White Paper

Integrierte Cyber-Security: EtherCAT schützt bereits zuverlässig

Dr. Guido Beckmann[1], Technical Committee Chair, EtherCAT Technology Group
Florian Essler[1], Conformance TWG Chair, EtherCAT Technology Group
Torsten Förder[1], Cybersicherheits-Experte, Beckhoff Automation
Alexander W. Köhler[2], S&S Principal Security Advisor Cybersecurity, UL Solutions Germany
Fatma Kotzaoglan, Senior Project Engineer, UL Solutions United Kingdom
Martin Rostan, Executive Director, EtherCAT Technology Group

[1]Member of CENELEC TC65X WG3 Cyber Security
[2]DKE TBKON Chair of the Cybersecurity Advisory Board for Conformity Assessment

EtherCAT erfüllt mit seinen Cybersecurity- und Systemsicherheitsfunktionen die Anforderungen von Security Level 2 gemäß IEC 62443. Für nahezu alle gängigen Anwendungen ist keine Modifikation oder Erweiterung des EtherCAT-Protokolls erforderlich, um die CRA-Konformität zu erreichen. Für Angriffe bis Security Level 3 reichen abwärtskompatible Softwareerweiterungen aus. Dies wird von UL Solutions bestätigt, das drei auf EtherCAT basierende Systemklassen bewertet und nach IEC 62443-3-3 zertifiziert hat.

Der europäische Cyber Resilience Act (CRA) hat die Cybersicherheit auch für Feldbussysteme auf die Agenda gesetzt. Der CRA legt die Anforderungen an Cybersicherheit von Produkten mit digitalen Elementen fest; hierzu zählen nicht nur Automatisierungskomponenten, sondern auch die damit ausgestatteten Maschinen und Anlagen. In Asien und Amerika werden ähnliche Gesetze vorbereitet, das Thema ist damit weltweit relevant.

Künftig müssen daher auch Feldbussysteme die Anforderungen des CRA erfüllen. Die Branche geht sehr unterschiedlich mit dieser Herausforderung um.

Klassische Feldbussysteme, aber auch manche Industrial Ethernet Systeme ziehen sich auf eine Art Zellenschutzkonzept zurück, quasi das „IT-Zoning“ im OT-Bereich: Die Kommunikation der Zelle bzw. Zone nach außen wird durch IT-Security-Maßnahmen wie Firewalls, Verschlüsselung und Zugriffskontrollen geschützt, sodass für Kommunikation und Komponenten innerhalb der Zelle kein zusätzlicher Schutz erforderlich sein soll. Voraussetzung für einen wirksamen Schutz ist allerdings, dass innerhalb der Zelle kein fahrlässiger oder gezielter Cyberangriff stattfinden kann: Folgerichtig müssen Bedienende und andere Personen effektiv vom direkten Zugriff auf den Feldbus ausgeschlossen werden.

Das mag funktionieren, wenn das Feldbussystem auf einen verschlossenen Schaltschrank beschränkt ist. Erstreckt sich die Zelle jedoch über eine ganze Maschine oder Anlage, bei der Feldbusleitungen physisch zugänglich sind, wird das schwierig. Zoning steht außerdem im Gegensatz zum Anspruch „vom Sensor bis zur Cloud“ — ein Claim-to-Fame mancher Busarchitekturen, der durch die Security-Anforderungen obsolet wird.

Andere Ansätze verlangen, IT-Security in jedes Feldgerät zu integrieren. Mit authentifizierter Verschlüsselung bis in die E/A-Baugruppe lassen sich die Anforderungen des CRA auch für Industrial-Ethernet-Systeme erfüllen, die dem Bedienpersonal zugänglich sind. Das verschlechtert jedoch nicht nur die Performance des Bussystems spürbar, sondern erhöht auch die Komplexität: Der Umgang mit Zertifikaten, die regelmäßig erneuert werden müssen, erschwert nicht nur die Inbetriebnahme, sondern vor allem die Wartung von Maschinen und Anlagen erheblich.

Da EtherCAT Standard-Ethernet-Frames (IEEE 802.3) und die übliche Ethernet-Physik nutzt, wird manchmal angenommen, es müsse aus Cybersicherheits-Sicht wie ein Ethernet-Netzwerk behandelt und mit denselben bewährten IT-Maßnahmen für Switch-basierte Ethernet-Netze geschützt werden.

Dies trifft jedoch nur teilweise zu, da die besonderen Eigenschaften von EtherCAT viele aus der IT-Welt bekannte Angriffsszenarien von vornherein unmöglich machen und die üblichen Abwehrmaßnahmen daher auch nicht erforderlich sind. Wenn dies nicht berücksichtig wird, prüfen IT-Security-geschulte Experten, ob die gängigen IT-Maßnahmen vorhanden sind - nicht vorhandene Maßnahmen führen dann pauschal zu einer Abwertung. Den besonderen Eigenschaften von EtherCAT wird dies jedoch ebenso wenig gerecht wie die Forderung nach einem Dieselpartikelfilter einem Elektroauto gerecht werden würde.

EtherCAT verfolgt einen anderen Ansatz: Er orientiert sich an der IEC 62443, dem internationalen Standard für die Cybersicherheit von industriellen Automatisierungs- und Steuerungssystemen. IEC 62443 gilt in diesem Bereich als der international anerkannte Standard, der derzeit in Europa erweitert wird, um als Grundlage für die Beurteilung von Systemen und Komponenten im Sinne des CRA zu dienen. Der Standard passt auch deshalb gut zum CRA, weil beide einen risikoorientierten Ansatz verfolgen: soviel Cybersicherheit Maßnahmen wie nötig, nicht wie möglich. Dabei müssen die Risiken stets im Kontext der konkreten Anwendung und der erwarteten Angriffsstärke bewertet werden: Eine industrielle Waschmaschine ist deutlich weniger gefährdet als eine Anlage zur Energieverteilung, die der kritischen Infrastruktur angehört.

IEC 62443-3-3 beschreibt die Security Anforderungen an *Systeme* (nicht an einzelne Komponenten) und ist damit für ein System wie EtherCAT der geeignete Standard.

Die Norm gliedert die sieben Basis-Anforderungen („Foundational Requirements“) in über 100 Systemanforderungen („System Requirements“) und kategorisiert mittels Security Levels die jeweils zu berücksichtigende Angriffsstärke.

Security Level (SL) 1 entspricht dem Schutz vor zufälligen oder unbeabsichtigten Störungen, etwa durch Malware oder Ransomware im Fabriknetz. SL 2 deckt gezielte Angriffe durch Akteure ohne spezielles Expertenwissen ab SL 3 setzt bereits Expertenwissen, entsprechende Ressourcen und Motivation des Angreifers voraus. SL 4 schließlich adressiert Angreifer mit Fähigkeiten und Ressourcen, wie sie typischerweise nur staatlichen Akteuren zur Verfügung stehen — ein wirkungsvoller Schutz gegen derartige Angriffe ist praktisch kaum erreichbar und in den meisten Fällen wirtschaftlich nicht darstellbar.

EtherCAT Funktionsweise

Ein grundlegendes Verständnis der besonderen Funktionsweise von EtherCAT ist notwendig, um die besonderen Eigenschaften der Technologie und damit auch die besonderen Merkmale hinsichtlich der Cybersicherheit zu verstehen. Daher hier ein kurzer Überblick:

EtherCAT ist eine Industrial-Ethernet-Technologie, bei der das sogenannte MainDevice – in der Regel die Steuerung des Automatisierungssystems – die Ethernet-Frames sendet, die von den SubDevices, also den Feldgeräten, verarbeitet werden. Das MainDevice sendet die Frames über eine herkömmliche Ethernet-Schnittstelle mit einem Medium Access Controller (MAC) gemäß IEEE 802.3. Die SubDevices verwenden anstelle des MAC einen speziellen EtherCAT SubDevice Controller (ESC). Der ESC ist nicht in der Lage, selbst Frames zu senden.

EtherCAT nutzt das Prinzip der On-the-Fly-Verarbeitung. Im Gegensatz zu herkömmlichen Industrial-Ethernet-Netzwerken, in denen ein MAC den für das Feldgerät

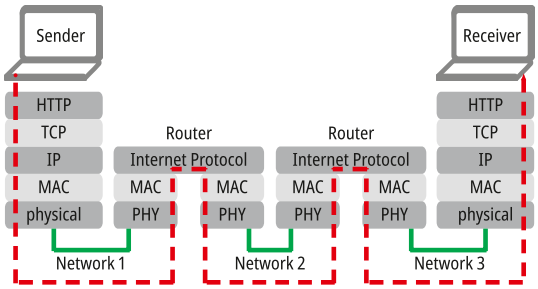
bestimmten Ethernet-Frame empfängt und dann zur Verarbeitung an den Software-Stack des Host-Controllers weiterleitet, verarbeitet EtherCAT die Frames kontinuierlich im oben genannten ESC. Das EtherCAT- SubDevice leitet das Frame daher bereits weiter, während es noch empfangen wird. Das Frame erfährt dabei nur die physikalisch minimale Verzögerung. Das Prinzip der Verarbeitung im Durchlauf erfordert die Hardware-Implementierung der ESC-Funktionalität: Da zu jedem Zeitpunkt nur wenige Bits des Frames zugänglich sind, stehen nur wenige Nanosekunden für die Verarbeitung zur Verfügung. Die ESC-Funktionalität kann daher nicht in Software implementiert werden. Die Hardware-Implementierung des EtherCAT-SubDevice-Controllers hat aus Sicht der Cybersicherheit den Vorteil, dass sie nur mit großem Aufwand manipuliert werden kann.

Außerdem werden die Frames immer mit einer festen Verzögerung verarbeitet. Einige der wichtigsten Funktionen der Chips sind auch vom Applikations-Controller im Feldgerät aus nicht zugänglich: So kann beispielsweise die Einstellung, welche Daten aus dem durchlaufenden Ethernet-Frame entnommen oder in diesen eingefügt werden sollen, nur extern über das EtherCAT-Bussystem, also vom MainDevice, geändert werden – nicht jedoch durch möglicherweise fehlerhafte oder manipulierte Firmware im Feldgerät.

EtherCAT Systemeigenschaften

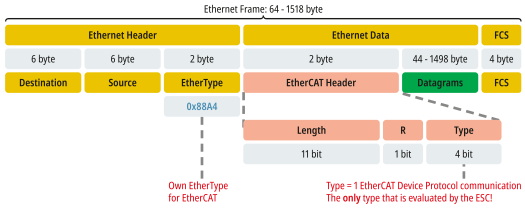
Betrachten wir nun die besonderen systembezogenen Eigenschaften von EtherCAT und deren Auswirkungen auf potenzielle Cyber-Sicherheitsangriffe:

1. Die Systemarchitektur von EtherCAT minimiert die Angriffsfläche. Kein Software-Stack hat Zugriff auf die Frames, wenn sie durch das SubDevice laufen, sondern nur die Hardware-Logik verarbeitet sie. Es gibt nur EtherCAT-Frames im Medium. Nur das MainDevice kann EtherCAT-Frames generieren
2. Das EtherCAT-Protokoll ist direkt in das Ethernet-Frame eingebettet und befindet sich somit auf Schicht 2 des ISO-OSI-Modells. Das Internetprotokoll (IP) auf Schicht 3 wird nicht für den Transport der EtherCAT-Nutzdaten verwendet. Da die Hauptaufgabe von IP das Routing von Daten über Subnetze hinweg ist, ist Malware praktisch immer auf das Vorhandensein der IP-Schicht angewiesen: Bösartige Inhalte, die direkt in den Ethernet-Frame eingebettet wären, könnten die Grenzen eines Subnetzes nicht überwinden. Das bedeutet, dass EtherCAT-Feldgeräte von vornherein vor gängigen Malware-Angriffen geschützt sind.



IP als Voraussetzung für Routing von Malware

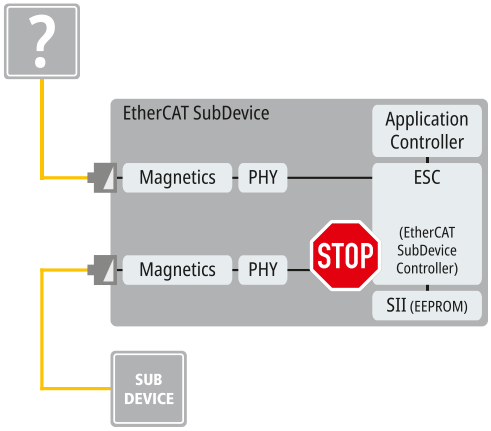
EtherCAT verwendet einen eigenen EtherType (0x88A4), und daran schließt sich der EtherCAT Header an.



EtherCAT: direkt im Ethernet Frame

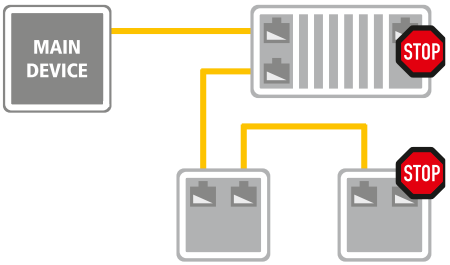
Dadurch können EtherCAT-SubDevice-Controller anhand des Frame- und des EtherCAT-Headers sofort erkennen, ob es sich bei dem ankommenden Frame um einen EtherCAT-Frame handelt.
Alle anderen Frame-Typen werden von der EtherCAT-SubDevice-Controller-Hardware zerstört: Ein Nicht-EtherCAT-Frame, das im EtherCAT-Segment ankommt, wird somit zuverlässig vom nächsten Feldgerät entfernt. Das bedeutet, dass Angriffe

durch Nicht-EtherCAT-Frames von vornherein nicht möglich sind.



ESC zerstört alle Nicht-EtherCAT-Frames

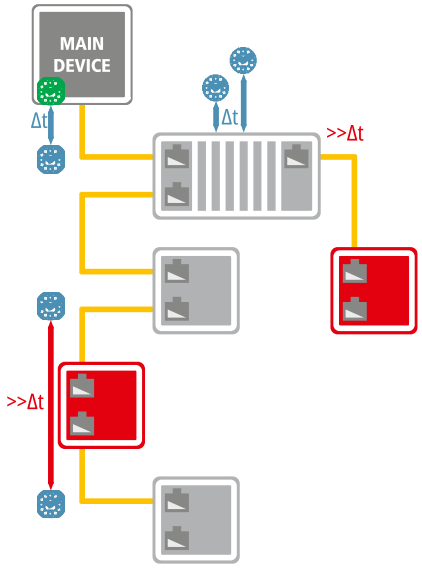
3. EtherCAT-SubDevices können keine Daten ändern, die nicht an sie adressiert sind. Dies gilt für Prozessdaten und Parameterdaten gleichermaßen.
   Da die FMMU – die Hardware-Einheit im ESC, die für die Adresszuweisung der Prozessdaten zwischen lokalem und globalem Speicher zuständig ist – nicht über die lokale ESC-Schnittstelle des SubDevice konfiguriert werden kann, kann eine versehentlich oder absichtlich manipulierte Firmware auf dem Feldgerät diese nicht auf dem Bus aktivieren. Somit hat ein Angriff durch Einfügen eines software-manipulierten Feldgeräts keine Auswirkungen auf andere Geräte.
4. Beim Start des Netzwerks kann das EtherCAT-MainDevice die Eigenschaften aller angeschlossenen SubDevices abfragen und die Netzwerktopologie erkennen. Der Detaillierungsgrad dieser Abfrage kann an die Anforderungen der Anwendung angepasst werden: So kann sich das MainDevice beispielsweise darauf beschränken, beim Start nur den Gerätetyp und dessen Kommunikationseigenschaften abzufragen, oder es kann auch Firmware-Version und Seriennummer vergleichen und so nicht nur das Hinzufügen von Geräten und Änderungen an der Topologie erkennen, sondern auch den Austausch von Geräten.
5. EtherCAT-SubDevice-Controller verfügen über bis zu 4 Ports und unterstützen daher eine Vielzahl von Netzwerktopologien. Nicht verwendete Ports können vom Master abgeschaltet und somit in der Hardware gesperrt werden.



Abschalten nicht verwendeter Ports

   In diesem Fall führt der Anschluss eines Geräts über einen nicht verwendeten Port nicht zu einer logischen Verbindung: Es wird zwar ein Linksignal hergestellt, aber die Kommunikation mit dem ESC wird blockiert. Somit ist der Angriff durch Einstecken eines Geräts in einen offenen Port unwirksam, und kann über den zusätzlichen Link sogar erkannt werden.
6. Der Datenverkehr in EtherCAT-Netzwerken kann über sogenannte „Probes“ überwacht und analysiert werden. Probes sind Hardwaregeräte, die im Netzwerk zwischen MainDevice und Feldgeräten oder zwischen zwei Feldgeräten installiert werden müssen. Diese Geräte können jedoch keine Daten manipulieren – sie können nur empfangen. Eine Probe kann daher zum Aufzeichnen des Datenverkehrs verwendet werden, nicht jedoch zum Ändern von Daten. Es ist äußerst komplex, aus dem Inhalt der aufgezeichneten Prozessdaten die Funktion der Maschine oder Anlage abzuleiten, und ohne genaue Kenntnisse der Maschinenmechanik und der Systemeigenschaften, die nicht über den Bus transportiert werden (z. B. Benennung der Prozessvariablen), ist dies fast unmöglich. Wenn das Ziel des Angriffs also darin besteht, die Funktionsweise der Maschine oder Anlage zu verstehen, ist ein Angriff auf das Steuerungssystem fast immer vielversprechender und effektiver.

7. Auch wenn EtherCAT selbst das Internet-Protokoll (IP) nicht verwendet, ist die Technologie dennoch in der Lage, mit Hilfe der Erweiterung „Ethernet over EtherCAT“ jeglichen Ethernet-Datenverkehr zu tunneln und so beispielsweise Daten von Webservern auf Feldgeräten abzurufen, OPC UA oder andere Protokolle zu transportieren, einschließlich IP-basiertem Datenverkehr. Da dieser Datenstrom getunnelt wird, ist sein Inhalt völlig unabhängig von der Funktionalität von EtherCAT selbst und allen am Transport beteiligten Geräten. Grundsätzlich kann er jedoch die Eigenschaften unzureichend geschützter Feldgeräte am Ende des Tunnels, d. h. des dedizierten Empfängers des Datenstroms aus dem Tunnel, beeinträchtigen. Wenn dies ein zu berücksichtigender und auszuschließender Angriffsvektor ist, kann das Protokoll „Ethernet over EtherCAT” entweder global oder selektiv im MainDevice abgeschaltet werden.
8. Die MainDevices können die Konfigurationsdaten bei jedem Startvorgang auf die SubDevices schreiben. Dank der hohen Effizienz von EtherCAT ist dies möglich. Dadurch werden alle Konfigurationen überschrieben, die möglicherweise offline auf das Gerät geschrieben wurden, sodass auch dieser Angriffsvektor ins Leere läuft.
9. Zu Denial-of-Service-Angriffen (DoS): Da die eingehenden Frames vom ESC in der Hardware verarbeitet werden, sind Bursts kein Problem: EtherCAT-Frames werden sofort verarbeitet. Ein Drei-Puffer-Mechanismus im ESC sorgt dafür, dass immer Speicher für eingehende Prozessdaten verfügbar ist, selbst wenn die Geräte-Firmware mit dem Leeren der Puffer nicht Schritt halten kann. Azyklische Daten wie Parameter werden quittiert, sodass eine Überforderung des Protokoll-Stacks nicht möglich ist. Nicht-EtherCAT-Frames werden von der ESC-Hardware sofort verworfen. Somit sind DoS-Angriffe wirkungslos.
10. Wie gezeigt kann ein SubDevice aufgrund der Eigenschaften des EtherCAT SubDevice Controllers weder Daten verändern noch eigenständig Frames senden. Das Einfügen eines SubDevice ist deshalb kein aussichtsreiches Angriffsszenario; zudem lässt sich das Hinzufügen eines Geräts bei EtherCAT über die dadurch verursachte Änderung der Signallaufzeit erkennen. ESC-Chips messen die Frame-Ausbreitungsverzögerung mit einer Genauigkeit von deutlich unter 50 Nanosekunden. Diese Messwerte liest das EtherCAT MainDevice aus, um die hochpräzise Synchronisation der verteilten Uhren sicherzustellen. Eine signifikante Abweichung dieser Werte – etwa nach einem Neustart – signalisiert eine Änderung der Netzwerktopologie, wie sie beim Einfügen eines Geräts auftreten würde.



Eingefügte Geräte werden über EtherCAT Laufzeitmessung erkannt

11. Selbst das Hinzufügen eines SubDevice, das über eine speziell zu diesem Zweck entwickelte „gefährliche“ EtherCAT SubDevice Controller Hardware verfügt, wird auf diesem Weg erkannt. Die Entwicklung eines solchen Chips erfordert erhebliches spezifisches Know-how und hohen Aufwand, sodass dieser Angriffsvektor sehr ineffizient ist. Nur in sehr wenigen

Systemen ist vorstellbar, dass der erzielbare Effekt – in diesem Fall vermutlich die Sabotage des Systems – den Aufwand wirtschaftlich rechtfertigen würde oder dass es nicht einfacher und kostengünstiger wäre, dies über andere, nicht auf EtherCAT basierende Angriffsszenarien zu erreichen.

Und wie sieht es mit dem Steuerungssystem aus?

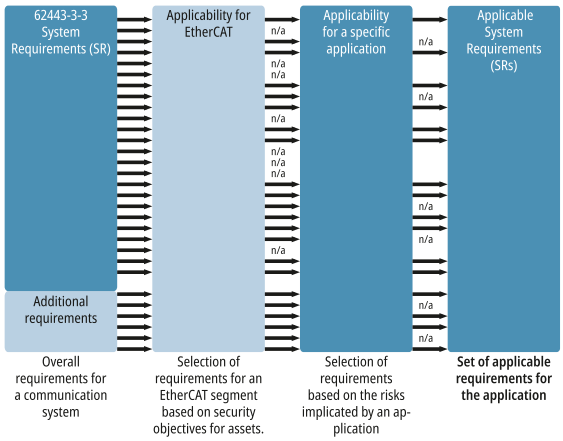
Zusätzlich zu EtherCAT verfügen die meisten EtherCAT-Steuerungen über weitere Schnittstellen, wie beispielsweise einen Ethernet-Anschluss für die Verbindung zu übergeordneten Netzwerken, Speicherkartensteckplätze oder USB-Anschlüsse. EtherCAT-Feldgeräte können ebenfalls über weitere Schnittstellen ähnlicher Art verfügen. Diese müssen natürlich durch geeignete Maßnahmen sehr sorgfältig vor Cybersicherheits-Angriffen geschützt werden! Dieser wesentliche Teil der Cybersicherheits-Strategie ist vom EtherCAT-Netzwerk unbeeinflusst und kann daher nicht zu den Security-Betrachtungen von EtherCAT gehören.

EtherCAT-MainDevice-Implementierungen reichen bewusst und absichtlich von sehr einfachen Geräten für geringe Anforderungen bis hin zu leistungsstarken Steuerungen, die deutlich mehr EtherCAT-Features unterstützen. Auch einige Security-Eigenschaften von EtherCAT hängen von der Implementierung des MainDevices ab. Beispielsweise überprüfen nicht alle Steuerungen das Netzwerk während des Startvorgangs auf Änderungen oder schalten standardmäßig ungenutzte Ports auf SubDevice-Geräten ab. Um entsprechende Cybersicherheits-Anforderungen zu erfüllen, ist es daher notwendig, geeignete MainDevices bzw. Steuerungen auszuwählen.

In der EtherCAT Technology Group werden Profil-Spezifikationen erarbeitet, die sowohl Anwender, Systemintegrator und Maschinenbauer, als auch Gerätehersteller anleiten, welche Maßnahmen genutzt bzw. implementiert werden müssen, um einen entsprechenden Security Level zu erreichen.

EtherCAT erreicht Security Level 2 ohne Modifikationen

Aufgrund der genannten Systemeigenschaften erfüllt die EtherCAT-Technologie bereits ohne Security-spezifische Erweiterungen die Cybersicherheits-Anforderungen für Systeme, gegen die Angriffe der Stärke Security Level 2 zu erwarten sind. Dies wurde in einer aufwändigen Analyse nachgewiesen: Jede der mehr als 100 Systemanforderungen der IEC 62443-3-3 wurde für ein typisches EtherCAT-Anlagennetzwerk detailliert geprüft und bewertet. UL Solutions Germany hat die Security-Eigenschaften des EtherCAT-Protokolls im Betrieb für drei typische Anwendungsszenarien bewertet, was zu drei Zertifikaten nach IEC 62443-3-3 geführt hat, die auf den Anforderungen an die Security-Fähigkeiten basieren und entsprechend der oben beschriebenen Bedrohungsszenarien ausgewählt wurden. Diese drei Zertifikate wurden von UL Solutions (Demko), Dänemark, veröffentlicht, der von der IECEE anerkannten nationalen Zertifizierungsstelle, die aufgrund des globalen MRA-Netzwerks der IECEE sowohl in der EU als auch weltweit offiziell anerkannt ist.



Systemanforderungen: Bewertung von Anwendbarkeit und Erfüllungsgrad für EtherCAT in den betrachteten Szenarien.

Höhere Security-Level ohne Hardwareänderung — nur Software

Für Systeme, die Schutz gegen Stärke eines Angreifers nach Security-Level 3 verlangen, genügen Software-Erweiterungen im MainDevice und im Konfigurationstool. Auch das wurde von UL Solutions bescheinigt. Die SubDevices können also unverändert bleiben. Unter anderem wird für den Schutz gegen diese Angriffsstärke die Laufzeitmessung aktiviert, mit der wie oben beschrieben zusätzliche Geräte im EtherCAT Segment erkannt werden.

Das mit manipulierten Gerätebeschreibungsdateien verbundene Cybersicherheits-Risiko ist bei EtherCAT überschaubar: schließlich werden diese nur einmalig von dem Tool eingelesen, das die Netzwerkkonfiguration erstellt. Eine veränderte Datei könnte zu verändertem Geräteverhalten führen, das wahrscheinlich bei der Inbetriebnahme bzw. dem Funktionstest des Systems auffallen würde. Falls nicht: Die EtherCAT Technology Group (ETG) richtet eine eigene Zertifizierungsstelle (Certificate Authority, CA) ein, damit ETG-Mitglieder EtherCAT-Gerätebeschreibungsdateien und -Software einfach und einheitlich signieren und authentifizieren können.

Optionale Verschlüsselung bei EtherCAT ohne Zertifikats-Handling

Nur in sehr wenigen Anwendungen fordern die Anwender zusätzlich die Verschlüsselung der über das Bussystem übertragenen Prozess- und Parameterdaten, um sie vor dem Mitlesen zu schützen: zwar steht „Verschlüsselung“ auf vielen Cybersicherheits-Checklisten, in der Praxis sind der Schaden und damit das Risiko meist gering, die durch Offenlegung der Daten entstehen könnten. Für Anlagen mit außergewöhnlich hohen Cybersicherheits-Anforderungen erweitert die ETG den EtherCAT-Standard vollständig abwärtskompatibel um eine quantensichere, authentifizierte Verschlüsselungsmethode, die auf Wunsch alle oder nur einen Teil der Daten sichert. Die Schlüsselverteilung erfolgt hierbei ohne Zertifikate, sodass die Erneuerung von Zertifikaten aufgrund des Ablaufdatums eliminiert und das Handling deutlich vereinfacht wird. „Vollständig abwärtskompatibel“ bedeutet dabei sogar, dass die ESC-Chips nicht verändert werden müssen: Diese Funktion lässt sich rein per Software ergänzen — im MainDevice und im SubDevice.

Referenzen:

UL Solutions: 3 Certificates IEC 62443-3-3 and Technical Reports TRF: Solution Application of Capabilities Assessment of EtherCAT Technology. issued by UL Solutions (Demko) Denmark, IECEE Certification Body: DK-177530-UL/DK-178394-UL/DK-178399-UL. IECEE CBTL (testing lab): UL Solutions Northbrook, IL, USA.