März 2024

SAFE NT SECURE

NEWS. TECHNOLOGIES. PEOPLE.

Ethernet:

Eines für alles? Seite 8

Creating safety.
With passion.

NewTec

Liebe Leserinnen und Leser,

täglich 70 neu entdeckte Schwachstellen in Software-Produkten verzeichnet der Lagebericht des BSI für das Jahr 2023. Das ist ein Anstieg von rund 25 Prozent gegenüber dem Vorjahr, über den sich wohl nur diejenigen freuen, die sich nach lohnenden Alternativen für Banküberfälle und Betäubungsmittelhandel umschauen. Für kleine und mittlere Unternehmen dagegen besteht laut Bericht besonderer Anlass zur Sorge, weil hier – u. a. wegen Personalmangels und Unkenntnis des eigenen Risikoprofils – oft nicht einmal regelmäßige Sicherheitsupdates installiert werden.

Die EU versucht derweil, mit dem Cyber Resilience Act und branchenspezifischen Regularien wie der Maschinen- oder Medizinprodukteverordnung „vor die Welle" zu kommen – um eine Formulierung aus dem Vorwort des BSI-Lageberichts aufzunehmen. Mehr dazu lesen Sie auf den Seiten 10 und 11 dieser Ausgabe.

Am Rande ist Security auch ein Thema unseres aktuellen Schwerpunkt-Artikels. Aber nur ganz am Rande, denn hier geht es um die außerordentliche Erfolgsgeschichte einer Netzwerktechnologie, eines Tausendsassas mit besten Zukunftsaussichten: dem Ethernet.

In diesem Sinne: Viel Spaß bei unserer Reise durch die Geschichte und die Anwendungsbereiche des Ethernets. Und natürlich auch bei all den anderen spannenden Geschichten dieser Ausgabe!

Matthias Wolbert
Geschäftsführer NewTec GmbH, Vertrieb & Marketing

Common-Criteria-Evaluation durch NewTec

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat zwei Security-Spezialisten von NewTec als Common-Criteria (CC)-Evaluatoren anerkannt. Damit können wir Hersteller und Entwickler nun mit der für eine CC-Zertifizierung erforderlichen technischen Bewertung unterstützen und sie von der Erstellung der Sicherheitsvorgaben bis zur Zertifizierung begleiten.

Die Common Criteria sind ein international anerkannter Standard zur Bewertung und Prüfung der Sicherheitsfunktionalitäten von Hard- und Software. Eine CC-Evaluation ist Voraussetzung für die CC-Zertifizierung eines Produkts durch das BSI. Anhand eines solchen Zertifikats können Anwender einschätzen, ob das jeweilige Produkt sicherheitstechnisch für einen bestimmten Einsatzzweck geeignet ist.

Vom BSI anerkannte CC-Evaluatoren: Stephan Strohmeier & Matthias Lai

SPS 2023: Safety und Security in Nürnberg

Im November war wieder SPS-Time in Nürnberg. Die Messebesucher trieb vor allem das Thema Security an den NewTec-Stand. Denn das Bewusstsein wächst, dass funktionale Sicherheit kaum ohne Security zu erreichen ist. Viele Fragen gab es zur Umsetzung regulatorischer Anforderungen. Häufig wurde auch konkrete Unterstützung angefragt. Meist konnten wir bereits vor Ort Lösungen aufzeigen.

Auch das Interesse an der NTSafe-Flex-Familie war anhaltend hoch. Neben den Vorteilen einer schnellen, kostengünstigen Entwicklung stand die Option im Vordergrund, dabei flexibel auf FPGA oder verschiedene Mikrocontroller zu setzen. Insbesondere in Hinblick auf mögliche Lieferengpässe bei Mikrochips begrüßten viele Besucher die Aussicht, die Abhängigkeit von bestimmten Chipherstellern mit den alternativen Entwicklungsplattformen SafeFlex STM32 und der neuen SafeFlex SAM D21 zu verringern.

Und dann war da noch das große Thema künstliche Intelligenz: Viele Unternehmen präsentierten KI-basierte Lösungen und Lösungsansätze, etwa im Bereich Predictive Maintenance. Am NewTec-Stand wurde vor allem diskutiert, wie KI-gesteuerte Prozesse funktionssicher (safe) gestaltet werden können.

CySecMed 2023

Am 17. und 18. Oktober fand in München die CySecMed, eine Konferenz zur Informationssicherheit in der Medizintechnik, statt. Im Mittelpunkt standen vor allem die einschlägigen Normen (mehr zu dem Thema auf S. 12), das Risikomanagement und die rechtlichen Aspekte von Cybersecurity.

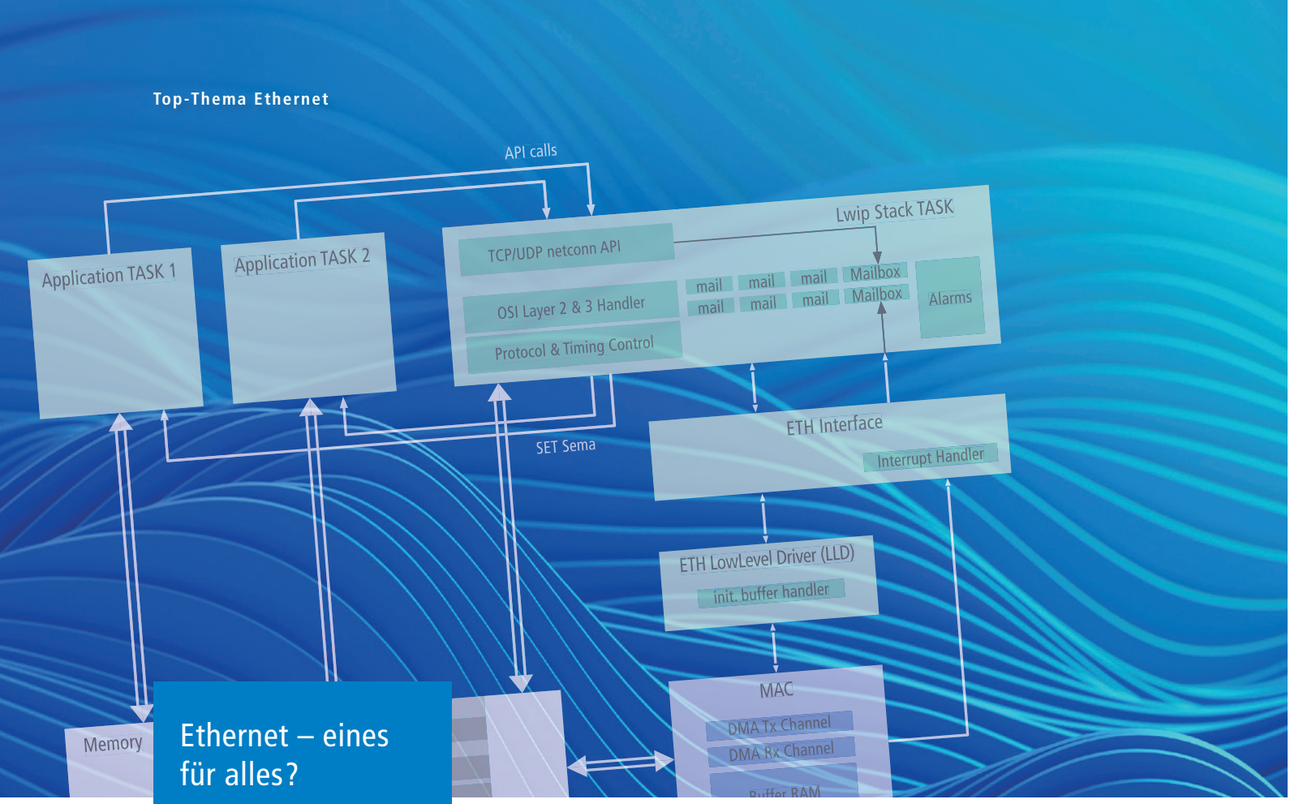
Als CySecMed-Partner war NewTec auch als Aussteller präsent. Dabei galt das Interesse der Standbesucher besonders dem Thema Security-Lifecycle und der Frage, wie die Security-Anforderungen der MDR (Medical Device Regulation) mithilfe der IEC 62443 umgesetzt werden können.

Messetermine 2024

Embedded World
Nürnberg
9. bis 11. April
Embedded Systems

Innotrans
Berlin
24. bis 27. September
Railway

SPS
Nürnberg
12. bis 14. November
Industrie



Ethernet – eines für alles?

Der Siegeszug des Ethernets dauert schon mehrere Jahrzehnte an und hat inzwischen fast alle Branchen erreicht.

Wenn es um kabelgebundene Vernetzung geht, kommt man heute kaum an dieser Netzwerktechnologie vorbei. Wir werfen einen Blick auf die Geschichte von Ethernet, die Gründe des Erfolgs, die verschiedensten Anwendungsbereiche und auf zukunftsweisende Entwicklungen.

Die Älteren unter uns erinnern sich vielleicht noch an den Kabelwildwuchs und das Haareraufen, das bis Mitte der 1990er Jahre herrschte, wenn es darum ging, Server, Rechner und Peripherie zu vernetzen. Damals gab es für diesen Zweck jede Menge proprietärer Systeme, die fast ausschließlich auf Punkt-zu-Punkt-Verbindungen ausgelegt waren. Das änderte sich mit ISO/IEC 11801, einem internationalen Standard für die anwendungsneutrale Verkabelung von Telekommunikationsanlagen, und der damit weitgehend identischen europäischen Norm DIN EN 50173. Mit ihrer Veröffentlichung im Jahr 1995 wurden zahlreiche Hemmschuhe für die wachsenden Local Area Networks (LAN) in den Büros ausgeräumt. Mit den Standards wurde es nun möglich, Rechner und Peripherie quasi per Plug und Play zu vernetzen.

Das Erfolgsgeheimnis der mehrfach erweiterten Normen liegt in der Vereinheitlichung der Topologie, der Klassifizierung der Übertragungsstrecken und der Definition einer einheitlichen Schnittstelle für Endgeräte. Dabei basieren IEC 11801 und DIN EN 50173 im Wesentlichen auf einer Entwicklung von Robert Metcalfe, die er Mitte der 1970er Jahre am Xerox Palo Alto Research Center angestoßen und später mit der von ihm eigens gegründeten Firma 3Com vorangetrieben hatte: dem Ethernet.

Heute hat sich Ethernet zur dominierenden LAN-Technik entwickelt, mit Bandbreiten von 1 Gbit/s oder 10 Gbit/s; für anspruchsvollere Anwendungen gibt es Verbindungen bis 400 Gbit/s. Und DIN EN 50173 wurde unterdessen um weitere Anwendungsbereiche wie etwa Wohngebäude (DIN EN 50173-4), Rechenzentren (DIN EN 50173-5) oder industriell genutzte Bereiche (DIN EN 50173-3) erweitert. Schnell war nämlich klar geworden, dass von den Vorteilen des einheitlichen Netzdesigns, der Topologie und der Übertragungstechnik zahlreiche andere Anwendungsbereiche profitieren konnten, auch solche, die außerhalb der Normenfamilie DIN EN 50173 liegen.

Im Folgenden wollen wir einen kurzen Blick auf Möglichkeiten werfen, die Ethernet in einigen Anwendungsbereichen bietet, und darauf, wie die dortigen spezifischen Bedingungen und Anforderungen mit Ethernet umgesetzt werden.

Industrial Ethernet

Auf der Feldbus-Ebene sieht es in vielen Fertigungshallen immer noch ähnlich aus wie Mitte der 1990er Jahre in den Bürogebäuden. Es gibt eine große Vielfalt systemspezifischer Verbindungen, die eine flexible, konvergente Nutzung der gesamten Infrastruktur unmöglich macht. Der Grund: Das Feldbus-System, das Sensoren und Aktuatoren mit der Steuerung verbindet, orientiert sich meist ausschließlich an der eingesetzten Steuerung.

Um die Erfordernisse moderner Produktion (Stichwort Industrie 4.0/ Industrial Internet of Things) erfüllen zu können, werden neue Anlagen daher zunehmend mit Ethernet-Technologie vernetzt und bestehende Anlagen umgestellt. Da die Umgebung und die Anforderungen im Produktionsumfeld allerdings andere sind als in Büroetagen, gelten für Industrial Ethernet etliche Besonderheiten. Das betrifft zum einen die physischen Verbindungen, die gegen Staub und Spritzwasser geschützt, öl- und säurebeständig sowie unempfindlich gegen Vibrationen und elektromagnetische Einstreuungen sein müssen.

Zum anderen müssen auch die Übertragungsprotokolle besondere Anforderungen erfüllen, insbesondere hinsichtlich der Übertragungsgeschwindigkeit und -sicherheit. In den 2000er Jahren entstand daher eine Reihe spezifischer, echtzeitfähiger Industrial-Ethernet-Systeme wie EtherCAT, EtherNet/IP, Ethernet POWERLINK, Profinet, Profisafe oder SafetyNET p. Jedes dieser Systeme hat individuelle Stärken, so ist EtherCAT auf eine exakte Synchronisierung, geringen Jitter (Genauigkeitsschwankung im Übertragungstakt) und geringe Hardwarekosten ausgelegt; Safety-NET p und Profisafe bieten Vorteile bei der Übertragung sicherheitsgerichteter Informationen bis SIL 3.

Mit diesen Ethernet-Systemen können neue Produktionsanlagen recht günstig in einer leistungsfähigen, flexiblen Dateninfrastruktur vernetzt werden. Bei bestehenden Anlagen allerdings kann der Aufwand erheblich sein. Denn hier gilt es, alles neu zu verkabeln, Maschinen generationsübergreifend zu verbinden und in diesem Zuge alte Maschinen mit Schnittstellen, ethernetfähigen Sensoren, Switches etc. auszurüsten.

Für eine effiziente Produktionssteuerung muss die Feldebene zudem an übergeordnete Ebenen zur Produktionssteuerung (SCADA), Produktionsüberwachung (MES) und Produktionsplanung angebunden werden, was mit besonderen Bedingungen für den Datenaustausch einhergeht.

Moderne Kommunikationsstandards für Ethernet – z.B. OPC UA

Viele Industrie-4.0-Anwendungen wie z. B. Dienste zur Prozessoptimierung sind darauf angewiesen, dass Maschinen und Komponenten eine semantische Beschreibung der Daten bereitstellen. Klassische Protokolle für die Vernetzung auf Feldebene sind aber auf die zuverlässige Übertragung von Rohdaten ausgelegt – semantische Datenstrukturen spielen hier keine große Rolle.

Für die Interoperation mit übergeordneten Ebenen bieten sich daher moderne Kommunikationsstandards wie OPC UA (OPC Unified Architecture) an, mit denen auch kontextbezogene, semantische Datenstrukturen ausgetauscht werden können. OPC UA ist ein offener, plattformunabhängiger Kommunikationsstandard, der inzwischen von vielen modernen Maschinen unterstützt wird.

Wo es um die sichere Vernetzung und Cloud-Anbindung von Maschinen und Anlagen geht, unterstützt NewTec Hersteller und Anwender mit **NTSecureCloudSolutions**. Das Lösungspaket enthält verschiedene Software- und Hardwarelösungen für sichere IIoT-Anwendungen. Mit dem **NTSecureGateway** können beispielsweise Maschinen, Anlagen oder Sensoren sicher per Ethernet verbunden werden. Dank umfassender Integrationsmöglichkeiten einschließlich eines eingebauten OPC-UA-Servers lassen sich alle Komponenten zudem ohne großen Entwicklungsaufwand direkt an das Leitsystem anschließen.

Mehr zur NTSecureGateway 1000 Family erfahren Sie unter:
https://www.newtec.de/loesungen/plattformen/ntsecuregateway-1000-family/

PROFIsafe
EtherCAT®
EtherNet/IP™
ETHERNET POWERLINK
PROFINET INDUSTRIAL ETHERNET

Automotive Ethernet

Ethernet ist längst nicht mehr auf den Einsatz in Gebäuden beschränkt. Mit zunehmender Digitalisierung gilt es auch bei Straßenfahrzeugen, neue Wege zur sicheren, schnellen und flexiblen Vernetzung einzuschlagen. Derzeit sind die verschiedenen Schlüsselfunktionen in Autos – beispielsweise für die Karosseriesteuerung, den Antriebsstrang, das Infotainment oder die Telematik – mit unterschiedlichen Bus-Systemen verbunden (CAN, LIN etc.). Bei einer wachsenden Anzahl zu vernetzender Sensoren, Aktoren und Steuergeräte sowie bei begrenztem Raum und Anforderungen an ein möglichst geringes Gewicht stoßen diese Systeme aber an ihre Grenzen.

Auch im Fahrzeugbau wird daher zunehmend Ethernet-Technologie eingesetzt. Für bestimmte Funktionen wie die Diagnose oder das Flashen von Steuergeräten hat sich Automotive Ethernet bereits etabliert. Auch für Audio- und Videoübertragung im Infotainmentbereich wird mit AVB (Audio Video Bridging) eine Ethernet-Technologie eingesetzt. Neben Standardprotokollen wie TCP/IP, UDP/IP oder ICMP kommen für verschiedene Anwendungen spezifische Protokolle wie Diagnostics over IP (DoIP) und Scalable Service-Oriented Middleware over IP (SOME/IP) zum Einsatz.

Zunehmend wird Automotive Ethernet auch für andere sicherheitsrelevante Schlüsselfunktionen wie die modernen Fahrassistenzsysteme (ADAS) genutzt. Da es sich hier um sicherheitskritische Anwendungen handelt, sind besonders geringe Latenzzeiten, deterministische Datenübertragung und garantierte Bandbreiten erforderlich. Daher kommt in diesem Bereich das sogenannte Time-Sensitive Networking (TSN) zum Einsatz (mehr zu TSN im nächsten Kapitel).

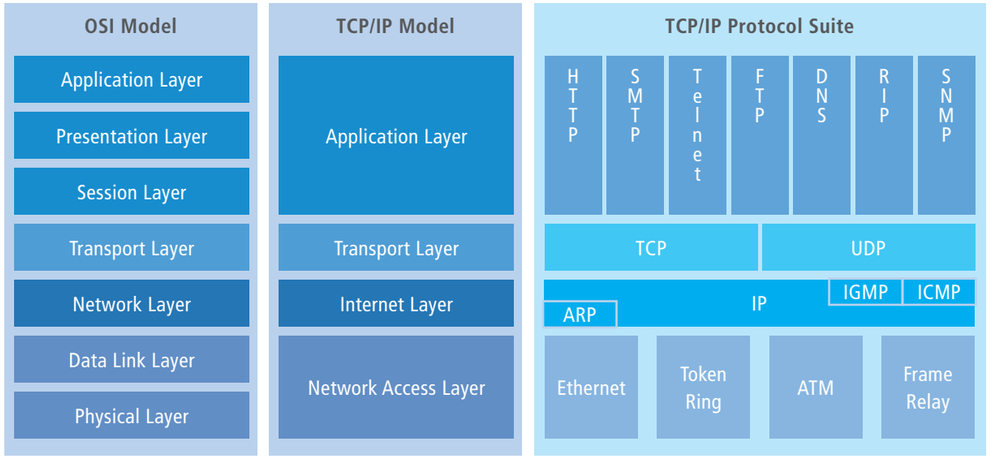
Allerdings gelten in Fahrzeugen spezielle Umgebungsbedingungen. Hohe Temperaturen, große Temperaturschwankungen oder Vibrationen und geringes Platzangebot stellen besondere Ansprüche an Leitungen und Steckverbindungen.

Single Pair Ethernet – Next-Generation Automotive Ethernet?

Single Pair Ethernet (SPE) ist ein moderner Standard für die Datenübertragung über ein einzelnes, verdrilltes Kabelpaar, der durchgängig das TCP/IP-Protokoll nutzt. Ursprünglich wurde SPE für Industrieanwendungen entwickelt, um Sensoren und Steuermodule zu verbinden. Dort stießen herkömmliche, mehrpaarige Verkabelungskonzepte mit ihrem Platzbedarf, ihrer beschränkten Flexibilität und dem höheren Installationsaufwand an Grenzen.

Die Beschränkung auf ein einzelnes Kabelpaar bietet hier deutlich bessere Möglichkeiten. Zudem sind SPE-Verbindungen flexibler – ein entscheidender Vorteil bei bewegten Komponenten oder in verwinkelten Einbausituationen. Auch hinsichtlich der Übertragungsraten ist SPE sehr flexibel. In drei auf dem IEEE 802.3-Standard basierenden Varianten unterstützt SPE derzeit Datenraten von 10 Mbit/s bis 1 Gbit/s – weitere Varianten mit Geschwindigkeiten bis zu 100 Gbit/s sind geplant. Damit bietet SPE bereits heute genügend Bandbreite für echtzeitfähige Datenübertragung.

Bedenkt man zudem das geringe Gewicht, die geringe Verkabelungskomplexität und die günstigen Systemkosten, ist SPE für viele Schlüsselfunktionen im Auto eine gute Wahl – zumal per Power over Data Lines (PoDL) auch die Versorgungsspannung für IP-Komponenten, Sensoren und Aktoren übertragen werden kann.



OSI-Modell vs. TCP/P-Modell und TCP/IP-Protokollsuite

Ethernet auf Schienen

Auch in schienengebundenen Fahrzeugen sind zahlreiche vernetzte Komponenten im Einsatz – von Antrieb und Bremsen über Klimaanlage und Toilettenanlagen bis hin zu Türsteuerungen. Häufig stammen sie von verschiedenen Herstellern und nutzen proprietäre Bussysteme. Diese Vielzahl verschiedener Bussysteme macht das Train Communication Network (TCN) nicht nur komplex und fehleranfällig. Die Uneinheitlichkeit ist vor allem auch ein erhebliches Hindernis für die Interoperabilität der einzelnen Fahrzeugkomponenten und für eine flexible Zugzusammenstellung.

Die Lösung heißt auch hier Ethernet. Seit 2015 sind In der Normenreihe IEC 61375 („Elektronische Betriebsmittel für Bahnen") ethernetbasierte Netzwerke für Wagen (Consist-Netzwerke) und den gesamten Zug (Zug-Backbone) spezifiziert. Als einheitliches Kommunikationsprotokoll dient dabei TRDP (Train Realtime Data Protocol), das den Austausch von Prozess- und Message-Daten ermöglicht und auch die „Zugtaufe" (Kopplung der Wagen im Zugverband) unterstützt. TRDP ist IP-basiert und bietet eine Bandbreite von 1 Gbit/s. Damit können auch die steigenden Performance-Anforderungen moderner Anwendungen und On-Board-Services wie Klimaanlage, Türsteuerung oder Fahrzeugdiagnose erfüllt werden.

TSN – Time sensitive Network

Um in Zukunft auch sicherheitskritische Funktionen wie Bremsen über Ethernet steuern zu können (Stichwort: Drive-by-Data), braucht es eine Echtzeit-Infrastruktur, die Nachrichten in kleinen Sendezyklen deterministisch überträgt. Zukünftige TCN sollen deshalb um den echtzeitfähigen Ethernet-Standard TSN (Time-sensitive Networking) erweitert werden. An der konkreten Ausgestaltung dieser Next-Generation TCN wird derzeit intensiv gearbeitet.

Die sichere Integration von IP-Technologie und TRDP stellt Hersteller von Zugkomponenten vor neue Herausforderungen. NewTec ist Experte für Zugkommunikationsnetze, Mitentwickler von TRDP und Mitglied der TCN-Open-Initiative, die sich für die Entwicklung von Schlüsselkomponenten für zukünftige Kommunikationsstandards im Bahnbereich engagiert.

NewTec unterstützt Sie mit:

- **Beratung** und **Projektbegleitung**
- umfangreichen kundenspezifischen Dienstleistungen für **Entwicklungen** und **Tests**
- **Schulungen** und **Coaching**
- der skriptbasierte Testumgebung **NTOnTrack**

Mehr dazu erfahren Sie unter:
www.newtec.de/loesungen/railway/

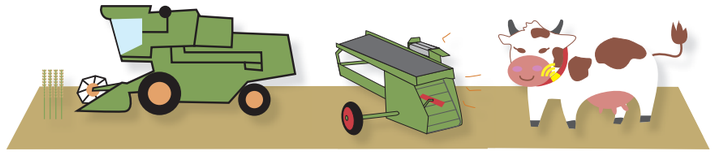
Und Landmaschinen?

Tatsächlich gibt es heute kaum eine Branche, in der Ethernet keine Rolle spielt. Auch in der Avionik oder der Medizintechnik wird Ethernet längst eingesetzt. Zum Schluss unserer kleinen Reise durch die Branchen wollen wir aber noch einen kurzen Blick auf eine Hightech-Branche werfen, bei der Ethernet bisher noch nicht im Rampenlicht steht: Landmaschinen.

Ein moderner Traktor verfügt heute über Hightech-Steuerfunktionen, verschiedene digitale Kameras und ein Onboard-System, das komplexe Sensordaten zu Bodenbeschaffenheit, Wasservorkommen und Pflanzenbeständen mit Wetter-, GPS- und Maschinendaten zusammenführt, um beispielsweise den Einsatz von Saatgut, Pflanzenschutz- oder Düngemitteln zu optimieren.

Ganz ähnlich wie in einem Eisenbahnzug sind aber die verschiedenen Schlüsselfunktionen eines Traktors und der koppelbaren Anbaugeräte (Düngerstreuer, Bodenfräsen, Unkrautvernichter etc.) herstellerspezifisch. Das ist – man ahnt es schon – der Interoperabilität nicht besonders zuträglich. Zudem erfolgt die Datenübertragung per ISOBUS, einem spezifischen CAN-Bus-System für landtechnische Anwendungen mit einer maximalen Bandbreite von 250 kbit/s. Da diese für moderne Anwendungen kaum ausreicht, werden häufig mehrere CAN-Busse parallel und zusätzlich noch Kabelsysteme für Videodaten verbaut.

Für die nächste Generation von Landmaschinen wird daher mit Hochdruck an einheitlichen Standards und Formaten für eine bessere Interoperabilität und einen besseren Datenaustausch gearbeitet. Mit dem High-Speed ISOBUS (HSI) erarbeitet die Agricultural Industry Electronics Foundation (AEF) als ISOBUS-Normierungsgremium einen neuen, zukunftsweisenden ethernetbasierten Standard. Eine hohe Bandbreite, Datenraten bis 1.000 Megabit pro Sekunde und eine geringe Latenz ermöglichen z. B. Echtzeitanwendungen oder die gleichzeitige Verwendung mehrerer hochauflösender digitaler Kameras.



Neue Technologien in der Agrarbranche erfordern ein hohes Level an Safety & Security.

Ethernet Safety & Security

Es klang bereits mehrfach an: Zunehmend sollen auch sicherheitskritische Anwendungen per Ethernet vernetzt werden. Eng damit verbunden sind besondere Anforderungen an die Zuverlässigkeit der Datenübertragung. Allerdings muss man bei Datenverbindungen grundsätzlich davon ausgehen, dass Nachrichten verloren gehen können oder veraltet sind, bevor sie weitergeleitet werden (Stichwort Congestion / Datenstau).

Um auch hohen Ansprüchen an Funktionssicherheit (Safety) gerecht zu werden, bietet die Ethernet-Technologie zahlreiche probate Lösungen, beispielsweise Switches, die bestimmte Zeitbereiche für sicherheitskritische Nachrichten (Telegramme) reservieren und damit für andere Datenpakete sperren. Um wiederum sichergehen zu können, dass eine Nachricht nicht veraltet, verloren oder verändert ist, wird sie zyklisch gesendet. Die Transportschicht wird dabei als ungesichert (Black Channel) betrachtet. Um die Gültigkeit der Nachrichten überprüfen und Fehler bei der Datenübertragung sicher identifizieren zu können, werden den Telegrammen Informationen und Prüfwerte angefügt, die ein laufender Zähler kontinuierlich checkt (CRC-Prüfung).

Um Ethernet-Verbindungen gegenüber Hackerangriffen abzusichern, können Nachrichten verschlüsselt versendet werden. Spezielle Switches oder Gateways wie die NTSecure-Gateways von NewTec sorgen mittels Kryptomodulen für eine cybersichere Datenübertragung.

Als Experten für Safety und Security beraten wir Hersteller verschiedenster Branchen bei der Auswahl geeigneter Ethernetsysteme und -protokolle.

Unsere Ingenieure kalkulieren die Sicherheitslevel, übernehmen Design-Reviews und Robustheitsprüfungen, um Schaltungsentwürfe auf Sicherheit und Zuverlässigkeit zu überprüfen.

Wir bieten vorzertifizierte Hardwarekomponenten zur Anbindung sicherheitskritischer Funktionen per Ethernet. Und wir entwickeln Lösungen für einen funktions- und cybersicheren Datentransfer.

Cyber Resilience Act – worauf müssen sich Hersteller einstellen?

Mit dem Cyber Resilience Act (CRA) soll die Cybersicherheit vernetzbarer Produkte auf ein EU- und produktübergreifend hohes, einheitliches Niveau gehoben und die Transparenz von Sicherheitseigenschaften verbessert werden. Die Regulierung ist sektorübergreifend und umfasst alle Bereiche der Cybersecurity und alle Produkte, die eine Datenverbindung zu einem anderen Produkt oder einem Netzwerk aufbauen können.

Was bedeutet das für Hersteller?

Ende 2023 einigten sich die Europäische Kommission, das Europäische Parlament und der Rat der Europäischen Union auf den endgültigen Text des Cyber Resilience Act (CRA). Derzeit (Stand März 2024) ist er allerdings noch nicht verabschiedet. Sobald dies der Fall ist, beginnt eine zweijährige Übergangsfrist. Nach deren Ablauf müssen Hersteller grundsätzlich für jedes Produkt „mit digitalen Elementen" ein Cybersecurity Risk Assessment durchführen und „das Ergebnis dieser Bewertung in der Planungs-, Konzeptions-, Entwicklungs-, Herstellungs-, Liefer- und Wartungsphase des Produkts" berücksichtigen (Art. 10 Abs. 2).

Die Anforderungen gelten also für den gesamten Lebenszyklus. Dafür werden die Produkte in verschiedene Risikokategorien eingeteilt. Als unkritisch werden beispielsweise Consumer-Produkte wie intelligente Lautsprecher oder Fotobearbeitungssoftware betrachtet. Als kritisch (Klasse I) gelten z. B. IIoT-Produkte, die in der Industrie eingesetzt werden. Produkte der kritischen Infrastruktur gelten grundsätzlich als hochkritisch (Klasse II).

Aber es gibt auch kategorische Ausnahmen: Für Medizinprodukte und In-Vitro-Diagnostika sowie für Kraftfahrzeuge gelten die Bestimmungen des CRA explizit nicht (Paragraf 12 und 13), da man davon ausgeht, dass mit Umsetzung der Medizinprodukte-verordnung bzw. der Verordnung über die Typengenehmigung von Kraftfahrzeugen ein hinreichendes Cybersicherheitsniveau erreicht wird.

CRA und IEC 62443

Für Industrieprodukte (gemäß Anhang III: alle IIoT-Produkte, Mikrocontroller, anwendungsspezifische Schaltungen, industrielle Automatisierungs- und Steuerungssysteme) gilt die CRA vollumfänglich. Hersteller und Entwickler stehen nun vor der Frage, welche zusätzlichen Entwicklungs- und Dokumentationsanforderungen die CRA enthält, die die einschlägige IT-Sicherheitsnorm IEC 62443-4-1 (Industrielle Kommunikationsnetze) nicht bereits abdeckt.

Wir haben die IEC 62443 und den CRA eingehend verglichen und kamen zu dem Ergebnis, dass Entwicklungen nach IEC 62443-4-1 bereits weitestgehend die Forderungen des Gesetzentwurfs abdecken – an vielen Stellen ist die einschlägige

Norm sogar detaillierter. Nicht von ungefähr wird IEC 62443 als erster Kandidat für eine Harmonisierung gehandelt.

In einem relevanten Aspekt allerdings geht der CRA über die Norm hinaus – und zwar hinsichtlich der Absicherung der Software-Lieferkette (Stichwort Software Bill of Materials). Während die IEC 62443-4-1 eine Bestandsaufnahme der Fremdkomponenten lediglich empfiehlt, wird nach dem CRA die Ermittlung und Dokumentation von „Schwachstellen und Komponenten des Produkts" verbindlich gefordert (Anhang I, Abs. 2.1). Sobald ein OEM oder Komponentenhersteller eine Sicherheitslücke in einer von ihm verwendeten Software findet, muss er diese an den Hersteller oder Anbieter der Software melden und dieser ist zur Behebung der Lücke (und Zurverfügungstellung von Patches) verpflichtet.

Das Open-Source-Problem

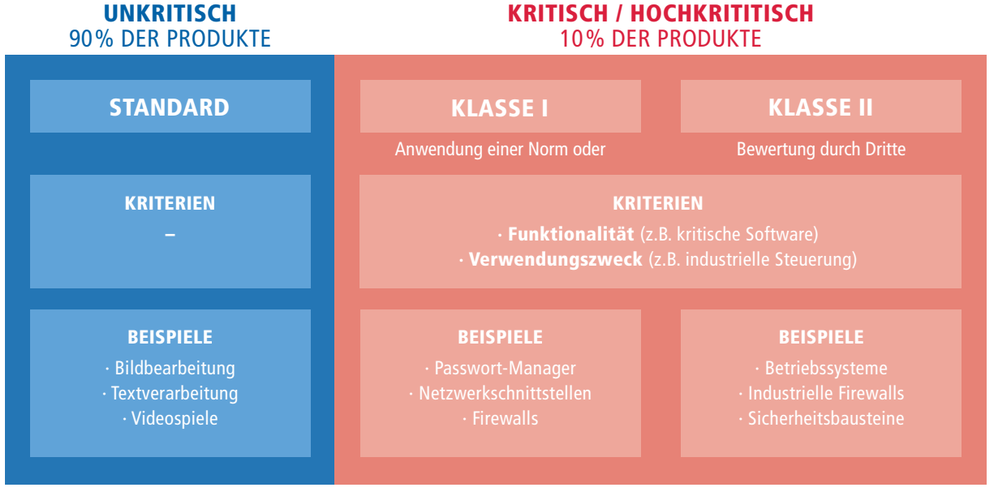
Besonders problematisch ist dies in Hinblick auf Open-Source-Komponenten. Denn laut CRA sind Hersteller von kommerzieller Open Source Software ebenso in der Pflicht und haftbar wie Hersteller proprietärer Software. Allerdings blieb der erste Gesetzesentwurf hinsichtlich der Definition von „kommerzieller" Software sehr allgemein und unklar.

Diese Unklarheiten hatten zunächst zu massiven Befürchtungen geführt, mit dem CRA könne jegliche Vermarktung und Verwendung von Open Source Software in Europa mit hohen finanziellen Risiken verbunden sein. Dies zumal laut Paragraf 10 CRA nicht nur kostenpflichtige OSS als „kommerziell" gilt, sondern auch solche, bei der für Support oder Bereitstellung einer Softwareplattform ein Preis verlangt wird oder die erhobenen Daten für kommerzielle Zwecke verwendet werden.

Der inzwischen überarbeitete und ergänzte Gesetzestext geht nun in Anhang II ausführlich auf das Thema ein und schafft mit einer Präzisierung des Begriffs „kommerziell" mehr Rechtssicherheit. So gelten nach Anhang II, 10 nur solche Unternehmen als „kommerziell", die Open Source Software oder (Support-)Services (z. B. Plattformen) mit Gewinnerzielungsabsicht anbieten. Dagegen gelten Organisationen oder Personen explizit nicht als kommerziell, wenn sie ihre Software nur bepreisen, um so die tatsächlichen Kosten zu decken (Anhang II, 10a).

Demzufolge sind auch nur gewinnorientierte Hersteller und Anbieter für ihre Software vollumfänglich haftbar und müssen die Anforderungen des CRA umfassend erfüllen. Für sogenannte „Open-Source Software Stewards", die regelmäßig Support für die Weiterentwicklung von OSS anbieten und eine verantwortungsvolle Rolle für die Qualitätssicherung der entsprechenden Software spielen, ohne dabei selbst Gewinne zu erzielen, sollen die Anforderungen „locker und maßgeschneidert" angewendet werden (Anhang II, 10d). Für sie gilt z. B. keine Pflicht zur CE-Zertifizierung. Allerdings lassen auch die Formulierungen zu den Stewards und deren Pflichten nach Einschätzung von Fachleuten noch einigen Interpretationsspielraum.

Auch mit dem endgültigen Gesetzesentwurf dürfte also die Diskussion hinsichtlich der Verwendung quelloffener Software noch nicht gänzlich beendet sein – zumal der CRA bei Zuwiderhandlungen hohe Geldstrafen von bis zu 15 Mio. Euro oder 2,5 Prozent des globalen Jahresumsatzes vorsieht.



Praxis-Anwendung des CRA (Quelle: "How the Cyber Resiliance Act will work in practice", www.european-cyber-resilience-act.com)

Cybersicherheit von Medizinprodukten: Welche Normen sind relevant?

In der letzten Ausgabe berichteten wir, dass sich mit Inkrafttreten der Medizinprodukteverordnung (MDR) die Anforderungen für die Zulassung von neuen Medizinprodukten deutlich erhöht haben. Das betrifft insbesondere auch die Anforderungen an die Cybersicherheit.

In Anhang I fordert die MDR u. a. Maßnahmen zur IT-Sicherheit gemäß „allgemein anerkanntem Stand der Technik". Medizinprodukte sollen auch hinsichtlich der Cybersicherheit so konstruiert werden, dass während des gesamten Produktlebenszyklus Risiken für die Gesundheit und Sicherheit der Patienten sowie der Anwender so weit wie möglich reduziert werden. Allerdings bietet die MDR kaum Details zu den Anforderungen und deren Realisierung.

Mit der Umsetzung der einschlägigen Normen können Hersteller und Entwickler aber sicherstellen, dass ihr Produkt dem allgemein anerkannten Stand der Technik entspricht. So können sie beispielsweise mithilfe der ISO 13485 nachweisen, dass die MDR-Anforderungen an ein QM-System erfüllt werden.

➔ Wenn es nun um die Cybersicherheit von Medizinprodukten geht, sollten Hersteller besonders die fünf Normen auf der Seite 13 beachten.

Für Hersteller von Medizingeräten:

Wie Sie die Anforderungen an Cybersecurity bei Medizinprodukten umsetzen können.

Lesen Sie unser kostenloses Whitepaper und erfahren Sie mehr!

HIER DOWNLOAD

ISO 14971 Risikomanagement

ISO 14971 gilt als grundlegende Norm für die Entwicklung von Medizinprodukten. Sie gibt ein Verfahren vor, mit dem Hersteller und Entwickler mögliche Gefährdungen erkennen können, die mit Medizinprodukten verbunden sind. Darüber hinaus beschreibt die Norm, wie Risiken abgeschätzt, bewertet und kontrolliert werden können und wie die Wirksamkeit der Kontrollen überwacht wird. Gefordert wird eine vorausblickende Einschätzung, auf welche Weise ein vernetztes Gerät ausfallen kann und welche Folgen dies (insbesondere für die Patientensicherheit) haben könnte. In der dritten Ausgabe wurde auch Software explizit als Medizinprodukt aufgenommen.

IEC TR 60601-4-5 Sicherheit medizinischer elektrischer Geräte

Seit 2021 liegt der Technical Report IEC TR 60601-4-5 als Ergänzung zur Basisnorm EN 60601-1 (Sicherheit medizinischer elektrischer Geräte) vor. Während diese vor allem Anforderungen an die Safety elektrischer medizinischer Geräte spezifiziert, befasst sich IEC TR 60601-4-5 mit der IT-Sicherheit vernetzter elektrischer Medizingeräte und -systeme. Basierend auf sieben grundlegenden Anforderungen, die in der IEC 62443 (siehe letzter Kasten) beschrieben sind, bietet er einen Katalog von Spezifikationen für verschiedene Sicherheitsstufen.

IEC 81001-5-1 Entwicklung und Wartung sicherer Gesundheitssoftware

IEC 81001-5-1 formuliert konkrete Vorgaben für die Entwicklung und Wartung sicherer Software (eingebettet und standalone) zum Management von Sicherheitsrisiken und zu Problemlösungs-Prozessen. In den Anhängen finden sich zudem Hinweise zu Best Practices. Für Hersteller ist die Norm insbesondere relevant, weil sie eine Lücke zwischen bestehenden Normen schließt. Zum einen überträgt sie die primär auf Safety bezogenen Anforderungen der ISO 14971 zu Risikobewertung und -management auf Security-Aspekte. Zum anderen orientiert sie sich an den Security-Anforderungen der IEC 62443 für industrielle Kommunikationsnetze und zeigt auf, wie diese bei Entwicklung und Wartung von Gesundheitssoftware erfüllt werden können. Schließlich ergänzt sie die Safety-bezogenen Vorgaben der IEC 62304 um Vorgaben in Hinblick auf Security.

IEC 62304 Software-Lebenszyklus

IEC 62304 definiert Anforderungen an Entwicklung und Wartung von Medizinprodukt-Software (sowohl eingebetteter als auch Stand-alone-Software). Welche Maßnahmen dabei konkret umgesetzt werden müssen, richtet sich nach drei Sicherheitsstufen (A, B, C). So sind beispielsweise in den Klassen B und C Tests für die Softwareanforderungen erforderlich. Strenge Vorgaben macht die Norm bei Drittanbieter-Software unsicherer Herkunft (Software of Unknown Providence) einschließlich Open-Source-Bibliotheken, bei denen jeder Zugriff auf den Code hat.

IEC 62443 Industrielle Kommunikationsnetze

Obwohl die IEC 62443 eine Industrienorm ist, lassen sich die Cybersecurity-Anforderungen dieser Normenreihe weitgehend auf vernetzte Medizinprodukte übertragen. Die Norm verfolgt einen Defense-in-Depth-Ansatz, um der Vielzahl möglicher Angriffsvektoren Rechnung zu tragen. Auf Basis einer detaillierten Bedrohungs- und Schwachstellenanalyse wird das Gesamtsystem in verschiedene Sicherheitszonen („Zones") segmentiert und diese Zonen selbst sowie die Übergänge bzw. Kommunikationskanäle („Conduits") zwischen ihnen separat abgesichert. Darüber hinaus bietet die Norm u. a. eine Bewertung unterschiedlicher Cybersecurity-Tools, Gegenmaßnahmen und Technologien sowie Empfehlungen für ein sicheres Patch-Management.

Foto: Vossloh Rolling Stock

Vossloh Rolling Stock

Als einer der führenden Lokomotivhersteller in Europa sowie als traditionsreiches Unternehmen mit einer mehr als 150-jährigen Kompetenz im Lokbau engagiert sich Vossloh Rolling Stock für eine nachhaltige Mobilität – durch weitsichtiges und entschlossenes Handeln, im steten Dialog mit seinen Kunden. Das Erfolgskonzept, dem Kunden aus allen Bereichen – ob Staatsbahn, Vermieter oder Industrie- und Privatbahnkunden – vertrauen, ist eine exakt auf den Bedarf abgestimmte Traktion. Dabei liegt der Fokus seit jeher auf höchst wirtschaftlichen, robusten und bedienerfreundlichen Lösungen für sämtliche Transportaufgaben im Rangier- und Streckenbetrieb.

Cybersecurity auf der Schiene

Wenn Lokomotiven smart und vernetzt werden sollen, braucht es Cybersecurity auf Schienen. NewTec unterstützt die Entwicklung einer neuen Rangier- und Güterzuglok durch eine umfangreiche Risikoanalyse und die Entwicklung von Komponenten für sichere Update-Prozesse.

Auch im Schienenverkehr stehen die Signale für Digitalisierung und Vernetzung auf Grün. In unserer Ausgabe vom November 2020 berichteten wir bereits über eine Studie zur Eignung verschiedener Netzwerkprotokolle für die Vernetzung von Zugkomponenten, die NewTec im Auftrag Schweizer Bahngesellschaften durchführte. Nun unterstützte NewTec den Kieler Lokhersteller Vossloh Rolling Stock bei der Entwicklung einer smarten Lokomotive.

Mit seiner neuen Hybridlokomotive „Modula“ setzt Vossloh Rolling Stock neben innovativen Antriebskonzepten auch auf Digitalisierung und Vernetzung, um so eine flexibel einsetzbare Lösung für die Rangier- und Transportaufgaben der Zukunft anzubieten. Die Modula-Plattform ermöglicht u. a. eine nahtlose Kombination von Rangierdienst und Güterverkehr unter Einsatz verschiedener Traktionsarten (aktuell Diesel, Oberleitung, Batterie) mit ein und derselben Lok.

Um die Instandhaltungskosten zu minimieren und die Verfügbarkeit jeder Lok zu optimieren, verfolgt Vossloh Rolling Stock ein durchgehendes Konzept der vorausschauenden Instandhaltung. Dabei wird der Zustand aller wichtigen Lok-Komponenten kontinuierlich mithilfe von Grenzwerten und Überwachungslogiken ausgewertet. Die entsprechenden Zustands- und Standortinformationen werden von Sensoren und GPS-Modulen erfasst, an eine Cloud weitergeleitet und zentral ausgewertet. Das ermöglicht eine zustandsbasierte Instandhaltung der Maschine und ein optimiertes Werkstattmanagement. Die Behebung kleinerer Probleme an der Lok unterstützt das System via Augmented Reality.

Erfolgsfaktor Security

Klar, dass ein solch vernetztes System gegen unbefugte Manipulationen von außen geschützt werden muss, um das sichere Funktionieren und ein sicheres Arbeiten auf und an der Lok zu gewährleisten.

NewTec unterstützte Vossloh Rolling Stock daher bei der Entwicklung smarter Lokfunktionalitäten zunächst mit einer umfassenden Identifizierung und Bewertung von Security-Bedrohungen und -Risiken (Threat and Risk Assessment / TARA). Dabei wurde die Systemarchitektur entsprechend dem Schutzkonzept der IEC 62443 in Sicherheitszonen („Zones“) eingeteilt und für diese, ebenso wie für die Übergänge zwischen den Zones („Conduits“), spezifische Sicherheitsanforderungen definiert. Hieraus wurden u. a. verschiedene Anforderungen für Zulieferer abgeleitet. Auch ein Security-Audit der Deutschen Bahn konnte auf dieser Grundlage ohne Beanstandungen abgeschlossen werden.

Darüber hinaus unterstützt NewTec Vossloh Rolling Stock bei der Entwicklung kritischer Komponenten zur Kommunikation nach außen. So entsteht derzeit ein Content Delivery Network für sichere Update-Prozesse mit NTSecureCloud-Komponenten. Auf Basis einer PKI (Public-Key-Infrastructure) wurde zudem ein Berechtigungskonzept für Service-Techniker entwickelt. Somit können Lok-Betreiber Service-Technikern ein sicheres Einloggen auf der Lok ermöglichen.

Die Entwicklungen laufen derzeit auf Hochtouren.

Das Projekt-Team von NewTec/Fresh X live vor Ort bei Vossloh Rolling Stock (v.li.: Dominik Rössler, Stephan Strohmeier, Jürgen Pietrowsky).

Consulting für Safety & Security

Mit zunehmender Komplexität und Vernetzung steigen auch die Anforderungen an Safety (Funktionssicherheit) und Security (Informationssicherheit) technischer Produkte. Bei Neuentwicklungen gilt es daher, sicherheitsrelevante Faktoren und mögliche Risiken zu identifizieren und gemäß den jeweiligen regulatorischen Bestimmungen und normativen Anforderungen umzusetzen. Hersteller benötigen entsprechende Expertise und geeignete Prozesse. Fehlen diese, kann das schnell zur Innovationsbremse werden.

Unsere Consulting-Teams für Safety und Security unterstützen Hersteller dabei, sicherheitsgerichtete Projekte durchzuführen, und helfen beim Aufbau von Know-how und anwendbaren Prozessen sowie beim Erstellen und Umsetzen von Safety-Konzepten.

Herausforderung Safety

Wenn es darum geht, ein neues Produkt zu entwickeln und an den Markt zu bringen, stehen am Anfang meist eine Produktidee und eine mehr oder weniger konkrete Vorstellung, wie diese hinsichtlich der primären Funktionen realisiert werden kann. Wenig Klarheit besteht dagegen darüber, welche Anforderungen in Bezug auf Funktions- und Informationssicherheit sich aus dem Entwicklungsvorhaben ergeben und wie diese am besten umzusetzen sind.

Welche Regularien müssen beachtet werden, an welchen Standards sollte man sich orientieren und welche Best Practices gibt es? Hier fehlt es vielen Herstellern an Expertise und etablierten Safety-Prozessen – ganz besonders dann, wenn die Produktpalette in Richtung einer neuen Branche erweitert werden soll. So entpuppen sich Sicherheitsanforderungen schnell als Flaschenhals. Manchem Hersteller fehlt es auch gar nicht an Know-how, es steckt aber in Köpfen, die zeitlich in andere Projekte eingebunden sind; und in Fachkräfte-Mangelzeiten lässt sich zusätzliches Fachwissen auch nicht ohne Weiteres neu rekrutieren. Hier helfen die Safety Consultants von NewTec, ein Entwicklungsprojekt von Anfang an richtig auf- und umzusetzen.

Ganz am Anfang: Strategische Projektanalyse

Noch bevor der Blick auf Safety und Security gerichtet wird, können in einem strategischen Projektanalyseworkshop mit Unterstützung unserer Experten die marktrelevanten Aspekte des geplanten Produkts identifiziert und präzisiert werden. Dabei werden in einer detaillierten Produktanalyse auch Zielgruppe, Mitbewerber, Key-Features und Zweckbestimmung (Intended Use) unter die Lupe genommen. Denn eine größtmögliche Klarheit dieser Aspekte ist i. d. R. eine gute Basis für effizientes sicherheitsgerichtetes Engineering.

Gezielte Unterstützung bei Safety-Plan und Safety-Konzept

Die Safety-Consultants von NewTec unterstützen Hersteller bereits ab der Planungsphase eines Projektes (der Entwicklung vorgelagert) beim Auf- und Ausbau von normativem Know-how und funktionierenden Safety-Engineering-Prozessen.

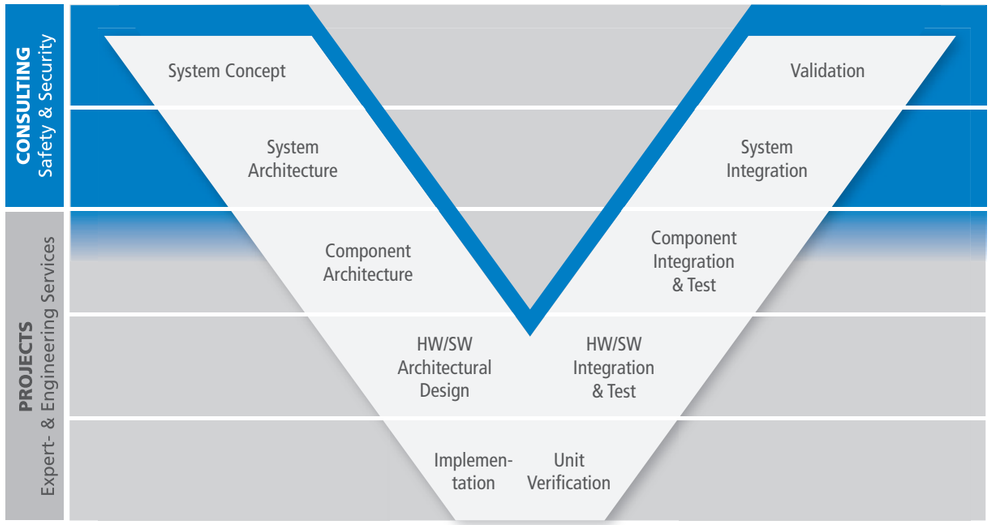
In der Konzeptphase helfen unsere Experten, Safety-Plan und Safety-Konzept zu erstellen und so die normativen Anforderungen von Anfang an zu integrieren. Mit einer Gefahren- und Risikoanalyse (HARA) werden zunächst die möglichen Risiken identifiziert und anschließend für jede Sicherheitsfunktion das Sicherheitslevel (je nach Branche SIL, ASIL, DAL) entsprechend ihrer Kritikalität festgelegt.

Mit einem Safety-Plan wird geklärt, welche Maßnahmen erforderlich sind, um den normativen Anforderungen an Funktionssicherheit gerecht zu werden. Dabei werden alle Safety-Anforderungen inkl. Maßnahmen zur Verifikation und Validierung detailliert beschrieben. Das Safety-Konzept klärt, wo Sicherheitsfunktionen lokalisiert sind und wie die Anforderungen konkret umgesetzt werden. Es betrachtet insbesondere auch das Zusammenspiel mit Security-Risiken und Security-Anforderungen (siehe unten „Kein Safety Engineering ohne Security"): Wo müssen Anforderungen harmonisiert und die Rückwirkungsfreiheit (Freedom of Interference) von Anwendungs- und Sicherheitsfunktionen gewährleistet werden?

Um während der Umsetzungs- und Zulassungsphase auf der sicheren Seite zu sein, empfehlen wir, Safety-Plan und Safety-Konzept vom TÜV prüfen zu lassen, und übernehmen die entsprechenden Schritte.

Im Rahmen der Konzeptphase analysieren die Safety-Consultants gemeinsam mit dem Hersteller auch den Reifegrad seiner Safety-Entwicklungsprozesse. Anhand eines Reifegradmodells (z. B. Automotive SPICE) wird geklärt, welche Voraussetzungen für das Erreichen der Entwicklungsziele bereits erfüllt sind und welche Prozesse noch aus- bzw. aufgebaut werden müssen.

Am Ende steht ein tragfähiges Konzept für die System- und Komponentenarchitektur. Damit ist auch eine fundierte Kalkulation der Projektkosten (in Entwicklung und Stückzahl) möglich. Damit der gesamte Safety-Entwicklungsplan möglichst reibungslos umgesetzt werden kann, bieten wir gezielte Coachings zu den System-Safety-Engineering-Prozessen.



Safety Engineering

Auf Wunsch übernimmt NewTec auch die Entwicklung einzelner Komponenten oder die komplette Safety-Entwicklung. Dann kommen die erfahrenen Senior Safety Engineers der NewTec Expert-Services mit ins Boot, um den Projektplan umzusetzen. Auch während des anschließenden Produktentstehungs- und Zulassungsprozesses, bleiben die Safety Engineering Consultants weiter an Board und übernehmen beispielsweise das kontinuierliche Assessment der funktionalen Sicherheit.

In enger Abstimmung mit dem Hersteller werden Produktentwicklung und Safety-Design effektiv synchronisiert und die gesetzlichen Anforderungen effizient umgesetzt. Auf Wunsch übernehmen wir auch die Rolle des Company-FSM (Functional Safety Manager) – beispielsweise, wenn es darum geht, Personalengpässe zu überbrücken.

Kein Safety Engineering ohne Security

Sind die zu entwickelnden Produkte vernetzbar, müssen sie auch gegen Hackerangriffe und unbefugte Manipulation über das Internet abgesichert werden. Denn ein vernetztes Produkt ist nur dann safe, wenn es gegen die Risiken von Hackerangriffen oder unbefugte Manipulationen abgesichert ist. Der Cyber Resilience Act der EU-Kommission fordert daher auch ein (Security) Risk Assessment für jedes Produkt (siehe Seite 10).

Allerdings gelten für das Security Engineering andere Voraussetzungen als für die Safety-Entwicklung. Denn während die Risikofaktoren für die funktionale Sicherheit über ein ganzes Produktleben gleich bleiben, sind Security-Risiken dynamisch. Dementsprechend umfasst die Security-Entwicklung etwa auch sichere Update- und Patchmöglichkeiten.

Für viele Hersteller und Zulieferer ist die Entwicklung cybersicherer Produkte noch Neuland, insbesondere wenn ihre Produktpalette bisher mehrheitlich analog ist. Oft haben sie keine Erfahrungen im Security-Design und verfügen über keine etablierten Security-Managementprozesse. Aber auch hier können Hersteller auf das Engineering-Know-how von NewTec zurückgreifen.

Safety Consulting

- Durchführung von Risikoanalysen
- Erstellung von System-Konzepten (System-Architektur, Safety-Concept, Safety-Plan, V&V Plan) mit der Safety Requirement Specification (SRS) als Ergebnis
- Reifegradbestimmung der Safety- und Support-Prozesse
- Einführung von Safety-Prozessen und Integration in den Produktentstehungsprozess
- Ausbildung von Safety-Prozessverantwortlichen
- Zulassungsunterstützung (z. B. „Bindeglied" zu TÜV)
- Interims-Safety-Management (z. B. zur Überbrückung von Personalknappheit)
- Moderation von Konformitätsprüfung mit benannten Stellen

Security Engineering: Herausforderungen meistern

Parallel zur Entwicklung eines Safety-Plans und -Konzepts helfen unsere Security Consultants bei der Entwicklung von Security-Plan und -Konzept – beispielsweise bei der Bedrohungs- und Risikoanalyse (TARA) oder bei einer sicheren Updatestrategie – und geben präzise Handlungsempfehlungen. Sie unterstützen Hersteller insbesondere dort, wo es um die Zusammenhänge von Security- und Safety-Risiken geht, um die jeweiligen normativen Grundlagen sowie um die Harmonisierung von Safety- und Security-Anforderungen.

Unsere Experten helfen Herstellern auch bei einer systematischen Security-Reifegradbestimmung. Auf Grundlage der Security-Basisnorm IEC 62443 und der branchenbezogenen Normen analysieren sie beispielsweise, welche Voraussetzungen vom Hersteller bereits erfüllt werden und welche Fähigkeiten aus- oder neu aufgebaut werden müssen.

Den Aufbau des nötigen Security-Know-hows unterstützt unser Team durch gezielte Trainings und Seminare. Spezielle Coachings und Awareness-Workshops sorgen zudem dafür, dass Security-Prozesse nicht nur auf dem Papier bestehen, sondern auch gelebt werden. Gerne übernehmen wir auch das komplette Security Engineering und holen dazu die Security Ingenieure unserer Expert-Services mit an Bord.

Unsere Experten für Cybersecurity

Um der wachsenden Nachfrage nach Beratung für die Entwicklung cybersicherer eingebetteter Systeme gerecht zu werden, haben wir unser Team für Security Consulting in den letzten Jahren systematisch ausgebaut. So stehen im Industriebereich (IEC 62443-3/4) und für die Automotive-Branche (ISO/SAE 21434) vom TÜV Rheinland zertifizierte „Cyber Security Specialists" zur Verfügung. Auch in anderen Bereichen unterstützen wir Hersteller mit pragmatischer Security-Expertise, z. B. helfen BSI-zertifizierte Security-Experten bei einer Common-Criteria-Zertifizierung.

Security Consulting

- Durchführung von Bedrohungsanalysen (TARA, IRA, DRA)
- Erstellung von Security-Konzepten mit der Cyber Security Requirements Specification (CSRS) als Ergebnis
- Reifegradbestimmung der Entwicklungs- und Begleitprozesse
- Seminare und Trainings zum Aufbau von Security-Know-how
- Awareness-Workshops
- Beratung und Konzeption beim Aufbau einer PKI-Infrastruktur
- Sichere Update-Strategien
- Beratung und Unterstützung bei der CC-Zertifizierung (Common Criteria)
- Penetration & Security Robustness Testing
- Interims-Security-Management
- Moderation von Konformitätsprüfung mit benannten Stellen

Startpunkt für die Entwicklung gesicherter Systeme NTSecurityAnalysis: TARA, IRA, DRA nach IEC 62443-3

Wie funktioniert NTSecurityAnalysis?

In zwei Session identifizieren wir mit Ihnen relevante Cyber-Gefährdungen, bewerten die Risiken und bestimmen Maßnahmen zur Reduzierung auf akzeptables Restrisiko.

Phase 1: Initial Risk Assessement

- Systemarchitektur und Zonierung
- Schutzbedarfsanalyse (Assets)
- Normenlage
- Schutzziele und Schutzbedarf
- Bedrohungsanalyse / Angreiferprofile
- Risikoanalyse und Priorisierung

Phase 2: Detailed Risk Assessement

- Bedrohungsanalyse für jede Zone (Ergebnis aus Phase 1)
- Risikobehandlung (Liefergegenstand: Maßnahmenkatalog)

Warum NTSecurityAnalysis?

Hersteller vernetzter Embedded-Geräte müssen heute zwingend Fragen der IT-Sicherheit in ihre Produktstrategie einbeziehen:

Produkthaftung:
Die Zahl von Cyber-Angriffen auf IoT-Geräte wächst seit Jahren. Schon aus Haftungsgründen dürfen Hersteller dieses Thema nicht auf die leichte Schulter nehmen.

Relevante Normen:
- IEC 61508
- IEC 62443
- Cyber Resilience Act
- IEC 13849 Maschinenrichtline
- branchenspezifische Normen

Gespräch mit Johannes Werbach: Ein Unternehmen braucht einen Sinn und ein Ziel

Johannes Werbach war von 1991 bis 2022 Mitglied der NewTec-Geschäftsführung. In dieser Zeit hatte er einen maßgeblichen Anteil an der Ausrichtung des Unternehmens und an der Entwicklung unserer werteorientierten Unternehmensführung.

Herr Werbach: Obwohl sie 1991 eine sichere Anstellung hatten, haben Sie sich damals entschieden, in ein kleines Start-up zu wechseln. Wie kam es dazu?
Tatsächlich war meine Anstellung gar nicht so schlecht. Aber ich hatte den Eindruck, dass man Unternehmensführung besser machen kann als damals oft üblich – also weniger hierarchisch und mit weniger Druck. Und dann reizte mich die Aussicht, zusammen mit Harald Molle und Ulrich Schwer ein Unternehmen aufzubauen.

1991 markiert noch einen anderen Meilenstein der NewTec: den ersten richtigen eigenen Unternehmenssitz …
Wir zogen in die „Alte Molkerei" in Steinheim. Ich war der Meinung, die NewTec braucht eine Heimat. Eine Firma muss man spüren und erleben können. In den Firmenräumen entsteht die Gemeinschaft der Mitarbeiter und die Wertschöpfung für die Kunden.

Die Gemeinschaft der Mitarbeiter und eine sinnstiftende Wertschöpfung waren Ihnen immer besonders wichtig.
Ich denke, für Unternehmen – insbesondere Technologieunternehmen – ist es essenziell, den Mitarbeitern einen Sinn anzubieten und ein Ziel, mit dem sich alle identifizieren können. Darüber hinaus brauchen wir in den Unternehmen eine Potenzialentfaltungskultur, also einen Blick auf die Möglichkeiten und Stärken der einzelnen Mitarbeiter – darauf, wo die Reise mit diesem Mitarbeiter hingehen kann. Da sind die Führungskräfte gefragt, eigenverantwortliches Handeln und Engagement zu unterstützen, damit Mitarbeiter motiviert sind, einen sinnvollen Beitrag für die Entwicklung der Firma zu leisten.

Stichwort „Entwicklung der Firma": Seit Ihrem Eintritt ist NewTec kontinuierlich gewachsen, auch in allgemeinen Krisenzeiten. Wie konnte das gelingen?
1991 sind wir zu dritt in Steinheim eingezogen. Als wir 1999 in dieses Gebäude in Pfaffenhofen einzogen, waren wir schon 45 Mitarbeiter und in diesen Jahren sind wir gesund gewachsen. Dann ging es Schlag auf Schlag: Noch im selben Jahr haben wir eine Niederlassung in Freiburg eröffnet: Es folgten weitere in Mannheim, Friedrichshafen und schließlich – weit weg im Norden – in Bremen. In dieser Zeit ist etwas sehr Wichtiges passiert: Die NewTec hat sich von einem Entwicklungsdienstleister für Hard- und Software zu einem Spezialisten für Safety und Security entwickelt. Das war ein langer Prozess, der immer noch nicht zu Ende ist. Aber damit haben wir unserem Unternehmen einen Sinn gegeben, auch gesellschaftlich: nämlich Systeme zu entwickeln, in die die Menschen Vertrauen haben können. Und blickt man in die Zukunft, wird dieser Sinn wohl noch mehr an Bedeutung gewinnen, wenn man beispielsweise an autonomes Fahren oder KI-gelenkte Systeme denkt.

Und Ihre persönliche Zukunft? Sie sind Ende 2022 aus der aktiven Geschäftsführung ausgeschieden. Wie sieht Ihre Planung aus?
Ich bin zwar aus der aktiven Geschäftsführung ausgeschieden, als Gesellschafter werde ich NewTec aber weiter begleiten. Neu ist für mich jetzt, dass ich in der Auswahl meiner Tätigkeiten freier bin. Und ich kann meine Freizeit etwas aktiver gestalten, Reisen und Dinge spontan mal machen. Zum Beispiel mit der Harley durch die Gegend cruisen …

Spenden statt Geschenke

Unsere Aktion „Spenden statt Geschenke“ hat inzwischen Tradition: Auch 2023 verzichteten wir auf das Verteilen von Weihnachtsgeschenken und unterstützten stattdessen soziale Einrichtungen in unseren Standortregionen. Über jeweils 3.500 Euro freuten sich diesmal die Lebenshilfe Region Mannheim-Schwetzingen-Hockenheim e.V., die Lebenshilfe Donau-Iller e.V. und die Lebenshilfe Breisgau e.V. Mit den Spenden sollen u. a. ein Tischkicker angeschafft, ein Bandprojekt mit behinderten und nicht behinderten Musikern und Musikerinnen sowie ein Projekt für Geschwister von Kindern mit Beeinträchtigungen unterstützt werden.

Geschäftsführer Matthias Wolbert bei der Spendenübergabe bei der Lebenshilfe Mannheim.

Fünf Jahre NewTec Pumptrack Ulm

Am 14. Oktober war „High5“-Time. Mit dem Event feierte der NewTec Pumptrack Ulm sein fünfjähriges Bestehen mit coolen Bike-Vorführungen und vielen Angeboten für die Besucher. Betrieben wird das bei Radsportenthusiasten sehr beliebte ca. 4500 m² große Gelände vom Deutschen Alpenverein. NewTec unterstützt den Betrieb als Namenssponsor.

Ein Pumptrack ist eine Übungsstrecke für Radfahrer, Skater und Inlineskater. Auf dem kurvenreichen, gewellten Streckenprofil wird Geschwindigkeit durch geschickte Körperbewegungen (anstatt etwa durch Pedalieren) aufgebaut.

Werteorientierte Führung

Bei NewTec setzen wir seit langem auf selbstorganisierte Teams als Kern der Wertschöpfung im Unternehmen. Dabei ist für uns eine Kultur der Potenzialentfaltung essenziell, die den Menschen mit seinen individuellen Möglichkeiten in den Mittelpunkt stellt.

Damit das auch in Zeiten ambitionierten Wachstums funktioniert, ist ein gutes Verständnis von Führung nötig. Für neue – aber auch für bewährte – Mitarbeitende in Führungsverantwortung haben wir daher elf Leitsätze in einem „Manifest der Führung“ zusammengefasst.

Sie sollen als Orientierung für eine werteorientierte Führung dienen und die Basis für ein vertrauensvolles Miteinander sowie ein lösungs- und zielorientiertes Arbeiten für die nächsten Jahre schaffen.

Schulungen für Requirements Engineering (IREB)

Gutes Anforderungsmanagement ist die Basis für ein erfolgreiches Projekt. Requirements-Engineering-Seminare von NewTec vermitteln das nötige Grundwissen. An drei Schulungstagen erhalten Einsteiger einen umfassenden Überblick über das Erheben und Dokumentieren sowie die Verifikation und Validierung von Anforderungen.

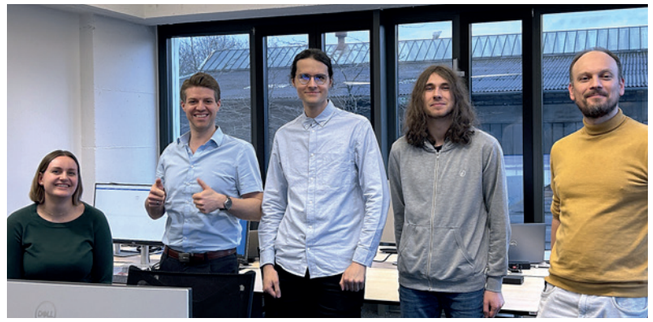
Anhand eines Praxisbeispiels wird das Gelernte angewendet und vertieft. Die Schulung orientiert sich am Lehrplan des International Requirements Engineering Board (IREB) und eignet sich zur Vorbereitung auf die Zertifizierungsprüfung zum Certified Professional for Requirements Engineering (CPRE).

Infos unter
www.newtec.de/trainings/

Neuer NewTec-Standort Ulm: Seit 1. Februar sind die Räume bezogen

NewTec wächst und ebenso die Zahl unserer Kundenprojekte in der Alb-Donau-Region. Da die räumlichen Kapazitäten und die Ausbaumöglichkeiten in unserer Unternehmenszentrale in Pfaffenhofen begrenzt sind, gibt es nun einen neuen NewTec-Standort in Ulm. Die Büros sind seit 1. Februar 2024 bezogen.

Mit der Neueröffnung soll die Zusammenarbeit mit den Technologie-Unternehmen in der Region und den Hochschulen in Ulm vorangetrieben werden. Die Nähe zu Pfaffenhofen ermöglicht darüber hinaus eine enge Kooperation der beiden Standorte.



Alle aktuellen Stellen für den neuen Standort Ulm und weitere finden Sie unter: **career.newtec.de**

> Ich freue mich sehr auf die spannende Aufgabe, den Standort Ulm aufzubauen und die Zukunft der NewTec mitzugestalten.
>
> *Matthias Spägele, Abteilungsleiter Ulm*

NewTec in Bremen

2017 gründete NewTec den ersten Standort in Norddeutschland. Bislang war diese Dependance in Bremen mit knapp 10 Mitarbeitern die kleinste. Aber klein sollte sie nicht bleiben.

Mitte 2023 bezog man daher neue Räumlichkeiten im Bremer Innovations- und Technologiezentrum (BITZ) – Tür an Tür mit der ESA, in unmittelbarer Nachbarschaft zur Universität und mit Blick auf den „Fallturm Bremen“, wo das Zentrum für angewandte Raumfahrttechnologie Experimente in kurzzeitiger Schwerelosigkeit durchführt.

Auf 120 m² gibt es im BITZ nun genügend Raum, um die Zahl der Mitarbeiter im nächsten Jahr deutlich zu vergrößern. Genug zu tun gibt es für das Bremer Team, das sich auf Software-Entwicklung und Systems Engineering spezialisiert hat, allemal.

„Wichtig ist uns dabei, die beiden Standorte Bremen und Mannheim gemeinsam weiterzuentwickeln“, sagt Richard Schwinn, der beide Standorte leitet. Bremen setzt dabei vor allem auf einen attraktiven, verkehrsgünstigen Standort, auf ein tolles Team und spannende Kundenprojekte.

Impressum

NewTec GmbH
Redaktion:
unlimited communications
Verantwortlich:
Brigitte Kunze, Matthias Wolbert

Herausgeber

NewTec GmbH
Buchenweg 3
89284 Pfaffenhofen a. d. Roth
Germany
www.newtec.de

Creating safety.
With passion.

NewTec

Neu mit HVC5x von TDK Micronas:

Bewährtes NTMicroDrive mit neuem, leistungsfähigerem Microcontroller!

Mit unserem NTMicroDrive und dem neuen HVC5x Microcontroller von TDK Micronas optimieren Sie die direkte Ansteuerung für BLDC-Motoren (bis zu 25 Watt):

- Doppelter Flash-Speicher
- Doppelter Motorstrom
- Kompakteres Gehäuse
- Bessere Verfügbarkeit
- Optimierte Motorregelung

NTMicroDrive ist eine seriennahe und hochflexible, anpassbare Firmware mit ausgefeilten Kommunikations-, Überwachungs- und Power-Management-Funktionen. Der Software-Stack mit minimalem Ressourcenverbrauch ermöglicht komplexe Motorsteuerungsalgorithmen wie Space Vector Modulation (SVM) für Permanent Magnet Synchronous Motoren (PMSM), Six-Step Commutation mit oder ohne Sensor-Feedback. Der Motorregler unterstützt dabei die Regelung von Geschwindigkeit und Position.

Kundennutzen

- Konform zu ISO 26262 ASIL A
- Gebrauchsfertige Software ermöglicht verkürzte Time-to-Market
- Kompatibel mit verschiedenen Motorentypen
- Viel Speicher für kundenindividuelle Anpassungen
- MISR-konform
- PC-Lint getestet

Typische Anwendungsbereiche

Automotive
Höhenverstellung der Scheinwerfer, elektrische Fensterheber, elektrische Sitzverstellung, elektrische Spiegelverstellung, Steuerung von Klimaanlage und Ventilen (z. B. im Kühlkreislauf von Traktionsbatterien)

Industrie
Sicherheitsverriegelung, Materialtransport, Werkzeughandhabung, Robotik

Baugewerbe
Sicherheitsverriegelung, Haltebügel, automatisches Ausrichtungsgerät, einfache Elektrowerkzeuge

NT SECURITY SOLUTIONS

NewTec

MKT014TE_0324