CAN-XL-Controllern in Hardware zu implementieren.
- Im Juli dieses Jahres wurde die **SIG „Higher-layer protocol"-Security** gegründet. Das Ziel ist, Security-Maßnahmen für die oberen OSI-Schichten (Layer 3 bis Layer 7) zu spezifizieren, die auf den Datenverbindungsprotokollen CAN-CC und CAN FD basieren (eine Software-Lösung). Sie soll auch für CANopen-Lift-Netzwerke anwendbar sein.

Bei CAN-CC-Rahmentelegrammen mit einer maximalen Datenfeldlänge von acht Byte muss man sicherlich Kompromisse eingehen. Für einen höheren Schutz muss man auf das CAN-FD-Protokoll umsteigen, welches Datenfeldlängen bis 64 Byte ermöglicht. Das Technische Komitee des CiAs modelliert diese beiden Optionen in einer Task-Force entsprechend ISO 7498-2. Wenn all diese Aufgaben erledigt sind, können die CANopen-Lift-Experten diese Lösungen in den CiA-417-Dokumenten einpflegen.

POLITISCHE DISKUSSION NÖTIG

Diese Dinge müssen aber auch politisch diskutiert werden. Nach meiner Meinung kann es auch ausreichend sein, dass in speziellen

Anwendungen eine mechanische Absicherung genügt, wenn beispielsweise die CANopen-Lift-Netzwerke nicht zugänglich sind (zum Beispiel in einem Schacht oder einem nicht öffentlich zugänglichen Gebäude). In anderen Anwendungen kann eventuell eine Ende-zu-Ende-Absicherung auf Applikationsebene ausreichend sein (die Kommunikation ist dann sozusagen transparent). ⇤

can-cia.org

Der Autor ist Managing Director des Vereins CAN in Automation (CiA)

which have to be met in Europe. Manufacturers are now obliged to take measures against cyber-attacks throughout a digital product's entire life cycle (LIFTjournal reported on this in the last issue). What manufacturers and users need to do in detail is still unclear. There are many questions and uncertainties. CAN networks consist of hardware and software, meaning they are also affected by the European Cyber Resilience Act.

CAN networks are not per se protected against cyber-attacks. Cybersecurity needs to be added. In other words: a CAN interface is like a door without a lock. Depending on the application and risks of attacks, you need to apply appropriate measures. The internationally standardized OSI (Open Systems Interconnection) model describes corresponding security measures (ISO 7498-2:1989). It models the secure communication between networked entities. Theoretically, each of the seven layers can implement security measures.

CYBER SECURITY IN CIA

CANopen Lift is specified in the CiA document series 417. Devices developed according to it may need additional functions to be protected against cyber-attacks. Within the nonprofit CiA (CAN in Automation) organization, there are currently two groups dealing with cyber security:

- *The **Special Interest Group (SIG) 01 of Interest Group (IG) 04** is developing the CANsec sublayer for CAN XL. It is intended to implement it in the CAN-XL controllers in hardware.*
- *In July this year the **SIG "Higher-layer protocol" Security** was established. The aim is to specify security measures for the higher OSI layers (Layer 3 to Layer 7), which are based on the data protection protocols CAN-CC and CAN FD (a software solution). Using them for lift networks should also be possible.*

In the case of CAN-CC frame telegrams with a maximum data field length of 8 byte, compromises will no doubt be necessary. If you need higher protection, migration to the CANopen FD protocol, supporting payloads up to 64 byte, is a good option. The CiA Technical Committee of the CiA is modelling these two options as specified in ISO 7489-2. When all these tasks have been performed, the CANopen Lift experts can adapt these solutions to the CiA 417 documents.

POLITICAL DISCUSSION NEEDED

There is also a need to discuss the political dimension of these matters. In my opinion, it could be that in special applications a mechanical access protection is sufficient, e.g., if the CANopen lift networks are inaccessible (for example in the shaft or buildings not open to the public). In other applications, an end-to-end protection might be adequate (the communication is transparent, as it were).

If an attacker has access to the CAN network lines, defensive measures are required. When the lift control system is connected via external interfaces to diagnostic systems or emergency call services, firewalls are required to avoid attacks to the CAN communication – just as you need to lock all doors and even windows in your house to make it harder for thieves. Sometimes, locks on internal doors improve the overall security. This means, CAN-to-CAN bridges as used in most CANopen Lift network systems should implement firewalls, too. ⇤

can-cia.org

Holger Zeltwanger, CiA Managing Director

CAN IN AUTOMATION (CIA)

Am 5. März 1992 wurde der eingetragene Verein CAN in Automation (CiA) auf Initiative von Holger Zeltwanger gegründet, er hat heute über 700 Mitglieder. Er dient als neutrale Plattform für Anwender und Hersteller des Controller Area Network (CAN). Der Verein hat das CANopen-Lift-Protokoll (CiA 417) entwickelt, das eine standardisierte Vernetzung von Aufzugskomponenten ermöglicht.

CAN IN AUTOMATION (CIA)

The registered association CAB in Automation (CiA) was established on the suggestion of Holger Zeltwanger in on 5 March 1992. Today, it has over 700 members and serves as a neutral platform for users and manufacturers of the Controller Area Network. The association developed the CANopen Lift Protocol (CiA 417), which permits standardized networking of lift components.