Creating safety.
With passion.

NewTec

WHITEPAPER

Industrial Internet of Things und Industrie 4.0: Neue Herausforderungen für Hersteller und Anwender

Industrial Internet of Things und Industrie 4.0: Neue Herausforderungen für Hersteller und Anwender

Inhalt

Management Summary

Industrie 4.0 und Industrial Internet of Things (IIoT) stellen Anwender ebenso wie Hersteller von Anlagen und Geräten vor erhebliche Herausforderungen. Denn die wenigsten Maschinen- und Anlagenbauer haben schon umfangreiche Erfahrungen im Umgang mit intelligenten Netzen – ebenso wenig wie die meisten Produktionsunternehmen.

Zwar gibt es seit Längerem modulare Automatisierungskonzepte mit einer zunehmend dezentralen Verteilung von Steuerungsintelligenz. Die dezentralen Komponenten – einschließlich von Sicherheitssteuerungen – kommunizieren zunehmend über Netzwerktechnologien. Über ihre Absicherung machen sich Hersteller und Anwender aber häufig keine Gedanken. Schon heute nutzen Cyberkriminelle das aus, um Unternehmen zu sabotieren, zu erpressen oder auszuspionieren.

Industrie 4.0 wird jedes Unternehmen zwingen, Sicherheit auf die Agenda zu setzen. Produktionsmaschinen, die autonom miteinander kommunizieren; abteilungsübergreifende Vernetzung von Maschinen, Material und Menschen; Kunden und Partner, die nahtlos in die Geschäfts- und Produktionsprozesse integriert sind – die Digitalisierung der Industrie verlangt nach neuen Konzepten für sichere Lösungen.

Sicherheit in vernetzten industriellen Systemen umfasst zwei Aspekte, die früher wenig miteinander zu tun hatten: einmal den Schutz von Menschen und Umwelt vor Gefahren, die vom Betrieb eines Systems ausgehen (Safety) und zum anderen den Schutz der Systeme vor Angriffen aus ihrer Umwelt (Security). Zwei unterschiedliche Welten treffen aufeinander, die Welt der industriellen Automatisierung und die Welt der IT.

Functional Safety oder die funktionale Sicherheit liegt traditionell im Verantwortungsbereich der Produktentwicklung. Diese verfügt über jahrzehntelange Erfahrungen, umfangreiches Know-how und Best Practices zur funktionalen Sicherheit. Security dagegen, die Absicherung von IT-Systemen gegen Angriffe, liegt in der Verantwortung der IT-Abteilung. Aber die herkömmlichen Waffen der IT-Sicherheit – Firewalls, Intrusion Detection, Virenscanner etc. – reichen allein nicht aus, um die vernetzte Industrie-4.0-Produktion zu schützen, und bereiten dort oft sogar Probleme. Hinzu kommt, dass Safety und Security in vernetzten Produktionsunternehmen miteinander interagieren: Maßnahmen der Security können die funktionale Sicherheit gefährden und umgekehrt. Und beide Bereiche haben verschiedene Schutzziele, die miteinander harmonisiert werden müssen.

Das vorliegende Whitepaper zeigt, warum Industrie 4.0 zwingend ein neues, integriertes Konzept von Sicherheit verlangt, das Safety- und Security-Aspekte gleichermaßen umfasst. Die Umsetzung eines solchen Sicherheitskonzepts verlangt einen strukturierten und ganzheitlichen Prozess, der schon bei der Entwicklung eines IoT-Produktes oder einer Industrie-4.0-Anwendung und über ihren kompletten Lebenszyklus hinweg diese Aspekte berücksichtigt: „Security & Safety by Design".

Für Unternehmen, denen es an Know-how und/oder Ressourcen für funktional sichere und geschützte Entwicklungen fehlt, bietet der Technologie- und Sicherheitsspezialist NewTec ein breites Portfolio an Leistungen und Produkten an.

1 Einleitung

1.1 Industrial Internet of Things (IIoT) und Industrie 4.0

Industrie 4.0 und das (Industrial) Internet der Dinge (IoT bzw. IIoT) sind auf dem Vormarsch. Viele Fertiger, vor allem im Maschinen- und Anlagenbau und der Automobilindustrie, nutzen bereits digitale Technologien, um effizienter zu produzieren, aber auch für eigene Produkte und neue Dienstleistungen. Intelligente, vernetzte Systeme unterstützen durchgängig Aktivitäten entlang der gesamten Wertschöpfungskette. Wer im Wettbewerb bestehen will, darf bei der digitalen Transformation den Anschluss nicht verpassen.

IIoT-Technologien können überall dort von Nutzen sein, wo prozessrelevante Daten anfallen, beispielsweise Produkt-, Betriebs-, Zustands-, Umgebungs- oder Ortsdaten. Das betrifft alle Elemente der Wertschöpfungskette: Produktionsanlagen, Material und Teile, Logistiksysteme und Fahrzeuge, Mitarbeiter, Lieferanten und Kunden und auch die fertigen Produkte. Diese Daten können vielfältig genutzt werden: zur effizienten Steuerung von Fertigung und Logistik, zur Optimierung von Wartung und Instandhaltung oder für die Erschließung völlig neuer Geschäftsfelder durch innovative informationsbasierte Business-Modelle.

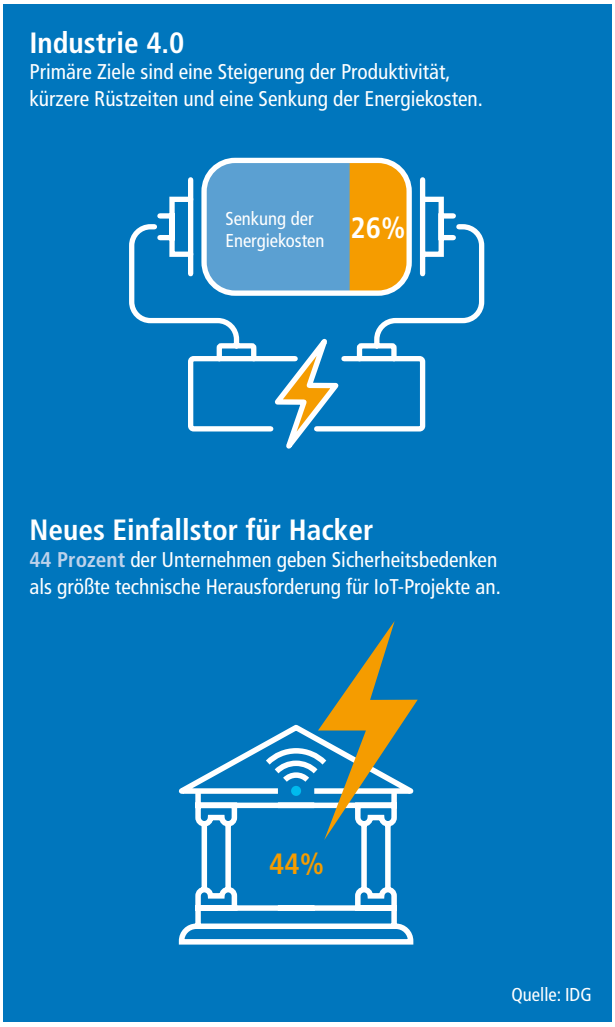
Ein Beispiel: Ein Kunde stellt sich online sein individuelles Produkt zusammen, etwa ein Motorrad. Er wählt Modell, Stil, Rahmendesign, Farbe, Tankgröße usf., klickt auf den Bestellknopf und generiert damit automatisch einen Fertigungsauftrag. Die Produktionsanlagen wiederum sind vernetzt: Bestände und Position der benötigten Teile sind bekannt, ebenso Auslastung und freie Kapazitäten von Maschinen. Alle Teile auf der Stückliste gelangen punktgenau zur Montage, mögliche Probleme in Fertigung oder Logistik werden sofort erkannt und in der Produktionssteuerung berücksichtigt. Wenige Stunden später ist das bestellte Motorrad bereits fertig montiert.

Das ist keine Zukunftsmusik: Harley-Davidson fertigt so in seiner Fabrik in York, Pennsylvania, Maschinen in über tausend verschiedenen Konfigurationen – mit einem Zeithorizont von sechs Stunden ab Bestellung.

1.2 Technische und organisatorische Herausforderungen

Einer aktuellen Studie von IDG zufolge erwarten Unternehmen im D-A-CH-Raum vom IoT zahlreiche positive Impulse für ihr Geschäft, sehen aber auch erhebliche organisatorische und technische Herausforderungen, zum Beispiel mit Bezug auf die Anpassung der Geschäftsprozesse, die Komplexität des Themas IoT, die IT-Infrastruktur oder die Kommunikation zwischen den Abteilungen (siehe nächste Seite).

Die größte Herausforderung ist für die Befragten die Gewährleistung von Sicherheit und Compliance. 44 Prozent der Befragten sehen im Internet of Things ein mögliches neues Einfallstor für DDoS-Attacken (Distributed Denial of Service) oder Hacker-Angriffe. Auch Themen wie Datensicherheit / Disaster Recovery (39 Prozent), Industriespionage (32 Prozent) und Compliance (28 Prozent) beunruhigen die Studienteilnehmer.



In der Studie „Internet of Things 2018" befragte IDG im Herbst 2017 per Online-Umfrage 385 IT-Verantwortliche von Unternehmen in der D-A-CH-Region, darunter strategische (IT-) Entscheider im C-Level-Bereich und in den Fachbereichen, IT-Entscheider und IT-Spezialisten aus dem IT-Bereich.

Was sind die größten technologischen Herausforderungen in Bezug auf IoT bzw. bei der Umsetzung von IoT-Projekten?

Angaben in Prozent. Mehrfachantworten möglich. Basis: n = 310

Security (neues Einfallstor)	43,9
Datensicherheit / Disaster Recovery	39,0
Komplexität des Themas	32,9
Safety / Betriebssicherheit	29,7
ITK-Infrastruktur	29,4
IT-Systeme mit veralteten Betriebssystemen ohne Patch-Möglichkeit	26,5
Mangelnde Netzqualität	25,2
Integration der Devices (Sensoren / Aktoren) in die IT-Infrastruktur	24,2
Das Finden einer geeigneten IoT-Plattform	23,2
Fehlende Technologien / Plattformen / Standards	22,9
Verfügbarkeit / Ausfallsicherheit	21,6
Zu große Datenmengen	20,3
Fehlende oder ineffektive Big-Data-Lösung / Mangelndes Analytics	19,7
Netzzugang für bisher isoliert stehende Produktionsanlagen	16,1
Fehlende Updates für vorhandene Produktionsanlage(n)	7,7
Andere technologische Herausforderungen	1,3

Was sind die größten organisatorischen Herausforderungen in Bezug auf IoT bzw. bei der Umsetzung von IoT-Projekten?

Angaben in Prozent. Mehrfachantworten möglich. Basis: n = 310

Geschäftsprozesse müssen verändert und angepasst werden	40,6
Mangelnde Kommunikation zwischen den beteiligten Abteilungen	31,3
Fehlende Skills der eigenen Mitarbeiter	30,3
Umstrukturierung der Unternehmensorganisation auf IoT-Belange	29,4
Problemfeld „Schnittstelle IT und Fachabteilung (z.B. Produktion)"	29,4
Entwicklung eines Geschäftsmodells	27,1
Fehlende IT-Fachkräfte	26,8
Fehlende Offenheit für Partnerschaften	25,5
Return on Investment von IoT-Projekten ist unklar	25,5
Fehlende Ressourcen (zu wenig Stellen)	21,9
Fehlende Akzeptanz bei Geschäftspartnern und Dienstleistern	19,7
Fehlende Unterstützung durch das Management	18,7
Fehlende Akzeptanz bei Kunden	17,7
Fehlende Skills bei externem Partner (z. B. Systemhaus)	17,1
Zu geringe Forschungsetats in den für IoT relevanten Themen	14,5
Bedenken der Mitarbeiter	13,2
Andere technologische Herausforderungen	1,9

2 Herausforderung Sicherheit

Immer wieder finden sich in IoT-Systemen zum Teil gravierende Sicherheitslücken – in Routern, Druckern oder Kameras, Alarmanlagen oder Herzschrittmachern bis hin zu Kraftwerken. Solche Sicherheitsprobleme bei IoT-Geräten betreffen bei weitem nicht nur Consumer-Produkte. Auch IT-Systeme in der Produktion beinhalten Router, Switches, Steuerungskomponenten oder Workstations, die Schwachstellen aufweisen können.

In der Industrie setzt man darüber hinaus auf die Vernetzung von zahllosen eingebetteten Systemen, die heute oft nur mangelhaft vor Angriffen geschützt sind. Die Produktion wird immer enger mit anderen Bereichen, mobilen Einheiten und sogar Fremdsystemen in der Supply Chain vernetzt. Damit schafft die zukünftige „Industrie 4.0" zahllose potenzielle Schwachstellen und Einfallstore für Schadsoftware.

Außerdem darf nicht vergessen werden, dass es zunehmend Angriffe gibt, die kein Internet benötigen, etwa infizierte USB-Sticks oder Social Engineering (siehe Kasten). Es gibt auch bereits Malware, die gezielt Sicherheitslücken von industriellen Steuerungen ausnutzt. Eine einzige anfällige Komponente reicht aus, um das ganze interne Netz zu kompromittieren.

Die Vernetzung ermöglicht neue Bedrohungen, die die Funktions-, Ausfall- und Manipulationssicherheit gefährden und zu erheblichen Sicherheitsrisiken führen. Die Risiken reichen vom Diebstahl kritischer Informationen bis hin zur Sabotage.
Fazit: Vernetzte Geräte müssen sicher sein, egal wo sie stehen.

2.1 Gezielte Angriffe nehmen zu

Die meisten Cyber-Angriffe verlaufen breit gestreut, und das mit Erfolg auch im Industrieumfeld: Schadprogramme wie WannaCry beeinträchtigten so die Produktion bei hunderten Unternehmen. Angriffe richten sich zunehmend auch auf konkrete Unternehmensanwendungen, z. B. Buchhaltungssoftware (Petya/NotPetya). Sogar über infizierte Firmware-Updates für Industriekomponenten auf gehackten Herstellerseiten wird Malware verbreitet (sog. Waterhole-Attacken).

Gleichzeitig finden seit einigen Jahren immer mehr gezielte Angriffe auf individuelle Unternehmen statt. Davor warnt unter anderem eine globale Studie von B2B International (2017) im Auftrag von Kaspersky Lab. Bereits 27 Prozent der dort befragten Unternehmen berichten von gezielten Angriffen auf ihre Infrastruktur (vs. 21 Prozent im Vorjahr).

Bei gezielten Angriffen verschaffen sich Hacker zunächst Zugang zum Firmennetzwerk, v. a. über automatisierte Schwachstellenscans, aber auch etwa über das Täuschen von Mitarbeitern (Social Engineering), z. B. über Phishing- oder Malware-Mails, die scheinbar aus dem Unternehmen stammen. Ist eine Lücke gefunden, wird manuell Malware für Spionage oder Erpressung installiert. Zunehmend werden dabei gezielt industrielle Steuerungssysteme (ICS) kompromittiert (Stuxnet, Havex, BlackEnergy2). Gefährdet sind u. a. SCADA-Server, HMIs (Human-Machine Interfaces), Workstations, speicherprogrammierbare Steuerungssysteme (SPS) oder Netzwerkkomponenten. Durch Eingriffe in die Steuerung wird auch die Sicherheit der Belegschaft gefährdet. Die neue Malware Trisis/Triton manipuliert sogar direkt Safety-relevante Systeme und gefährdet damit Menschenleben.

2.2 Probleme bei der Absicherung produktionsnaher IT

Viele IoT-Geräte sind für Hacker leichte Ziele: Offene Ports ohne Authentifizierung, voreingestellte Standard-Logins mit Passwörtern wie „admin" oder „1234" oder fehlende Security-Updates sind nur einige verbreitete Fehler der Hersteller. Im Industrieumfeld kommt hinzu, dass bestimmte Besonderheiten produktionsnaher IT-Systeme ihre Absicherung erheblich erschweren. Dazu gehören etwa die Heterogenität der produktionsnahen IT-Systeme, ihre geschäftskritische Bedeutung, Anforderungen der funktionalen Sicherheit und auch die begrenzten Kapazitäten von Embedded-Systemen. Deshalb benötigen Maßnahmen für die IT-Sicherheit bei Industrie 4.0 andere Lösungswege als bei Standard- IT-Systemen.

Heterogene Systeme

Produktionsnahe IT ist häufig nicht standardisiert. Es gibt Tausende Produkte verschiedenster Anbieter mit eigenen Software-Stacks. Experten schätzen, dass in der Industrie ca. 2.000 verschiedene Protokolle im Einsatz sind. Verbindliche Standards für Fertigungsanlagen-Software stecken noch in den Kinderschuhen. Anders als im Office-Umfeld, wo Produkte einiger weniger Hersteller wie Microsoft oder Adobe den Markt dominieren, können Sicherheitsprobleme daher nicht flächendeckend per Update beseitigt werden.

Updates und Sicherheitschecks erschwert

Anders als im Office-Umfeld müssen produktionsnahe IT-Systeme rund um die Uhr einsatzbereit sein. Um Software-Updates einzuspielen, muss der Produktionsbetrieb gegebenenfalls heruntergefahren werden. Viele Systeme mit Auswirkungen auf die funktionale Sicherheit – zum Beispiel Steuerungssysteme – können auch gar nicht ohne Weiteres per Update abgesichert werden, ohne eine erneute Zertifizierung notwendig zu machen. Die Lebensdauer von Steuerungssystemen ist in der Regel um

ein Vielfaches länger als die von klassischen IT-Systemen. Herkömmliche, ressourcenhungrige Sicherheitstechnologien, etwa Virenscans und Netzwerkanalysen, sind häufig in Embedded-Systemen in der Produktion nicht einsetzbar, weil sie die Echtzeitsteuerung gefährden.

2.3 Haftungsrisiken steigen

Anbieter und Betreiber von IoT-Systemen sollten sich auf verschärfte Haftungsregeln einstellen. Unsichere IoT-Geräte, die als Einfallstor in Unternehmensnetze dienen oder als Teil von Botnetzen für Angriffe missbraucht werden, gefährden die Sicherheit. Sicherheit beinhaltet neben dem Schutz vor Angriffen (Security) auch den Schutz von Menschen und Umgebung (Safety). Denn die möglichen Folgen von Cyber-Angriffen umfassen nicht nur wirtschaftlichen Schaden, sondern auch Gefahren für Leben und Gesundheit, wenn Hacker etwa die Kontrolle über vernetzte Fahrzeuge, Brandschutzanlagen, Industrieroboter oder Kraftwerke erlangen.

Es gilt daher als sicher, dass sich die Rechtslage bei IoT-Produkten ändern muss und wird. In den USA und der EU werden bereits Gesetzesvorhaben wie der IoT Cybersecurity Improvement Act diskutiert, die einen Mindeststandard für IT-Sicherheit sichern sollen. Diverse Gremien, darunter der Innenausschuss des Bundestages und die Innenministerkonferenz, fordern die Schaffung verbindlicher IT-Sicherheitsvorgaben auf EU-Ebene und Regelungen zur Produkthaftung für IoT-Produkte.

Schon jetzt greifen in Deutschland auch in Industrie-4.0-Szenarien in vielen Fällen die allgemeinen Regelungen der deliktischen Haftung (§§ 823 ff. BGB) oder vertraglichen Haftung zwischen Kooperationspartnern (§§ 280 ff. BGB). Hinzu kommen ggf. Regelungen der Produkthaftung (ProdHaftG). Angesichts der neuen Rahmenbedingungen durch Digitalisierung und IoT wird intensiv über Gesetzesanpassungen diskutiert.

Neue Gesetze geben die Richtung vor

Das IT-Sicherheitsgesetz (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme), in Kraft seit Juli 2015, verpflichtet Hersteller oder Betreiber von kritischen Infrastrukturen (KRITIS) zu angemessenen organisatorischen und technischen Vorkehrungen (nach dem „Stand der Technik" gemäß IEC 62443) zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse. Kritische Infrastrukturen umfassen u. a. Einrichtungen und Anlagen aus den Bereichen Energie, Informationstechnik, Transport/Verkehr und Gesundheit. Die neue europäische Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie) und das entsprechende deutsche Umsetzungsgesetz nehmen darüber hinaus ab Mai 2018 auch Anbieter digitaler Dienste, z. B. Cloud-Anbieter, in die Pflicht. Die meisten Unternehmen aber fallen nicht unter den Geltungsbereich dieser Gesetze. Deshalb sieht u.a. auch die BMWI-Studie „IT-Sicherheit für die Industrie 4.0" hier weiteren Regelungsbedarf.

EU-Datenschutzverordnung
Die neue Datenschutz-Grundverordnung der EU (DSGVO), die ab Mai 2018 in allen EU-Mitgliedsstaaten verbindlich wird, fordert wirksame technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten (Privacy by Design and Default). Bei Datenschutzverstößen drohen Unternehmen zum Teil drastische Sanktionen bis hin zu Schadenersatzforderungen und Bußgeldern in Millionenhöhe (Art. 83 DSGV). Das gilt unmittelbar auch für IoT-Geräte, wenn sie Daten mit Personenbezug sammeln.

Neues Haftungssubjekt im Verkehrsrecht
Bei der Gefährdungshaftung im Straßenverkehr hat der deutsche Gesetzgeber schon gehandelt. Seit Juni 2017 gibt das Straßenverkehrsgesetz einen rechtlichen Rahmen für autonomes Fahren vor. Damit treten zum ersten Mal auch neue potenzielle Haftungssubjekte in Erscheinung: Führt im Modus des autonomen Fahrens ein Fahrfehler zu Schäden und hat das System den Fahrer nicht aufgefordert, die Kontrolle zu übernehmen, können Fahrzeughersteller und Zulieferer in Regress genommen werden. Das zeigt, wohin die rechtliche Entwicklung gehen kann: Bisher haftete nur, wer einen Schaden verursacht und auch zu verantworten hat. Jetzt kommt auch eine Haftung desjenigen in Betracht, der es nicht verhindert hat, dass ein Schaden entstanden ist. Damit steigt das Haftungsrisiko für Betreiber, Hersteller und Entwickler.

3 Risiken minimieren: Security & Safety

Sicherheit hat strategische Bedeutung

Wenn Anbieter und Anwender von vernetzten Geräten und Lösungen Geschäftseinbußen, Imageverluste und zukünftig auch haftungs- und strafrechtliche Konsequenzen vermeiden wollen, müssen sie bereits bei Konzeption und Entwicklung ihrer Anwendungen den Faktor Sicherheit berücksichtigen (Security & Safety by Design). Wege der Risikominimierung sind die konsequente Einhaltung von Normen und Richtlinien über den gesamten Produktlebenszyklus hinweg und der Nachweis durch Zertifizierung von Komponenten, Software und Prozessen.

Damit wird die strategische Dimension von Sicherheitsprozessen deutlich: Wenn Hersteller ihre Entwicklungs- und Sicherheitsprozesse entsprechend anpassen und weiterentwickeln, verbessern sie mit der Sicherheit ihrer Produkte auch ihre Wettbewerbsfähigkeit. Unternehmen, die nicht über das notwendige Know-how verfügen, müssen es sich aneignen oder einkaufen.

Vertrauenswürdige Systeme brauchen Safety und Security

„Sicherheit" bedeutet für die meisten Unternehmen noch immer vor allem funktionale bzw. Betriebssicherheit, englisch „Safety". Safety umfasst den Schutz von Menschen und Umwelt vor Gefahren, die vom Betrieb eines Systems ausgehen. Dass Systeme ihrerseits auch vor ihrer Umwelt geschützt werden müssen, im Englischen „Security", war lange Zeit kein besonderes Problem. Mit digitaler Transformation und IoT hat sich das grundlegend geändert. Deshalb müssen Unternehmen heute ein neues, integratives Konzept von „Sicherheit" verinnerlichen, welches beide Aspekte – Security & Safety – gleichermaßen berücksichtigt.

Neue Safety-Konzepte für Industrie 4.0

Die flexible Produktion in Industrie-4.0-Szenarien benötigt auch flexiblere, dezentrale Sicherheitskonzepte. Moderne Maschinen sind komplex, modular und flexibel konfigurierbar, und sie arbeiten immer enger mit anderen Maschinen, Robotern und vor allem auch mit Menschen zusammen. Der Trend bei Sicherheitssystemen geht daher weg von starren Schutzzäunen hin zur Ausrüstung von Maschinen mit Sensoren, Sicherheitslogik und Aktoren, die bei Bedarf die Anlage in einen gefahrlosen Zustand bringen können. Maschinen, Sensoren, Aktoren und dezentrale Steuerungen sind zunehmend über Ethernet vernetzt; auch Safety-Controller werden häufig im Verbund betrieben und müssen Informationen sicher untereinander austauschen. Damit entsteht eine immer engere Verflechtung von Safety mit Security.

Security und Safety beeinflussen einander

Ohne Security ist auch keine Safety möglich. Dass Security-Schwachstellen auch die funktionale Sicherheit gefährden, wenn Hacker etwa in kritische Infrastrukturen eindringen, Medizingeräte manipulieren oder Systeme in der Produktion lahmlegen können, ist unmittelbar einsichtig. Zudem werden in Industrie-4.0-Anwendungen auch sicherheitskritische Funktionen mit verteilten und vernetzten Komponenten realisiert. Jede dieser vernetzten Komponenten ist wiederum auch ein potenzieller Zugang zum Netz und muss deshalb gesichert werden.

Häufig werden sich die jeweiligen Schutzziele von Security & Safety auch widersprechen. Einerseits kann es Security-Maßnahmen erschweren, wenn im Interesse von Safety Daten erhoben und zusätzliche Eingriffsmöglichkeiten geschaffen werden müssen. Und andererseits können Security-Maßnahmen wie Verschlüsselung oder Authentifizierung die funktionale Sicherheit beeinträchtigen, indem sie etwa benötigte Systemressourcen binden oder zeitkritische Funktionen verzögern.

Vertrauenswürdige Systeme brauchen Safety und Security. Beide Aspekte von Sicherheit sind miteinander verflochten, beeinflussen einander und müssen daher von Anfang an gemeinsam berücksichtigt werden.

4 Integrierte Sicherheitsentwicklung: Umsetzungsempfehlungen

4.1 Security & Safety by Design

Sicherheit von Anfang an

Produkt- und Anwendungsentwickler können sich an dem Ansatz „Security by Design" orientieren, der sich in der Softwareentwicklung bereits vielfach bewährt hat, u. a. bei Microsoft, Google, Adobe oder Oracle.

Kurz gesagt, bedeutet dieser Ansatz, dass Sicherheitsanforderungen – und zwar jetzt sowohl Safety- als auch Security-Anforderungen – schon vor der Entwicklung eines Produktes genau analysiert und entsprechend berücksichtigt werden. An Funktionen wird nur implementiert, was tatsächlich gebraucht wird, und für alle bei der Bedrohungs- bzw. Gefahrenanalyse identifizierten Szenarien werden schon im Produktkonzept entsprechende Sicherheitsvorkehrungen vorgesehen.

Bei der Gewährleistung der funktionalen Sicherheit ist dieses grundsätzliche Vorgehen ebenfalls schon seit langem Standard. Für die integrierte Sicherheit – Safety und Security – ist zum einen zu beachten, dass dabei jeweils die Maßnahmen aus den oben genannten Safety- und Security-Normen und Anleitungen zur Anwendung kommen. Zusätzlich aber müssen auch die Wechselwirkungen zwischen Security- und Safety-Gefahren und -Maßnahmen analysiert und einbezogen werden.

Nachträgliche und externe Schutzmaßnahmen ungeeignet

Auch der Arbeitskreis Industrie 4.0, initiiert von der Forschungsunion Wirtschaft – Wissenschaft des Bundesministeriums für Bildung und Forschung (BMBF), hält es für unabdingbar, alle Aspekte der Sicherheit von Anfang an in das Design von Produktionssystemen einzubeziehen: Industrie 4.0 erfordere „ein sehr viel proaktiveres Vorgehen in puncto Sicherheit als bisher (insbesondere Security by design)", denn heute würden Sicherheitsfragen oft erst gestellt, nachdem es konkrete Sicherheitsvorfälle gab.

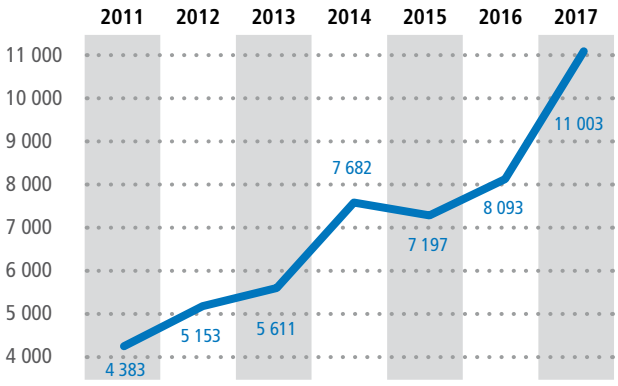
Sicherheitsmaßnahmen nachträglich umzusetzen ist nicht nur aufwändiger und teurer, es schützt auch nur unvollkommen – nämlich nur bis zur nächsten Lücke. Bei vernetzten Embedded-Systemen im Industriebereich sind Nachbesserungen ohnehin schwierig: Ist ein System erst einmal in Betrieb, ist es zu spät für grundlegende Änderungen an seiner Architektur. Wie aufwändig es ist, eine Firmware zu aktualisieren, hängt vom jeweiligen Gerät ab. Und häufig – etwa bei sicherheitsgerichteten Anwendungen – sind nachträgliche Änderungen nicht vorgesehen bzw. würden teure Nachzertifizierungen erfordern. Fazit: Ständig neue Sicherheitslücken in aufwändigen Patch-Zyklen zu schließen, kostet erheblich mehr, als von Anfang an sicher zu entwickeln. Trotzdem müssen natürlich System-Updates prinzipiell vorgesehen sein.

Von der Softwarebranche können IoT-Hersteller auch lernen, dass sich Anwendungen nicht komplett durch externe Schutzmaßnahmen wie Firewalls etc. absichern lassen. Zum einen lassen sich Sicherheitslücken in Komponenten durch externe Systeme nicht immer ohne Funktionalitätsverlust schließen. Und zum anderen zeigt die Erfahrung, dass es Angreifern immer wieder gelingt, die externen Sicherungsmaßnahmen zu umgehen und trotzdem in das Netz einzudringen.

„Eine nachträgliche Implementierung von Sicherheitsmaßnahmen ist bedeutend teurer und bietet im Allgemeinen weniger Schutz als Sicherheit, die von Beginn an in den Systementwicklungsprozess oder in den Auswahlprozess für ein Produkt integriert wurde. Sicherheit sollte daher integrierter Bestandteil des gesamten Lebenszyklus eines IT-Systems bzw. eines Produktes sein." (Bundesamt für Sicherheit in der Informationstechnik, BSI-Grundschutz)

Ständiges Security-Management

Safety-Maßnahmen werden einmalig implementiert und zertifiziert und dürfen dann nicht mehr verändert werden. IT-Security erfordert im Gegensatz dazu eine ständige Beobachtung der Bedrohungslage und immer neue Abwehrmaßnahmen. Denn während die Safety-Gefahrensituation relativ konstant bleibt – neue Gefahren treten nur bei Veränderungen an Maschinen und Prozessen auf – ändert sich die Bedrohungssituation in Bezug auf Security täglich. Eine Statistik des Potsdamer Hasso-Plattner-Instituts (HPI) weist für 2017 den Rekordwert von weltweit über 11.000 neu entdeckten Software-Sicherheitslücken aus – gegenüber ca. 8.100 im Jahr 2016 und ca. 5.000 in 2010. Die Zahl der neuen Schwachstellen mit „mittlerem" Schweregrad (nach dem Common Vulnerability Scoring System CVSS) nahm gegenüber 2016 sogar um über 50 Prozent zu, Lücken mit „hohem" Schweregrad um 17 Prozent.



Zahl neuer Schwachstellen erreicht Rekordwert (Quelle: HPI)

Sicherheit ist eine Eigenschaft des Gesamtsystems
Weil eine einzelne Komponente die Sicherheit des gesamten Systems gefährden kann und verschiedenste Wechselwirkungen auf das Verhalten von Komponenten und System Einfluss haben, müssen vernetzte Systeme immer ganzheitlich betrachtet werden.

Als ganzheitlicher methodischer Ansatz verfolgt „Security & Safety by Design" das Ziel, Bedrohungen und Gefährdungen systematisch und strukturiert zu beherrschen. Dabei müssen alle relevanten Ebenen eines Systems einbezogen werden:

- Menschen (Awareness, Qualifikationen)
- Technik (Komplexität, Vernetzung)
- Organisation (Prozesse, Verantwortlichkeiten)

Einige der Leitprinzipien sind:

- Die gesamte Sicherheitskette einbeziehen
- Maßnahmen auf Prozess-, System- und Komponentenebene
- Mehrstufige Security-Barrieren (die „Ritterburg")
- Security von innen nach außen auf allen Ebenen – von der Betriebs- bis zur Feldebene, von der Zutrittskontrolle bis zum Kopierschutz.

4.2 Normen und Anleitungen

Die Umsetzung integrierter Sicherheitsentwicklungen gestaltet sich allerdings schwierig. Denn die meisten Unternehmen im Industrieumfeld – Lösungsanbieter ebenso wie Anwender – haben damit kaum Erfahrung, und es gibt auch noch keine einschlägigen Normen für integrierte Sicherheit.

Unternehmen kennen in der Regel die spezifischen Anforderungen der funktionalen Sicherheit in ihrer Branche gut und können sich bei ihrer Umsetzung auf detaillierte Normen stützen, z. B. die Safety-Grundnorm IEC 61508 für sicherheitsrelevante elektrische und elektronische Systeme sowie sektorspezifische Normen wie z. B. EN ISO 13849 und IEC/EN 62061 für Maschinen oder ISO 26262 für die Automobilindustrie.

Für die IT-Sicherheit in Unternehmen gibt es wiederum die Norm ISO 27001 für Office-IT, die ISO/IEC 27034 (Anwendungssicherheit) und vor allem die IEC 62443 für „Industrial Communication Networks", also die IT-Sicherheit von industriellen Automatisierungs- und Steuerungssystemen.

Die meisten Industriezweige greifen heute beim Thema IT-Security auf die IEC 62443 zurück, die damit zur zentralen Norm für die Industrie 4.0 geworden ist. Die IEC 62443 kann gewissermaßen als Grundnorm für Industrial Security analog zur Safety-Grundnorm IEC 61508 angesehen werden (letztere verweist mit Bezug auf festzulegende Security-Anforderungen auf die IEC 62443). Somit wird eine integrierte Sicherheitsentwicklung diese beiden Normen (bzw. ggf. sektorspezifische Ausprägungen) zugleich berücksichtigen müssen.

Tipp

Generell empfehlenswert sind zudem die ausführlichen „IT-Grundschutz"-Standards und Kataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Vergleichbare Anleitungen für eine integrierte Umsetzung von Safety- und Security-Maßnahmen, welche die beschriebenen Wechselwirkungen berücksichtigen, gibt es noch nicht. Der IT-Grundschutz des BSI nimmt funktionale Sicherheit ausdrücklich aus. Für die Sicherheit „industrieller Steuerungssysteme" in der produzierenden Industrie und in kritischen Infrastrukturen hat das BSI 2013 sein „ICS-Security-Kompendium" herausgegeben, 2014 ergänzt durch einen Teil für Komponentenhersteller. Auch hier thematisiert das Amt fast ausschließlich die Security und verweist in Bezug auf die funktionale Sicherheit auf die genannten Safety-Normen.

4.3 Gefahren- und Bedrohungsanalyse

Ausgangspunkt jeder sicheren Entwicklung ist eine umfassende Risikoanalyse. Dabei gilt es sowohl Safety-Risiken (Gefahren) als auch Security-Risiken (Bedrohungen) zu identifizieren und zu bewerten. Alle Risiken, die über ein tolerierbares Restrisiko hinausgehen, müssen durch entsprechende Schutzmaßnahmen abgefangen werden.

Schutzziele definieren
Dabei sind jeweils verschiedene Schutzziele potenziell von Bedeutung, die je nach Anwendung auf ihre Relevanz geprüft und berücksichtigt werden müssen.

Bei der **Safety** geht es immer darum, ordnungsgemäße Abläufe zu sichern (Zuverlässigkeit) und – vor allem – Menschen und Umwelt vor Gefährdungen durch Fehlfunktionen von Maschinen und Anlagen zu schützen (funktionale Sicherheit). Was das im Einzelnen bedeutet, ist von der konkreten Anwendung abhängig.

Maßnahmen der **Security** sollen Personen und Systeme bzw. Infrastrukturen vor Angriffen durch unberechtigte Nutzung, Manipulation, Sabotage oder Datendiebstahl schützen und so die Steuerung und Kontrolle relevanter Prozesse sichern. Dazu gehören die Integrität von Daten und Diensten (Absicherung gegen Verlust und Manipulation von Daten; korrekte Funktion),

Vertraulichkeit (Absicherung vor Missbrauch; bestimmte Daten und Dienste sind nur einem autorisierten Nutzerkreis zugänglich) und Verfügbarkeit (Antwort mit tolerierbarer Verzögerung). Weitere Schutzziele von Security sind Datenschutz (Schutz personenbezogener Daten vor Missbrauch) und Know-how-Schutz (Intellectual Property).

Gefahren- und Bedrohungsszenarien identifizieren

Eine möglichst umfassende Identifizierung konkreter Gefahren- und Bedrohungsszenarien für eine Anwendung hilft, bestehende Risiken zu bestimmen und zu bewerten. Für jede Komponente eines Systems bzw. einer Anwendung muss das damit verbundene Schadenspotenzial ermittelt und der Schutzbedarf bestimmt werden. Dabei wird zunächst die Art des Risikos analysiert: Welche Bedrohungen können die betreffende Komponente konkret betreffen – etwa Manipulationen, Sabotage oder Datendiebstahl? Welche Gefährdungen für Menschen und Umgebung können von Fehlern oder erfolgreichen Angriffen ausgelöst werden?

Ein Beispiel ist der Einsatz von Industrierobotern, die direkt mit Menschen zusammenarbeiten (Cobots). Je nach Einsatzprofil wird eine Analyse sehr wahrscheinlich ergeben, dass bei bestimmten Fehlern, z. B. einem Sensor-Ausfall, die Gesundheit von Bedienern gefährdet sein kann. Parallel muss aber auch bedacht werden, was alles passieren kann, wenn die Infrastruktur kompromittiert wäre, die die Cobots parametrisieren und steuern soll. Gerade wenn im Herstellungsprozess Gefahrenstoffe verwendet werden oder hohe Temperaturen auftreten, kann eine manipulierbare Steuerung zu extremen Risiken führen.

Risiken bewerten und Sicherheitsstufen bestimmen

Um die Risiken adäquat abschätzen zu können, ist zu bewerten, unter welchen Voraussetzungen ein bestimmter Fehler auftreten oder ein Angriff stattfinden kann, wie schwerwiegend die Folgen sein können und mit welcher Wahrscheinlichkeit sie eintreten.

Für die **funktionale Sicherheit** unterscheidet die Safety-Basisnorm IEC 61508 vier Sicherheitsstufen, die sogenannten Safety Integrity Levels (SIL) 1 bis 4. Das Safety Integrity Level ist ein Maß für die zu erreichende bzw. erreichte risikomindernde Wirksamkeit von Sicherheitsfunktionen. Die SIL für jede Anwendung ist abhängig von dem bei Fehlern zu erwartenden Schadensausmaß bzw. der Schwere der drohenden Verletzung, der Häufigkeit und Dauer der Risiko-Exposition, der Eintrittswahrscheinlichkeit des Fehlers und den Möglichkeiten der Gefahrenabwendung bzw. -begrenzung.

Für branchenspezifische Anwendungen helfen dabei sektorspezifische Normen, z. B. IEC 62061 für Maschinen oder ISO 26262 für die Automobilindustrie. Bei der Bewertung der Sicherheitsperformance muss stets die gesamte Sicherheitskette betrachtet werden, also alle möglichen Fehler für alle Komponenten eines Systems.

Für die **Security** wird bei der Risikobewertung unter anderem gefragt, welche bekannten Schwachstellen bestehen, wie groß der Aufwand für einen erfolgreichen Angriff sein müsste und wie gravierend die Folgen eines solchen wären. Die Analyse richtet sich dabei auf technologische und infrastrukturelle ebenso wie auf organisatorische Schwachstellen (Stichwort Anwender). Ziel ist es, eine möglichst erschöpfende Aufstellung der wahrscheinlichsten und schädlichsten möglichen Angriffe zu erhalten, die zeigt, vor welchen Bedrohungen und Angriffsvektoren man sein Produkt vornehmlich schützen muss.

Insbesondere wird bei einer Bedrohungsanalyse auch das Risiko für verschiedene Angreiferprofile bzw. Angriffsvektoren errechnet. Ein potenzieller Angreifer könnte etwa ein Hacker sein, ein Wettbewerber, Angestellter eines Dienstleisters (etwa des Cloud-Anbieters) oder ein unzufriedener eigener Mitarbeiter. Daraus ergeben sich Annahmen darüber, welches Vorgehen ein Angreifer wählen wird, wie hoch seine Motivation einzuschätzen ist, welchen Schaden er anrichten kann und welche Erfolgsaussichten er hat. Aus diesen Aspekten – Mittel, Ressourcen, Fähigkeiten, Motivation – ergeben sich risikobasierte Prioritäten: Vor welchen Angreifern muss das Produkt vor allem geschützt werden?

Darauf basierend definiert auch die Industrial-Security-Norm IEC 62443 vier Sicherheitsstufen (Security Levels, SL), die ein Maß für die zu erwartende Bedrohung eines Systems durch Angriffe darstellen. SL-1 gilt für die Gefahr zufälliger Beeinträchtigungen oder Manipulationen etwa bei Fehlanwendungen durch beliebige Nutzer, SL-2 bis SL-4 beziehen sich auf gezielte Angriffe. SL-2 geht dabei von einem Angriff mit einfachen Mitteln und begrenzten Ressourcen aus (durchschnittliche Fähigkeiten, niedrige Motivation, etwa Hobby-Hacker). SL-3 bezieht sich auf Angriffe mit ausgefeilten Mitteln und begrenzten Ressourcen (professionelle Hacker, kosteneffektive Angriffsszenarien) und SL-4 auf Angriffe mit ausgefeilten Mitteln und umfangreichen Ressourcen (z. B. Geheimdienste mit Spezialwissen).

Diese Sicherheitsstufen werden in der IEC 62443 sowohl als Zielstellung (SL-Target/SL-T als Ergebnis der Bedrohungs- und Risikoanalyse), erreichbares Schutzniveau (SL-Capability/SL-C als Fähigkeit bei richtigem Einsatz) oder tatsächlich erreichtes Schutzniveau des Gesamtsystems (SL-Achieved/SL-A) verstanden. Um eine Komponente mit einem bestimmten Schutzniveau SL-C auszustatten, muss der Komponentenhersteller bei der Entwicklung bestimmte funktionale und nicht-funktionale Security-Anforderungen berücksichtigen und einen IT-sicheren

Entwicklungsprozess sicherstellen. Der Integrator, z. B. Maschinenbauer, erreicht in einem konkreten Projekt und mit der Gesamtheit der verwendeten Komponenten ein resultierendes Schutzniveau SL-A (das mindestens eine vom Betreiber definierte SL-T erreichen muss). Außerdem bezieht die Norm auch den Reifegrad der Sicherheitsprozesse eines Unternehmens ein – aus Sicherheitsstufe der technischen Lösungen und Reifegrad der Prozesse ergibt sich die Schutzklasse (Protection Level, PL-1 bis PL-4) einer Anlage.

4.4 Maßnahmen zur Risikominimierung

Mit der Kenntnis der Risiken, Bedrohungen und Gefahren ist man in der Lage, für jede Komponente des Systems geeignete Maßnahmen zur Risikominimierung zu definieren. Das umfasst zum einen vorbeugende Maßnahmen, die Fehler oder Angriffe von vornherein unmöglich machen, als auch solche, die helfen, Fehler abzufangen oder Attacken zu erkennen und abzuwehren. Für die funktionale Sicherheit ergeben sich die Maßnahmen aus den genannten Safety-Normen, für die Security können etwa die IEC 62443, die BSI-Grundschutz-Dokumente sowie Anleitungen der Branchenverbände (z. B. VDMA, VDI, ZVEI) oder der Plattform Industrie 4.0 herangezogen werden. Die Plattform Industrie 4.0 ist ein Netzwerk von Experten aus den Bundesministerien für Wirtschaft und für Forschung, der Wirtschaft und der Wissenschaft.

Allerdings berücksichtigen diese Anleitungen, wie schon erwähnt, noch nicht ausreichend die Wechselwirkungen zwischen Safety- und Security-Aspekten. Trotzdem ist es sehr wichtig, diese Beziehungen zu analysieren, und zwar einerseits auf Ebene der Risiken (Security-Schwachstellen von Safety-Systemen, mögliche Auswirkungen von Security-Angriffen auf funktionale Sicherheit etc.) und zum anderen auch auf Ebene der Maßnahmen (z. B. Auswirkungen von Security-Maßnahmen auf die Verfügbarkeit von Safety-Funktionen).

Modul- und Systemtests sowie Netzwerk-Penetrationstests helfen festzustellen, ob die definierten Maßnahmen korrekt umgesetzt und wirksam sind. Außerdem sollten die Entwicklungs- und Fertigungsprozesse und die ergriffenen Sicherheitsmaßnahmen sorgfältig dokumentiert werden. Die Einhaltung von IEC 62443 und ISO 27001 sowie IEC 61508 oder sektorspezifischen Normen kann geprüft und zertifiziert werden, zum Beispiel durch den TÜV. Das betrifft die Einhaltung von Sicherheitsstandards für Entwicklungs- und Fertigungsprozesse, Systeme oder Systemkomponenten inkl. Security-Funktionen oder SIL.

4.5 Sicherheitsmanagement

Mit Security & Safety by Design können Hersteller und Betreiber von IIoT-Produkten gewährleisten, dass ihre Geräte und Anwendungen nach dem neuesten Stand der Technik abgesichert sind und allen geltenden Sicherheitsnormen entsprechen. Aber auch nach der Markteinführung sind sie weiterhin gefordert. Durch kontinuierliches und konsequentes Sicherheitsmanagement müssen sie sicherstellen, dass insbesondere neue Security-Bedrohungen schnell erkannt und Sicherheitslücken zügig geschlossen werden. Bei der Vielzahl von Komponenten, die in den vernetzten Wertschöpfungsketten der Industrie 4.0 zusammenarbeiten, ist das alles andere als trivial. Zudem ist Herstellern auch aus Haftungsgründen dringend zu empfehlen, neue Entwicklungen bei Normen und Standards aufmerksam zu beobachten.

Die Plattform Industrie 4.0 empfiehlt in diesem Zusammenhang die Etablierung eines Informationssicherheits-Managementsystems (ISMS). Der BSI-Standard 200-1 beschreibt den Aufbau eines solchen Systems mit den vier Komponenten Sicherheitsprozess, Ressourcen, Mitarbeiter und Management-Prinzipien. Der Sicherheitsprozess als zentrales Element des Management-Systems ist als zyklischer Prozess nach dem PDCA-Modell (Plan, Do, Check, Act) konzipiert. Im Zusammenhang mit Industrie 4.0 ist dabei ein ganzheitlicher Ansatz erforderlich, der alle Unternehmensteile mit Office-IT, Produktentwicklung und Produktions-IT beinhaltet.

Um ein ISMS umzusetzen, müssen eindeutige Rollen und Zuständigkeiten festgelegt werden. Zusätzlich zum „Chief (Information) Security Officer (C(I)SO)" empfiehlt die Plattform Industrie 4.0 die Einsetzung eines „Industrial Security Officers", der dafür sorgt, dass die Security bereichsübergreifend verwaltet und das mit der organisatorischen Trennung von Office- und Produktions-IT verbundene Silodenken überwunden wird.

5 NewTec unterstützt bei „Security & Safety by Design“

Hersteller und Anwender müssen die Sicherheit von IIoT-Anlagen umfassend gewährleisten. Wenn sie nicht über genügend Know-how und Ressourcen verfügen, müssen sie diese aufbauen oder die Hilfe von Experten suchen.

Als Technologie- und Sicherheitsspezialist unterstützt NewTec Unternehmen bei der Umsetzung von Security- und Safety-Anforderungen für Industrie 4.0: Die Safety- und Security-Experten führen detaillierte Gefahren-, Bedrohungs- und Risikoanalysen durch, leiten notwendige Maßnahmen ab und helfen auf Wunsch bei der Umsetzung. Für viele Anforderungen im IIoT- und Cloud-Umfeld hat NewTec auch schon fertige Lösungen, die an die individuellen Anforderungen des jeweiligen Anwenders angepasst werden.

Auszug aus dem NewTec-Portfolio

5.1 NTSafetySolutions

Produktentwicklung
nach geltenden Sicherheitsnormen, z. B. IEC 61508, IEC 62061, ISO 26262, ISO 13849

- Konzeption und Realisierung von sicherheitsrelevanten, komplexen elektronischen Systemen
- Als beratender Partner oder Full-Service-Auftragnehmer
- Produktentwicklung über gesamten Lebenszyklus Ihres Produktes
- Inkl. Industrialisierung und Serienbetreuung, Zulassung, kontinuierliche Verbesserungen bestehender Systeme

Plattformlösungen
inkl. IP-Cores für die schnelle Realisierung funktional sicherer Lösungen bis SIL 3

- NTSafeDrive: Plattform zur Ansteuerung von Servoantrieben mit erweiterten Sicherheitsfunktionen
- NTMicroDrive: Kompakte Software- und Hardware-Lösung für das sichere Ansteuern von Elektromotoren bis 10 W
- NTSafePLC: Hochperformante SPS-Plattform für Industriesteuerungen bis SIL 3 / PL e Cat 4
- SafeFlex: Entwicklungsumgebung für FPGA-basierte Safety-Lösungen mit Evaluierungsboard

Beratung & Services

- Gefahren- u. Risikoanalyse
- Fehleranalyse (FMEA)
- Strategieberatung: Fehler vermeiden, Fehler beherrschen

Know-how-Transfer

- Individuelle Trainings, Workshops und Seminare
- Methodik sicherer Produktentwicklung und Herstellung nach anerkannten Praktiken

5.2 NTSecuritySolutions

Security-Prozessberatung und Bedrohungs-/Risikoanalysen
gemäß geltender Normen wie IEC 62443

- Prozessberatung in der IT-Sicherheit
- Planung der IT-Sicherheit
- Schwachstellenanalysen
- Trainings und Workshops IEC 62443
- Beratung IEC 62443

Security-Strategieberatung
für die Absicherung von Systemen

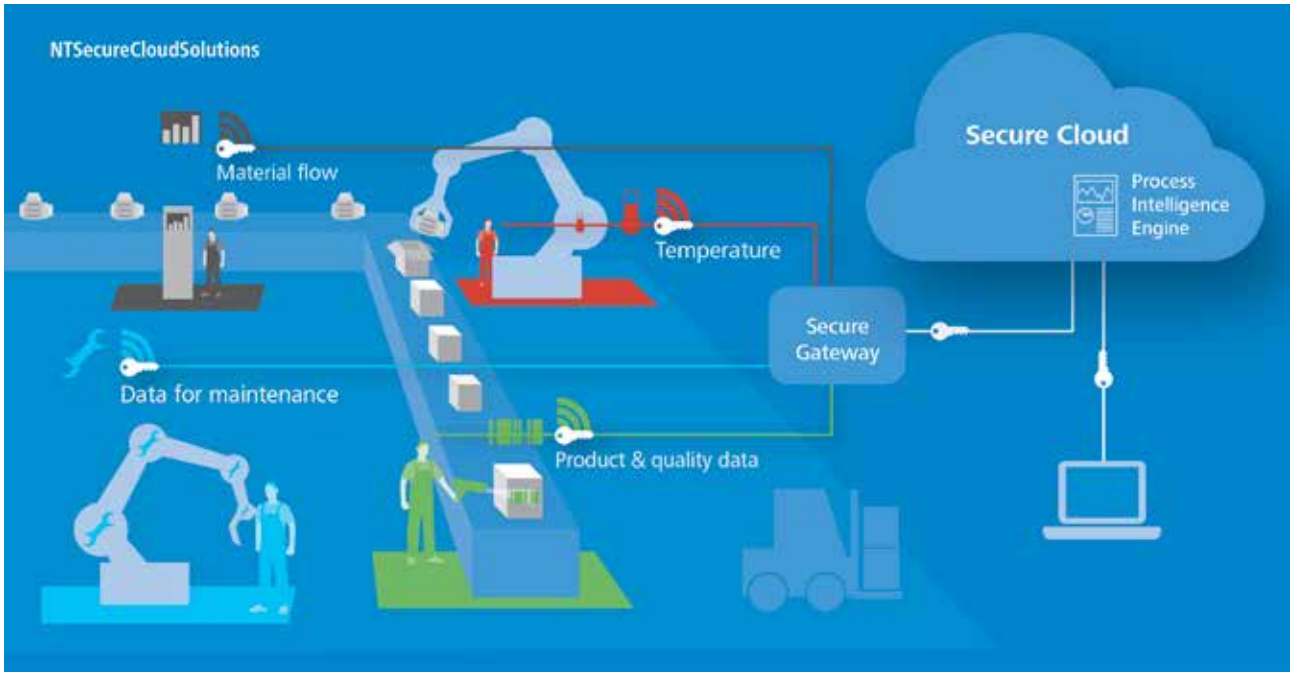
- Entwicklung von Security-Konzepten
- Sichere Datenübertragung
- Kryptographieverfahren
- Zugangskontrollverfahren
- Trainings und Workshops
  - Ermittlung von Schutzzielen
  - Bedrohungs- und Risikoanalyse
  - Festlegung von Security Requirements

Verifizierung und Validierung
der Wirksamkeit von Security-Maßnahmen

- Penetration-Tests
- IT-Security-Robustness-Test (DoS, CRC Violation, ...)
- Statische Codeanalyse (mit z. B. Polyspace)
- Validierung der Anforderungen und des Security-Konzepts
- Beurteilung der IT-Sicherheit
- Handlungsempfehlungen

Security-Monitoring
von Systemen im laufenden Betrieb

- IT-Störungsmanagement im Sicherheitsprodukt-Lebenszyklus
- Kontinuierliche Identifikation und Bewertung von Bedrohungen und Schwachstellen



5.3 NTSecureCloudSolutions

NTSecureCloudSolutions umfasst in der Entwicklung befindliche IoT-Lösungen und Services, die in Verbindung mit anderen Lösungen aus dem Safety- und Security-Portfolio von NewTec Unternehmen bei der Umsetzung von Produkten und Dienstleistungen im Cloud-Umfeld unterstützen und dabei helfen, heterogene Dienste, Technologien und Prozesse in eine sichere Cloud-Architektur zu integrieren.

Lösungen

Kern der NTSecureCloudSolutions ist eine schlüsselfertige Plattform zertifizierter sicherer Hard- und Softwarelösungen mit essenziellen Sicherheitsfunktionen wie z. B. Ende-zu-Ende-Verschlüsselung, Zertifikate-Management, Policy-Management und drahtloser Geräteaktualisierung. Im Endausbau enthalten:

- NTSecureDevices: IoT-Endgeräte / Sensorknoten
- NTSecureGateway: IoT-Gateways für die geschützte Cloud-Anbindung
- NTSecureCloud: Baukastensystem für sichere Cloud-Anwendungen (Secure Application Framework)

Dienstleistungen

- IoT-Geschäftsmodellentwicklung
- Security-Beratung und Schulungen
- Safety-Beratung und Schulung
- Managed Services rund um den sicheren Betrieb.