Der „CRA-Day“ naht – sind Sie vorbereitet?

von Oliver Roth

Bilder: Grossenbacher Systeme

Der Universal Controller ist laut Hersteller Grossenbacher Systeme „CRA-ready“: Er ist IEC-62443-konform und bietet beste Voraussetzungen für die Einhaltung des „CRA-Stichtags“ im Dezember 2027.

Ab 11. Dezember 2027 müssen „Produkte mit digitalen Elementen“ den Anforderungen des Cyber Resilience Acts entsprechen, wenn sie in der EU vertrieben werden sollen. Maschinenbauer und Industrieausrüster sollten deshalb zeitnah klären, ob und wie die verwendeten digitalen Elemente CRA-tauglich gemacht werden können.

Mit dem Cyber Resilience Act (CRA) schafft die EU einen verbindlichen Rechtsrahmen, der Herstellern eine klare Verpflichtung auferlegt: Sie müssen erstmals die Cybersicherheit ihrer Produkte über den gesamten Produktlebenszyklus systematisch umsetzen und nachweisen. Der 11. Dezember 2027 ist dabei der Stichtag, zu dem dieser Nachweis spätestens vorliegen muss. Als entscheidende Etappe auf dem Weg dorthin tritt im September 2026 die erste konkrete Maßnahme in Kraft: die Meldepflicht für aktiv ausgenutzte Schwachstellen. Das verpflichtet Hersteller nicht nur dazu, Sicherheitslücken innerhalb weniger Monate zu erkennen und zu melden. In rund eineinhalb Jahren sollten sie zudem Produkte bereitstellen, die dem Prinzip ‚Security by Design‘ entsprechen. Je mehr Produkte betroffen sind, desto wichtiger wird die Durchführung einer angemessenen Risikoanalyse und -bewertung des eigenen Produktportfolios. Denn letztlich kann nur sie die zentrale Frage beantworten: Welche Maßnahmen sind erforderlich, um ein Produkt CRA-konform zu gestalten?

Wie wird ein Produkt CRA-konform?

An einem Beispiel lassen sich verschiedene Antworten skizzieren:

- Ein vorhandener, individuell entwickelter Controller entspricht bereits den Kriterien für „Security by Design“ und benötigt allenfalls kleinere Software-Updates. Dann sollte die Einhaltung des CRA-Stichtags keine größeren Probleme bereiten.
- Der Controller lässt sich mit vertretbarem Aufwand an die Anforderungen des CRA anpassen, beispielsweise durch größere Software-Updates oder eine grundlegende Neuprogrammierung, gegebenenfalls ergänzt durch kleinere Hardware-Upgrades. In diesem Fall sollte der Entwicklungsprozess frühzeitig gestartet werden.
- Die Vorgaben des CRA erfordern eine weitgehende oder vollständige Neuentwicklung. Diese Antwort führt zu weiteren Entscheidungen: Ist es zeitlich möglich und wirtschaftlich sinnvoll, die Entwicklung eines neuen individuellen Controllers anzustoßen, oder ist ein Wechsel zu einer Standardlösung die geeignetere Alternative?

TARA liefert Antworten

Vor diesem Hintergrund empfiehlt sich der Einsatz einer strukturierten Bedrohungsanalyse nach dem TARA-Standard („Threat Analysis and Risk Assessment“). Der CRA schreibt dies zwar nicht ausdrücklich vor, verlangt von Herstellern jedoch angemessene Maßnahmen zur Identifikation von Bedrohungen, zur Ableitung von Schutzmaßnahmen sowie zum Nachweis von ‚Security by Design‘ und Compliance.
Grossenbacher empfiehlt Kunden den Einsatz von TARA, da die Methode technische, organisatorische und betriebliche Aspekte gleichermaßen berücksichtigt, eine nachvollziehbare Dokumentation ermöglicht und die Anforderungen des CRA unterstützt.

Systemverständnis

TARA beginnt auf organisatorischer Ebene: Alle relevanten Produkt-Stakeholder aus Bereichen wie Entwicklung, Supply Chain und Anwendung müssen eingebunden werden. Was zunächst unspektakulär erscheint, erweist sich in der Praxis häufig als anspruchsvoll. Denn bereits die systematische Bestandsaufnahme der technischen Anforderungen zeigt oftmals, dass Anpassungen an Soft- oder Hardware erforderlich sind. Dadurch entsteht schrittweise ein besseres Verständnis für die Auswirkungen des CRA auf Produkt und Prozesse.
Im nächsten Schritt werden nicht nur konkrete Security-Features abgeleitet. Sobald Produktverantwortliche, Systemarchitekten, Servicetechniker etc. Cyberrisiken und Bedro-

hungen im realen Einsatz bewerten, wird auch der Einfluss des CRA auf den gesamten Entwicklungsprozess sichtbar.

Systemabgrenzung

Im nächsten Analyseschritt wird das betrachtete System eindeutig definiert. Ziel ist ein für alle Beteiligten verbindliches und dokumentiertes Verständnis darüber, welche Komponenten, Schnittstellen und Funktionen analysiert werden.
Typische Embedded-Systeme verfügen über eine Vielzahl potenzieller Angriffspunkte: lokale Schnittstellen wie USB oder SD-Karte, Debug-Interfaces wie JTAG, Netzwerkverbindungen über WLAN oder Ethernet sowie drahtlose Kommunikationsschnittstellen wie Bluetooth. Zudem können selbst Displays sicherheitsrelevant sein. Eine Visualisierung in Form von Blockdiagrammen oder Netzplänen schafft Transparenz und bildet die Grundlage für die weiteren Analyseschritte.

Security Context

Anschließend folgt die Beschreibung des Security Context. Dabei werden Annahmen über Einsatzumgebung, Nutzungsverhalten und Betriebsanforderungen dokumentiert. Sie definieren, unter welchen Bedingungen ein Produkt als sicher gilt.
Zum Security Context gehören auch physische Zugangsbeschränkungen, Netzwerkarchitekturen oder Anforderungen an die Passwortsicherheit. Der CRA verlangt ausdrücklich eine solche Kontextdefinition, da sie die Grundlage für eine realistische Risikobewertung und die Abgrenzung zwischen Herstellerverantwortung und Betreiberpflichten bildet.

Eine strukturierte Bedrohungsanalyse nach dem TARA-Standard umfasst mehrere Stufen und liefert wichtige Entscheidungsgrundlagen für Maschinenbauer und Industrieausrüster.

Inventur von Assets

Anschließend werden schutzwürdige Assets und Schnittstellen identifiziert sowie hinsichtlich Protokollen, Zugriffsmöglichkeiten und übertragener Daten analysiert. Dazu gehören beispielsweise Fernwartungszugänge über SSH, Datenschnittstellen wie MQTT oder lokale Konfigurationsschnittstellen.
Zu den schutzwürdigen Assets zählen neben Zugangsdaten und personenbezogenen Informationen auch Firmware, Konfigurationsdateien und proprietäre Algorithmen. Auch Hardwarekomponenten können kritische Assets darstellen, wenn ihr Ausfall oder ihre Manipulation den Systembetrieb beeinträchtigt.
Bei einem Controller mit Betriebssystem erfolgt die Betrachtung auf drei Ebenen: Hardware, Betriebssystem- und Applikationssoftware. Bei mikrocontrollerbasierter Hardware verschmelzen Betriebssystemfunktionen für den sicheren Betrieb mit der Applikationssoftware zu einer sicheren und updatefähigen Firmware.
Diese strukturierte Erfassung schafft Transparenz und bildet die Grundlage für die eigentliche Risikobewertung.

Wirkung und Wahrscheinlichkeit

Die Risikobewertung im engeren Sinne betrachtet zwei Dimensionen: die mögliche Schadensauswirkung und die Eintrittswahrscheinlichkeit. Die Auswirkungsanalyse befasst sich mit den Folgen eines erfolgreichen Angriffs, beispielsweise Systemausfällen, Datenverlusten, Sicherheitsrisiken für Personen, regulatorischen Folgen sowie wirtschaftlichen Schäden und Reputationsverlusten. Für die Bewertung der Eintrittswahrscheinlichkeit empfiehlt sich eine differenzierte Betrachtung von Ausgesetztheit und Ausnutzbarkeit. Während die Ausgesetztheit beschreibt, wie zugänglich eine Schnittstelle ist, bewertet die Ausnutzbarkeit den technischen Aufwand eines Angriffs.

Bedrohungen und Maßnahmen

Auf Basis dieser Vorarbeiten werden konkrete Bedrohungsszenarien identifiziert. Methoden wie Angriffsbäume helfen dabei, mögliche Angriffspfade systematisch zu analysieren. Hierfür ist ein breites Expertenwissen entscheidend, da viele Risiken aus der spezifischen Kombination von Hardware, Firmware und Einsatzumgebung entstehen.
Aus den Bewertungen ergibt sich ein Risikoniveau, typischerweise anhand einer mehrstufigen Matrix, von „akzeptabel“ über Zwischenstufen bis hin zu „nicht akzeptabel“. Risiken der letzten Kategorie erfordern zwingend Gegenmaßnahmen, die auf unterschiedlichen Ebenen ansetzen können: Eine stärkere Authentifizierung reduziert die Ausnutzbarkeit, deaktivierte Schnittstellen verringern die Ausgesetztheit, und Fail-Safe-Konzepte begrenzen potenzielle Schäden.
Wichtig ist, dass alle Maßnahmen systematisch dokumentiert und in die Produktanforderungen integriert werden. Dabei sollte die grundlegende Zielsetzung des CRA berücksichtigt werden: die nachvollziehbare und angemessene Beherrschung von Sicherheitsrisiken während des gesamten Produktlebenszyklus, nicht die vollständige Eliminierung sämtlicher Risiken.
Die zentrale technische Maßnahme bleibt die Umsetzung einer sicheren, schlüsselgestützten Updatefähigkeit. Ohne sie ist eine CRA-Konformität nicht möglich.

TARA als dauerhafte Aufgabe

Da neue Funktionen, Updates oder veränderte Einsatzbedingungen die Risikolage jederzeit verändern können, kann TARA zu einer dauerhaften Aufgabe und einem festen Bestandteil moderner Embedded-Entwicklung werden. Dazu gehört auch die kontinuierliche Überwachung der Sicherheit aller eingesetzten Softwarekomponenten.
Unternehmen stehen daher vor wichtigen Entscheidungen: einer frühzeitigen Durchführung von TARA sowie der Auswahl geeigneter Partner und Prozesse, um die Anforderungen des CRA rechtzeitig erfüllen zu können. ag

Oliver Roth
ist CEO von Grossenbacher Systeme und der Amalthea Gruppe.