



Cybersicherheit: Was auf Embedded Devices zukommt

In wichtigen Absatzmärkten für Schweizer Unternehmen tut sich was im Bereich Cybersicherheit: Während auf europäischer Ebene der «Cyber Resilience Act» (CRA) noch diskutiert wird, zwingt die «Radio Equipment Directive» (RED) ab August 2024 die meisten Geräte mit Datenfunkverbindung zu mehr Cybersicherheit. Unternehmen der Automatisierungstechnik – OEMs ebenso wie Embedded-Entwickler – sollten deshalb rechtzeitig reagieren. Die Grossenbacher Systeme AG aus St. Gallen geht mit gutem Beispiel voran.

Quelle: Grossenbacher

Die EU-Verordnung «Radio Equipment Directive» (RED) betrifft auch Controller und Gateways im Umfeld der Automatisierungstechnik: Zur Funk-Kommunikation fähige Geräte dürfen ab August 2024 ausdrücklich kein Netzwerk gefährden oder betrieblich einschränken;

sie müssen stattdessen aktiv personenbezogene Daten schützen und Betrug entgegenwirken. Zudem wird Updatefähigkeit ein Muss – und Over-the-Air(OTA)-Updates über Cloudportale damit de facto zu einer Basisanforderung für eine CE-Kennzeichnung. Zudem ist

absehbar, dass sich die Anforderungen in diesem Bereich auch für die Standard-Ethernet-Kommunikation erhöhen.

Bestehende Normen beachten

Das Thema Cybersicherheit sollte mithin auch bei Embedded-Systemen Priorität besitzen. Für Jonas Schuster, Geschäftsleitung Entwicklung beim EEMS-Spezialisten Grossenbacher Systeme AG, bedeutet das in erster Linie, bei der Produktentwicklung auf Konformität zu bestehenden Normen wie ETSI EN 303 645 (Verbraucherprodukte) oder IEC 62443 (Industrieprodukte) zu achten: «Die RED bezieht sich auf diese Normen, die nach vorherrschender Meinung die Grundlage für künftige harmonisierte Vorgaben darstellen. Dazu kommt Folgendes: Immer mehr Anwender im Umfeld der Automatisierungstechnik – und infolgedessen auch OEMs – fordern von ihren Entwicklungspartnern schon heute «Secure Embedded Devices», weil sie sich einer wachsenden Bedrohung durch Hacker-Angriffe ausgesetzt sehen.»



Bild: Grossenbacher Systeme

Systematisch sicher: der Universal Controller (UC)

Mit ihrem aktuellen universal einsetzbaren Linux-SPS-, IoT- und Edge-Controller bietet die Grossenbacher Systeme AG schon heute ein derartiges «Secure Device», das konform zur IEC 62443 entwickelt wurde. Der CODESYS-SPS-Controller auf Basis einer i.MX 8 CPU besitzt ein integriertes Linux-Yocto-Betriebssystem und unterstützt diverse Open-Container-Initiative(OCI)-Spezifikationen, sodass die Containerisierung direkt auf die Hardware zugreifen kann. Mittels der zahlreichen Schnittstellen können Erweiterungen mit geringem Aufwand angeschlossen werden – natürlich auch Module für Wireless-Datenkommunikation zur Durchführung von OTA-Sicherheitsupdates.

Eine wichtige Rolle bei der Entwicklung der Hard- und Software des UC hat das Schichten-Konzept der Norm IEC 62443 gespielt. Es sieht verschiedene Schichten von Sicherheitsmechanismen vor, die auch dann Schutz bieten, wenn einzelne Schichten kompromittiert werden. Zusätzlich hat die Grossenbacher Systeme AG systematisch auf Tools, Prozesse und Best Practices zur Sicherung ihres Embedded-Geräts gesetzt:

- Vertrauenswürdige Laufzeitumgebung (Trusted Execution Environment oder kurz TEE), im ARM-Umfeld auch TrustZone genannt: In einer TEE können nur speziell dafür freigeschaltete Applikationen ausgeführt werden, jedoch z. B. keine Hackerprogramme.
- Partitionierte Hardware-Ressourcen: Trennung von CPU, Cache, Speicher und Schnittstellen, um ihre Funktion möglichst unabhängig und getrennt voneinander bereitzustellen. Dies ermöglicht gegenseitigen Schutz bei Fehlern.

Die Grossenbacher Systeme AG hat für ihren Universal Controller Cybersecurity gemäss IEC 62443 umfassend umgesetzt – inklusive sicherer Kommunikationsmechanismen zwischen Applikation und System.



«Immer mehr Anwender im Umfeld der Automatisierungstechnik ... fordern von ihren Entwicklungspartnern schon heute «Secure Embedded Devices», weil sie sich einer wachsenden Bedrohung durch Hacker-Angriffe ausgesetzt sehen.»

Jonas Schuster, Geschäftsleitung Entwicklung Grossenbacher Systeme AG

- Speichersperrung: Mit der sogenannten Executable Space Protection werden explizit bestimmte Speicherbereiche als nicht rechtmässig nutzbar gekennzeichnet. Der Missbrauch löst einen Alarm oder Gegenmassnahmen aus.
- Secure Boot: Jedes Embedded Device bootet ähnlich einem PC und sucht dazu sein kleinstes Startprogramm (Boot), in welchem der korrekte Startvorgang detailliert festgelegt ist. Mit dem Secure-Boot-Feature wird das Boot-Programm mittels kryptografischer Algorithmen bei jedem Start geprüft.
- Schutz der gespeicherten Daten (Protect Data at Rest): Dazu gehören Anwendungsdaten, Konfigurationsdaten, Sicherheitsschlüssel, aber auch Usernamen, Userrechte und Kennwörter. Diese sollten in spezieller Sicherheitshardware im Controller explizit verschlüsselt und geschützt gespeichert werden.

Wichtig: Schwachstellen beseitigen

Zudem hat die Grossenbacher Systeme AG bei der Entwicklung des UC grossen Wert auf die Analyse und Beseitigung typischer Software-Schwachstellen gelegt:

- Buffer Overflow: Pufferüberlaufangriffe treten auf, wenn ein Angreifer Daten oder Code in einen Speicherpuffer schreibt, die Grenzen des Puffers überschreitet und benachbarte Speicheradressen zu überschreiben beginnt. Die Anwendung darf neue Daten oder neuen ausführbaren Code keinesfalls verarbeiten.
- Improper Input Validation: Wenn Benutzerangaben gefordert sind, kann ein böswilliger User oder Prozess Eingaben liefern, die zum Absturz einer Anwendung führen, zu viele Ressourcen verbrauchen, vertrauliche Daten preisgeben oder schädliche Be-

fehle ausführen. Textuelle Eingaben oder Inputwerte dürfen also nur im gültigen oder plausiblen Wertebereich verarbeitet werden.

- Improper Authentication: Die Authentifizierung beweist, dass Benutzer oder Prozesse auch jene sind, für die sie sich ausgeben. Eine unsachgemässe Authentifizierung kann es einem Angreifer ermöglichen, die Authentifizierung zu umgehen, wiederholt zu versuchen, ein Passwort zu erraten, gestohlene Zugangsdaten zu verwenden oder ein Passwort mit einem schwachen Passwort-Wiederherstellungsmechanismus zu ändern.
- Improper Restriction of Operations within the Bounds of a Memory Buffer: Wenn Programmiersprache oder Betriebssystem es

einem Programm ermöglichen, auf unerlaubte Speicherorte zuzugreifen, kann ein Bedrohungsakteur möglicherweise die Kontrolle über das System übernehmen oder es zum Absturz bringen. Jedes Programm darf also nur auf erlaubte Speicherbereiche zugreifen, keines Root-Rechte besitzen.

- Information Exposure: Sensible Informationen dürfen keinem Bedrohungsakteur zugänglich sein, Kommunikation und Speicherung müssen verschlüsselt erfolgen.

Fazit: Es ist höchste Zeit für «cybersichere» Systeme

Trotz aller Bemühungen um Sicherheit kann natürlich auch die Grossenbacher Systeme AG nicht garantieren, dass Lösungen wie der Universal Controller allen künftigen Regeln und Normen rund ums Thema Cybersicherheit entsprechen. Dafür sorgt allein die Tatsache, dass vieles noch im Fluss ist – selbst die RED ist nicht flächendeckend in nationales Recht umgesetzt. Dennoch gilt: Wer sichergehen möchte, dass er Controller oder Gateways im Industrieumfeld auch nach dem 1. August 2024 mit CE-Zeichen im Europäischen Wirtschaftsraum (EWR) vertreiben kann, sollte sie mit einer vertrauenswürdigen Ausführungsumgebung (TEE), einer Secure-Boot-Funktionalität und geschützten Speicherbereichen ausstatten. Vorhandene Defizite lassen sich dann unter Umständen nachträglich durch Updates der Firm- und Software ausgleichen. Deshalb steht für Jonas Schuster eines fest: «Es ist an der Zeit, alte Embedded-Systeme kritisch zu hinterfragen und gegebenenfalls durch neue Systeme zu ersetzen, die künftigen Cybersecurity-Standards entsprechen. Und bei Entwicklung dieser Systeme sollten OEMs auf Partner setzen, die Sicherheitsbewusstsein und Kompetenz verbinden.»

gesys.ch

Top 5 für sichere Embedded-Software

- Updates grundsätzlich verschlüsselt übertragen, mit einer Double Copy des OTA Signed Image, damit im Notfall ein sicheres Rollback möglich wird. Dabei den geschützten Speicherbereich der Running Code Section beachten.
- Container-Technologie zur Abgrenzung zwischen der Applikations- und der Systemsoftware (Betriebssystem & Co.) verwenden. Nur gezielte Transaktionen zwischen Containern und System zulassen und die Schnittstellen («Türen») besonders sichern.
- Unnötige Ports entfernen oder schliessen, das System insgesamt maximal verschlanken.
- Bei erhöhtem Sicherheitsbedürfnis Pen(etrations)-Tests durchführen (lassen).
- Niemals Standard-Passwörter verwenden.