Jan Ludwig Tiedemann

Digitalisierung der industriellen Dinge

Worauf es bei der Verbindung von IT und OT ankommt

Von der Nachrüstung alter Geräte, über die Vernetzung bis hin zu den eigentlichen digitalen Wundern, die den Kern von Industrie 4.0 ausmachen, sind bei der Digitalisierung von Sensoren, Aktoren, Maschinen und Anlagen – den ‚industriellen Dingen' – höchst unterschiedliche Aufgabenstellungen zu meistern und Risiken zu umschiffen. Sie alle haben jedoch eines gemein: Die Anforderungen an Effizienz, Bedien- und Beherrschbarkeit, Interoperabilität und Sicherheit steigen und werden komplexer. Ganzheitliche Lösungsansätze sind deshalb unerlässlich. Den ‚Dinge'-nahen Edge Plattformen und ihrer Sicherheit sind hierbei besondere Bedeutung beizumessen.

1 Einführung

Als Maschinen noch mit speicherprogrammierbaren Steuerungen oder sogar analogen Mechanismen automatisiert wurden, war es für manche Maschinenschlosser schon Hightech, wenn ihre Maschine über das Stromnetz gleichzeitig auch einfache Stellbefehle übertragen konnte. Heute weiß dagegen jedes Kind, dass man sich aus der Ferne Dinge bedienen und sie in der vollen Bandbreite ihrer Möglichkeiten steuern kann. Wenn Computerspieler komplexe Abwehrsysteme gegen Monsterhorden oder die Besiedlung von Sonnensystemen automatisiert und von überall betreiben können, warum sollte dies nicht auch für Horden von Maschinen im Ballett der modernen industriellen Produktion gelten?

Wirklich beeindruckend sind heute allenfalls noch Lösungen, die auf künstlicher Intelligenz oder den diversen, fast magischen[1] Vorstufen dieser Vision basieren. Wenn beispielsweise ein Roboter nicht arbeitet, weil er selbstständig erkennt, dass ein Mensch in der Nähe keinen Helm trägt. Wenn der Kunde bei seiner Bestellung aus 16 Millionen Farben oder mehr wählen kann und jedes Werkstück ein Unikat (‚Lot Size 1') ist. Oder wenn eine Maschine selbst Ersatzteile bestellt und eine Wartung beauftragt, weil sie die Ermüdungserscheinungen ihrer eigenen Verschleißteile erkennt.

Neben den Chancen ergeben sich aber auch Risiken. Was digital steuerbar ist, lässt sich prinzipiell auch digital angreifen. Wer Produktionsanlagen in Brasilien aus der deutschen Provinz zugreifbar macht, der ermöglicht dies – wenn er nicht aufpasst – schnell auch Kriminellen aus einem Internetcafé in Manila. Und wer komplexen selbstlernenden Algorithmen eine einfache Vernetzung ermöglicht, schafft potentiell den fruchtbaren Boden für eine sich selbst verbreitende Schadsoftware. Jede Betrachtung der Digitalisierung muss daher die helle und die dunkle Seite der neuen Welt adressieren.

2 Neue Geschäftsmodelle

Bereits seit vielen Jahren streifen uns Themen wie Industrie 4.0, das Industrielle Internet der Dinge (IIoT) und Edge Computing. Zahlreiche Unternehmen haben schon in entsprechende neue Geschäftsmodelle investiert: der ‚Digital Transformation Markt' wächst kräftig mit einer durchschnittlichen jährlichen Rate von 16,5%[2]. Ein großes neues Anwendungsfeld stellen beispielsweise datenbasierte Dienstleistungen wie vorausschauende Wartung dar, die nicht nur Kosten senken können, sondern auch zusätzliche Umsätze und Gewinne erzielen. Das FIR der RWTH Aachen geht davon aus, dass derzeit zwar immerhin noch 80% der Umsätze durch den Verkauf neuer technischer Geräte und nur 20% durch Services erzielt würden. Diese 20% könnten aber 60% des Gewinns erzielen.[3]

Im Zuge der Digitalisierung der Industrie darf daher nicht unterschätzt werden, dass diese auch einen Wandel – oder zumindest eine Umverteilung – vom statischen Produktgeschäft zum Servicemodell mit sich bringt. Der Trend hin zur ‚Subscription Economy' ist in diesem Rahmen ein weiterer Beschleuniger für die Digitalisierung. Denn wer Geräte, ganze Anlagen oder auch einzelne Anwendungen nicht mehr nur verkauft, sondern auch ‚as a Service' – beispielsweise über Pay-per-Use-Modelle anbietet

1 in leichter Überhöhung zu Arthur C. Clarkes „Jede hinreichend fortschrittliche Technologie ist von Magie nicht zu unterscheiden."

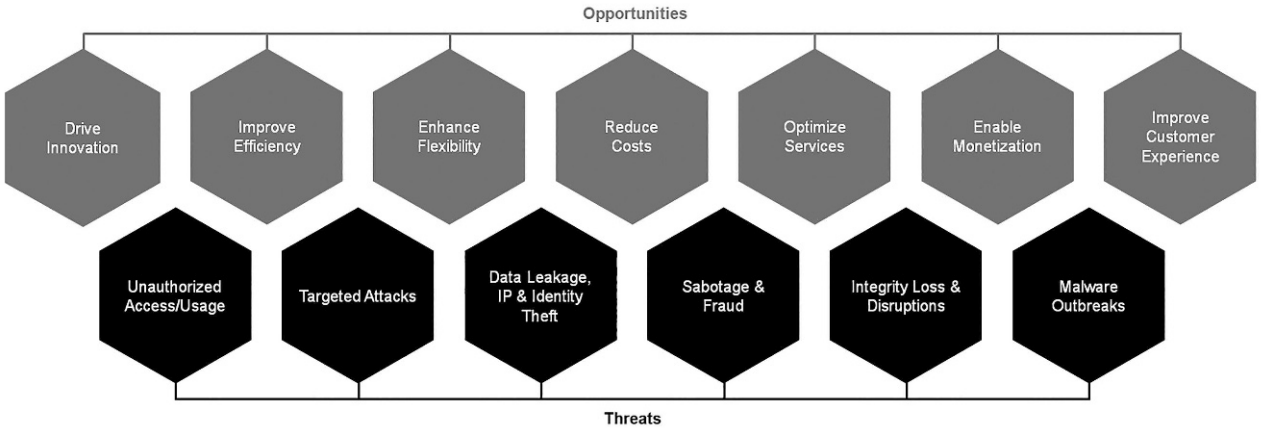
2 https://www.marketsandmarkets.com/PressReleases/digital-transformation.asp

3 https://www.zuora.com/resource/nutzen-sie-subscriptions-als-grundlage/

Jan Tiedemann

ist der Lösungsarchitekt der Industrie-Division von secunet und dort für die Pflege und Weiterentwicklung der Solutions im Industrieportfolio verantwortlich. In seiner Rolle sorgt er für den Informationsaustausch zwischen bzw. mit Interessenten, Kunden, Partnern sowie internen und externen Stakeholdern und arbeitet in der agilen Produktentwicklung mit.
E-Mail: jan.tiedemann@secunet.com

Abb. 1 | Chancen und Risiken der IT-Anbindung der OT



und/oder Feature-basierte Lizenzen in agilen Abonnements bereitstellt – der braucht auch valide Daten über die Nutzung seiner Services.

Ob man im Strudel der Digitalisierung erfolgreich ist oder nicht entscheidet sich insbesondere an der Fähigkeit, Daten absolut zuverlässig und manipulationssicher zu erfassen, effektiv und effizient zu verarbeiten und sicher übertragen zu können. Wird hier jedoch manipuliert oder die digitale Infrastruktur als Einfallstor für dunkle Gestalten missbraucht, verliert der Geräte-, Maschinen- und Anlagenbau mit jeder nicht erfassten Betriebsstunde Umsatz und Gewinn. Unsicherheit und das daraus resultierende Zögern sind mitunter die wichtigsten Gründe, warum gerade in der deutschen Industrie noch nicht jeder beim Upgrade auf die Version 4.0 so mitziehen kann, wie sie oder er das gerne möchte.

3 Edge Computing

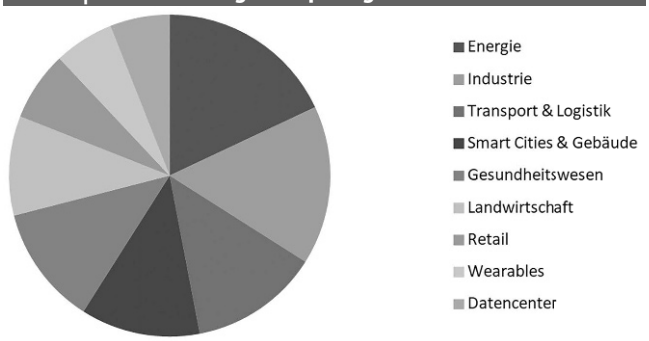
Für all das und noch viel mehr steht das Mega-Buzzwort Digitalisierung, und an keiner Stelle zeigt es sich mehr als dort, wo sich ‚die Dinge' befinden. Am Rande der Netzwerke – am Edge – trifft die IT (Information Technology) auf die sogenannte OT (Operational Technology). Hier endet das Datenübertragungsnetz und bindet Dinge wie Steuerungen an, die heute keine hardwarebasierte SPS sondern eine Soft-SPS konform der Norm IEC 61131 sein können – oder auch alles andere, was mindestens eine serielle RS-232 oder RS-485 Schnittstelle besitzt. Hier befinden sich neben Aktoren auch Sensoren, die Daten aus der ‚physischen Welt' in die ‚digitale Welt' senden. In den seltensten Fällen handelt es sich dabei um neue Strukturen ‚auf der grünen Wiese'. Vielmehr sind es ‚Brownfields', also ein Mix aus installierter Basis – die man nicht mal eben neu anschaffen kann, weil sie immens viel gekostet hat – und neuen Systemen.

Betrachtet man den Energiesektor, so gibt es hier eine Vielzahl von Dingen zu digitalisieren. Beispielsweise Endanwender-nahe Lösungen wie Verbrauchszähler, e-Mobility Ladestationen oder Solarzellen, die man heute bereits ‚as a Service' beziehen kann[4]. Aber auch bei der Energiegewinnung und Verteilung gibt es noch zahlreiches Optimierungspotenzial. Die Internationale Energieagentur schätzt beispielsweise, dass die Digitalisierung im Öl- und Gassektor die Produktionskosten um bis zu 20 Prozent senken kann. In diesem sogenannten Upstream- und Midstream-Sektor könnten viele Milliarden an Kapital- und Betriebskosten eingespart werden[5]. Zahlreiche weitere Anwendungsfelder finden sich beispielsweise in der Wasserwirtschaft oder beim Management regenerativer Energien.

Der Industriesektor wiederum arbeitet daran, mit Virtuellen Fabriken die Produktionseffizienz zu steigern und über digitale Zwillinge von der Produktentwicklung bis hin zur vorausschauenden Wartung neue Potenziale aus der Digitalisierung zu schöpfen. Auch im Transport- und Logistikmarkt gibt es eine Vielzahl von Lösungen, die mittels Digitalisierung neue Mehrwerte schaffen sollen – von der intensiveren Nutzung der Strecken in Ballungszentren durch die Digitalisierung zunehmend kleinerer Gleisabschnitte bis hin zu Lösungen für das autonome Fahren, die – ganz gleich ob Zug, Straßenfahrzeug oder autonomes Logistik-Vehikel – von einer Erhöhung der ‚Situational Awareness' durch maschinelles Sehen und dem Austausch mit weiteren Devices profitieren.

Städte werden durch Digitalisierung vor allem nachhaltiger, das Gesundheitswesen durch eHealth vor allem effektiver, die Landwirtschaft erhöht mittels Smart Farming ihren Flächenertrag – bei geringerer Boden- und Umweltbelastung – und automatisiert die Bewirtschaftung. Im Retailsektor werden wir einen besonderen Boom von Technologien sehen, die wegen Covid-19 das kontaktlose Einkaufen fördern – beispielsweise durch automatisier-

Abb. 2 | Märkte des Edge Computings[6]



4 https://sonnen.de/sonnen-now/

5 https://www.strategyand.pwc.com/report/drilling-for-data

6 Quelle: www.grandviewresearch.com

te Checkout-Terminals mit Videoerkennung der Ware und angeschlossenen kontaktlosen Zahlungssystemen. Die Beispiele ließen sich beliebig fortsetzen.

Märkte für diese Digitalisierung finden sich dabei viele und sie wachsen rasant. So geht Grand View Research davon aus, dass der Markt für Edge Computing bis 2027 ein jährliches durchschnittliches Wachstum (CAGR) von 37,4% erreichen wird[7]. Die wichtigsten Märkte haben die Analysten in den Branchen Energiewirtschaft, Industrie sowie Transport und Logistik ausgemacht. Sie tragen zu knapp der Hälfte des globalen Edge-Computing-Markts bei – gefolgt von Smart Cities & Gebäudedigitalisierung, Gesundheitswesen, der Landwirtschaft und dem Retail-Sektor.

4 IT und OT konvergieren am Edge

Im Zuge der Digitalisierung all dieser Märkte konvergiert letztlich die IT mit der bestehenden OT, denn die bislang noch vielfach autonom betriebene OT wird über Edge-Logik und Proxy zur IT und u. a. weltweit erreichbar. Je nach Anforderung erfüllen diese OT-anbindenden Edge Plattformen unterschiedliche Anforderungen. In manchen wird aufwendige Edge-Analytik gefahren, um nur die relevanten Daten an zentrale Management-Clouds zu senden. Weitere Aufgaben sind beispielsweise die maschinenübergreifende Kommunikation mittels OPC-UA Gateways beziehungsweise Servern. Verstehen sich alte und neue Welt noch nicht, dann gibt es Protokollkonverter, die serielle Schnittstellen auf IP-Pakete oder veraltete Protokolle auf neueste Standards heben, um beispielsweise die Speicherung bisher nicht nutzbarer Daten zu ermöglichen.

Mit Blick auf die ‚dunkle Seite' ist es weiterhin wichtig, unsichere Technologien wie das kompromittierbare SMBv1-Protokoll auf SMBv3 zu konvertieren, um reale Bedrohungen – beispielsweise diese Schwachstellen automatisiert ausnutzende Ransomware – auszuschalten. Zum Schutz gegen bereits im Netz befindliche Angreifer oder für den Transfer über unsichere Netze ist es zudem ratsam, die Datenübertragung zu verschlüsseln. Seit Jahren im Einsatz befindliche OT-Systeme werden leider in den seltensten Fällen regelmäßig mit neuer Software bespielt, um offene Flanken zu schließen oder von sich aus modernere beziehungsweise sicherere Optionen zu ergänzen – sofern überhaupt einspielbare Updates existieren. In Folge sind sie oft noch lange nach dem eigentlichen ‚Day Zero' über eine entsprechende Schwachstelle verwundbar.

Abb. 3 | Typische Transcodier- und Verschlüsselungsaufgaben bei Windows NT/ XP/7 basierter Brownfield-OT

OT-Systeme erhalten vor allem deshalb keine Updates und Upgrades, weil sie als eine Einheit mit allen Bestandteilen funktionsvalidiert und zertifiziert wurden. Dieser Systemzustand soll möglichst konstant gehalten werden. Gelten dann auch noch höchste Verfügbarkeits- und Sicherheitsanforderungen, wird der Zustand paradoxerweise meist sogar komplett eingefroren. Bauelemente, Platinen und Fertigungsprozesse sowie BIOS, Treiber, OS-Images: Alles muss immer identisch bleiben. Sehr verständlich, wenn man an Medizingeräte denkt oder Systeme in kritischen Infrastrukturen des Schienenverkehrs- und Energiesektors. Fehler können hier Leben kosten. Letztlich will auch kein industrieller Hersteller, dass ihm der Roboter ‚um die Ohren fliegt'. Es ist für Hersteller also nicht mal so eben möglich, Updates an bereits verkauften Systemen so durchzuführen, als wären es Smartphones für die es regelmäßig neue Updates und Patches gibt und wo Softwarefehler keine Menschenleben fordern können.

Und selbst wenn der OEM kontinuierliche Updates gerne als Services bereitstellen würde: Oft fehlen Standardprozesse im Patch-Management zur Installation bei Kunden. Die Devise lautet also selbst dann oft noch: ‚Never change a running system'. Noch weniger Spielraum haben Betreiber von Maschinen und Anlagen, für deren Systeme die Hersteller keine Migrationspfade anbieten. Um die digitale Transformation des Brownfields bewerkstelligen zu können ist es daher unumgänglich, über adaptive Edge-Plattformen das notwendige Retrofit zu betreiben – zumal jeder Betreiber auch eigene Strategien bei der Digitalisierung verfolgt, die er nicht zwingend mit jedermann teilen will.

5 Herausforderungen auf vielen Ebenen

An Plattformen, die am Edge die IT mit der OT konvergieren, müssen dabei die gleichen – wenn nicht sogar noch höhere – Sicherheitsanforderungen gestellt werden wie an die vernetzte Unternehmens-IT. Hält man sich vor Augen, dass Pay-per-Use Modelle aus jeder Maschine eine Geldmaschine machen; dass automatische Checkoutsysteme Waren und Geld umschlagen; dass gelieferter Strom Geld kostet und dass selbstverständlich auch Kritische Infrastrukturen vom Energie- und Transportsektor bis hin zur Industrie enorme Summen an Werten schaffen oder absichern, dann wird es schnell verständlich, dass die Anforderungen an eine zuverlässige und sichere Anbindung der Dinge zunehmend anspruchsvoller wird. Ganzheitliche Lösungsansätze sind deshalb unerlässlich.

Abb. 4 | Wichtigste Bedrohungen der Brownfield-OT[8]

Top 10 Bedrohungen seit 2016
Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware
Infektionen mit Schadsoftware über Internet und Intranet
Menschliches Fehlverhalten und Sabotage
Kompromittierung von Extranet- und Cloud-Komponenten
Social Engineering und Phishing
D(D)oS Angriffe
Ungewollt Internet-verbundene Steuerungskomponenten
Einbruch über Fernwartungszugänge
Technisches Fehlverhalten und höhere Gewalt
Kompromittierung von Smartphones im Produktionsumfeld

7 https://www.grandviewresearch.com/press-release/global-edge-computing-market

8 Quelle: BSI-CS 5

Die Praxis sieht jedoch anderes aus. Ist der Digitalisierungsbedarf erkannt, wird im schlimmsten Fall genutzt, was gerade zur Hand ist. Für Lernzwecke, Prototypen und Demonstratoren ist eine Raspberry Pi Plattform und ein ‚normales' Linux aus dem Netz mehr als ausreichend. Doch bereits bei der Hardware besteht hier das Problem, dass sie meist nicht für den rauen Industriealltag ausgelegt ist. Dezidierte Industriehardware wird dagegen in Klimakammern getestet und über Burn-in-Tests künstlich gealtert, um höchste Verfügbarkeiten in rauen Umgebungsbedingungen bieten zu können. Ganz zu schweigen von Softwarekomponenten und der Frage nach einer passenden Härtung gegen Angriffe. Diese Maßnahmen sind – zusammen mit Anforderungen an die Langzeitverfügbarkeit – bei größeren Deployments im industriellen Feld aber unerlässlich. Meist wird jedoch erst zu professionelleren Mitteln gegriffen, wenn diese Schwachstellen bereits zum Problemfall geworden sind.

Doch selbst industrietaugliche Hardware bringt von Haus aus noch nicht alles mit, was am Edge benötigt wird. Sie hat in Form von industrietauglichen Box-PCs oft nur ein Trusted Plattform Modul (TPM) integriert, das in der Praxis auch noch ungenutzt bleibt. An die physikalischen Robustheits- und Langzeitverfügbarkeitsanforderungen der Operational Technology wird bei größeren Installationen also durchaus gedacht. Bei der Sicherheit wird aber noch allzu oft geschludert, obwohl der Hersteller diese Herausforderung kennen sollte – nicht zuletzt da er z. B. ja auch sicherstellen will, dass die bei seinen Kunden im Einsatz befindliche Software sauber lizensiert ist.

Bei OT-anbindenden Edge-Systemen wird vielfach aber die Tatsache vergessen, dass es sich hier eben nicht mehr um eine geschlossene OT-Systemlösung, sondern um ein ‚offenes' System handelt. Edge-Plattformen sind nämlich der verlängerte, robustere Arm der umfassend vernetzten Unternehmens-IT, der zum Zuge der Digitalisierung nun bis an die Geräte, Maschinen und Anlagen heranreicht. Das globale IP-Netz dringt damit also – rund 20 Jahre nach dem Beginn des Siegeszug der offenen x86 Computing Plattformen im Bereich industrieller Steuerungen – zunehmend in die Automatisierungspyramide ein und dockt direkt mit seinen adaptiven industrietauglichen Plattformen über die Systeme der Steuerungs- und Prozessebene bis in die Feldebene an.

Wenn diese Ebenen und die in ihnen zirkulierenden Daten aber so viel Geld wert sind und wir sie monetarisieren wollen, dann wirken solche Installationen wie eine offen auf den Tisch gelegte Geldbörse. Im Online-Zahlungsverkehr wissen wir um die Notwendigkeit hoher Sicherheitsmaßnahmen, wie Verschlüsselung, Zwei-Faktor-Authentisierung und eine proaktive Gefahrenerkennung und -abwehr. Vergleichbares ist auch im Edge nötig, denn kriminelle Machenschaften wie im Online-Banking kann es auch bei digitalen Twins geben – ganz zu schweigen von all den Machenschaften und allgemeinen Bedrohungen der IT. Diese sind uns in den letzten Jahren – Stichwort: Verschlüsselungstrojaner bzw. ‚Ransomware' – hinlänglich bekannt geworden.

Worauf ist also bei der Installation von Edge-Plattformen zur Anbindung der OT an die IT-Welt zu achten, damit OEM und industrielle Endanwender ihre Chancen nutzen können? Und welche Sicherheitsfunktionen muss eine Plattform am Edge bieten, damit sie zum Vertrauensanker wird, mit dem man bedenkenlos und guten Gewissens das Brownfield und die Unternehmens-IT verbinden kann?

6 Funktion und Sicherheit am Edge

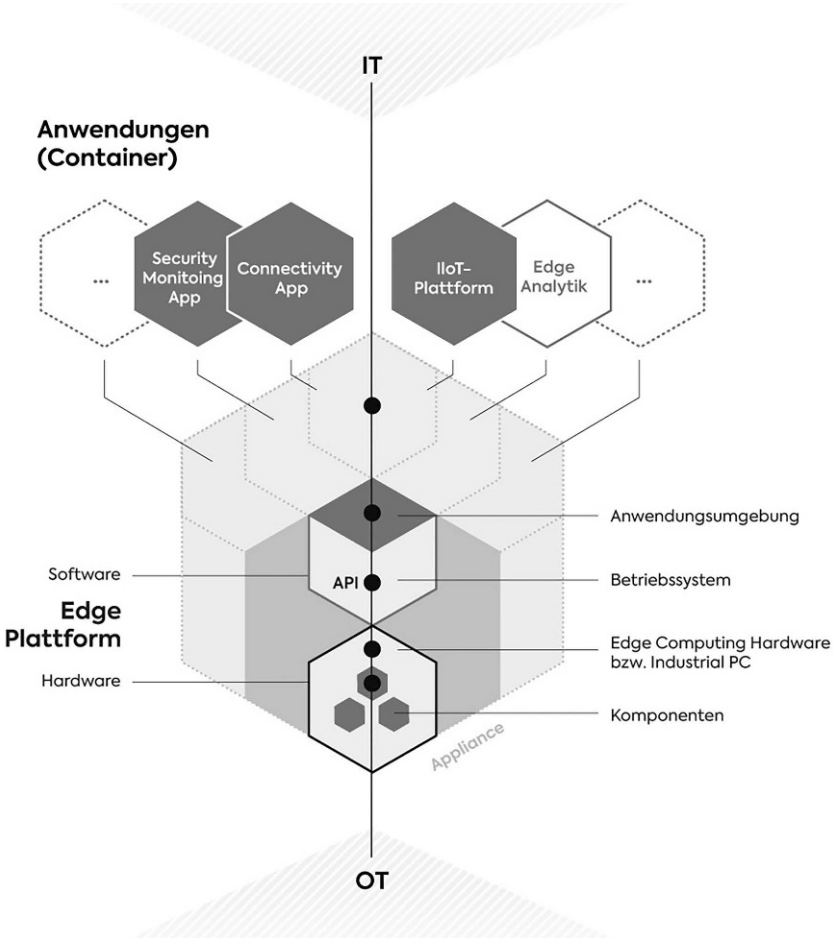
Hersteller sowie Betreiber und deren Systemintegratoren stehen vor der Herausforderung, eine effiziente, einfach anzuwendende und flexible Lösungsplattform für ihr heterogenes OT-Umfeld zu finden, die zudem alle wichtigen Sicherheitsanforderungen erfüllt. Im besten Fall soll sich der Nutzer nur noch um die Entwicklung oder Implementierung der eigentlichen Edge-Anwendungslogik kümmern müssen.

Das Prinzip einer Trusted Edge Plattform schafft es, alle erforderlichen Edge-Computing Funktionen im Rahmen der kundenspezifischen Digitalisierungsprojekte zu erfüllen, in dem sie offen und bedarfsgerecht skalierbar jede geforderte Edge-Funktionalität integrieren kann. Hierzu gehören sowohl komfortable Konfigurationsmöglichkeiten über Web-Interfaces oder eine REST API sowie Ökosysteme von eigenen und Third Party Anwendungen mit entsprechenden Support-Optionen. Gleichzeitig müssen solche Plattformen aber auch ‚off-the-shelf' alle fundamentalen Anforderungen an die IT-Sicherheit erfüllen respektive begleitende IT-Services für die Sicherheit anbieten können – beispielsweise eine kontinuierliche Sicherheitsüberwachung und ein zuverlässiges Patch-Management.

Abb. 5 | Während die Systemvielfalt im IT-Umfeld vergleichsweise übersichtlich ist, ist OT im Brownfield extrem heterogen

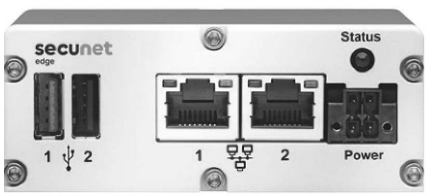
In ihrer Kernfunktion als Konnektoren zwischen der IT und OT bieten performance- und interfaceseitig bedarfsgerecht skalierbare Trusted Edge Plattformen die Basis für die eigentlichen Anwendungen. In der Regel wird dies über eine separierte – aber dennoch funktional verbundene – Containerumgebung ermöglicht. Im Idealfall existiert auch bereits ein Ökosystem von Apps – beispielsweise für die Anbindung spezifischer OT-Maschinentypen oder für die Integration von Private und Public Cloud Diensten – sodass die Aufgabenstellung der Digitalisierung im Kern schnell von der Hand gehen kann. Das Potenzial einer schnellen Entwicklung von passgenauer Ed-

Abb. 6 | Komponenten einer Trusted Edge Plattform



ge-Konnektivität steht also auch hier im Fokus. Bei Trusted Edge Plattformen soll dies jedoch auf Basis einer umfassenden und anhand dem Bedarf skalierbaren Sicherheit passieren, um dem Attribut ‚trusted' auch gerecht zu werden.

Abb. 7 | Beispielhafte Appliance einer Trusted Edge Plattform



Letztlich geht es also darum, ein robustes Geländefahrzeug, das zunächst nur mal für den Einsatz auf dem Brownfield-Acker entwickelt wurde, auch mit einer Straßenzulassung zu versehen und Sicherheitsgute, Airbags und Spurhalteassistenten zu integrieren, dabei aber den Footprint der Konnektivitäts- und Sicherheitsfunktionen so klein zu halten, dass man die Lösung auf einer industriell-robusten Plattform implementieren kann. Die Funktionalität einer solchen Plattform ist vielfältig, hat jedoch einige wichtige Kernaspekte.

6.1 Industriegerechte Firewall

Trusted Edge Plattformen sollen eine industriegerechte Firewall integrieren, welche auch die in der OT verwendeten Kommunikationsprotokolle beherrscht, da sie von herkömmlichen Firewalls oft nicht sinnvoll verarbeitet werden können. Nur so können auf industrielle Zwecke angepasste Regelwerke für White- bzw. Allow- und Black- bzw. Deny-Listen entwickelt werden, nach denen Pakete entweder durchgelassen oder verworfen werden. Über möglichst scharf eingestellte Listen lassen sich OT-Systeme wirkungsvoll vor Angriffen aus dem Netz schützen, indem sie von nicht erwünschter Kommunikation isoliert werden. Im besten Fall bietet die Plattform sogar die Möglichkeit, die bereits bestehenden, tatsächlichen Abläufe in einem Brownfield-Netzwerk zu erkennen und darauf basierend passende Regeln abzuleiten.

6.2 Härtung und Updates

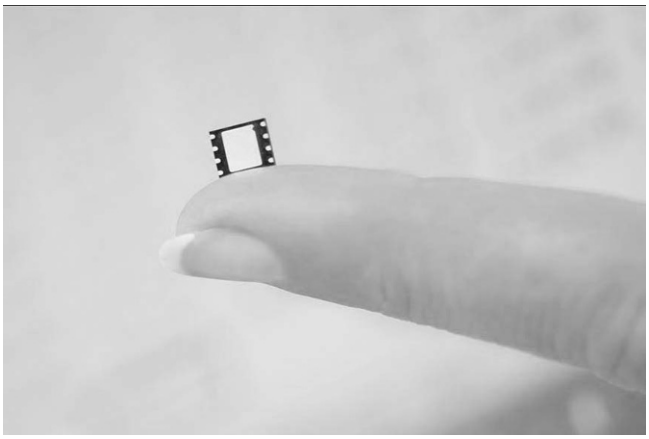
Eine Trusted Edge Plattform isoliert OT von der IT, soll aber auch selektive Kommunikation erlauben und bleibt vor allem selbst auch Teil des IT-Netzwerks. Folglich muss sie in der Lage sein, eigenständig Bedrohungen abwehren zu können. Eine entsprechende Härtung des Betriebssystems, eine Minimalisierung von Zugängen und Zugriffen und eine proaktive Systemüberwachung sollten deshalb inkludiert sein – genauso wie die Möglichkeit, Updates für die Plattform und ihre Anwendungen sicher durchzuführen – ohne dass Nebenwirkungen oder Auswirkungen auf die Verfügbarkeit der Maschinen in Kauf genommen werden müssen.

6.3 Sichere Elemente

Trusted Edge Plattformen haben im Idealfall nicht nur ein statisches TPM, sondern ein echtes Secure Element (SE) integriert, das als Vertrauensanker dient und es beispielsweise ermöglicht, Verschlüsselungsmechanismen zuverlässig auszuführen oder kryptographische Schlüssel innerhalb eines manipulationssicheren, dedizierten Chips mit eigenem Betriebssystem zu verwahren. Lösungen aus dem Hochsicherheitsbereich erfüllen dabei Standards wie FIPS 140-2 Level 3 oder BSI Common Criteria EAL 5, die nicht zu Unrecht u. a. im Finanzsektor entstanden sind und sich hervorragend auch zur Absicherung von kritischen OT-Daten und ihrem Monetarisierungspotenzial eignen.

Solche Sicherheitsfunktionen sollten auch für Third Party Anwendungen nutzbar sein, die auf der Plattform ausgeführt werden. Dadurch sind Datenverschlüsselung und Integritätsschutz – beispielsweise von Sensordaten – ebenso auf hohem Sicherheitsniveau umsetzbar wie auch die Authentifizierung von Fernzugriffen. Ebenfalls denkbar ist es, die mit der Trusted Edge Plattform verbundene Maschine mit einer digitalen Identität zu versehen und in eine Public-Key Infrastruktur (PKI) zu integrieren – was

Abb. 8 | Kleines Bauelement, großer Nutzen: Ein Secure Element bietet mehr Flexibilität als statische Trusted Platform Module



eine Vielzahl weiterer Anwendungsmöglichkeiten und Monetarisierungsoptionen schafft.

6.4 Fernwartung der OT

Trusted Edge Plattformen sollten auch Fernwartungsfunktionen für die OT bieten können. Hierzu reicht es nicht aus, dass die Plattform mit dem System verbunden ist. Oftmals sind vor Ort spezielle Apps erforderlich, da die Wartungssoftware beispielsweise unmittelbar auf die serielle Schnittstelle zugreifen muss. Entsprechend komfortabel ist es dann, wenn die Edge Plattform diese Lösung in isolierten Containern integrieren kann. Bietet das Edge-System zudem ‚Tarnkappen-Funktionen', kann die OT – abseits erwünschter Fernzugänge – im Netzwerk versteckt werden und ist somit für potenzielle Angreifer kaum aufspürbar und in der Konsequenz auch weniger angreifbar.

6.5 Mikrosegmentierung

Mitunter soll eine komplette Fertigungszelle abgesichert werden und nicht nur eine einzige Maschine. Eine multifunktionale Trusted Edge Plattform sollte deshalb auch Mikrosegmente verwalten können, indem sie eine dedizierte Zone schafft und möglichst vor äußeren Einflüssen schützt. Jede ein- und ausgehende Kommunikation mit diesen Mikrozonen wird dann separat vom Sicherheitssystem verwaltet und kann damit auch unterschiedlichen Regeln als der Rest des Netzes folgen. Datenfluss und Kommunikationsverbindungen werden somit vollständig und nach Segmenten abgestuft kontrollierbar.

6.6 Vorgefertigte Protokollübersetzer

Zum Schutz der Maschinen gehört auch der geeignete Umgang mit Protokollen, die mittlerweile als unsicher eingestuft werden. Die langen Laufzeiten von Maschinen bringen es mit sich, dass deren Datenkommunikation oft auf alten Protokollstandards basiert. Ein Nachrüsten geeigneter Maßnahmen ist schwierig, gerade wenn Daten noch über veraltete Schnittstellenstandards übertragen werden müssen. Wenn Maschinen im Netzwerk über unsichere Protokolle kommunizieren, kann weder auf die Vertraulichkeit noch auf die Integrität der zu übertragenden Daten vertraut werden. Infolgedessen besteht ein Risiko, dass der Netzwerkverkehr durch Dritte mitgelesen oder manipuliert wird.

Eine Protokollübersetzung von einem unsicheren in ein sicheres Protokoll verhindert eine solche ungesicherte Übertragung von Daten im Netzwerk und reduziert das Risiko auf die minimale Strecke zwischen der Trusted Edge Plattform und der damit verbundenen Maschine. Dazu werden die von einer vernetzten Maschine an das Sicherheitssystem gesendeten Daten – idealerweise ‚on the fly' und damit ohne Performance-Einbußen – übersetzt sowie unter Verwendung eines sicheren Protokolls weitergeleitet – z. B. von File Transfer Protocol (FTP) zu Secure File Transfer Protocol (SFTP) oder File Transfer Protocol über SSL (FTPS).

6.7 Permanente Überwachung

Da eine umfassende Prävention nie möglich ist, muss eine Trusted Edge Plattform auch überwachen können. Das beginnt bereits bei der Identifizierung aller Kommunikationspartner bzw. Assets in einem Netzwerk sowie der allgemeinen Analyse ihres IT-Sicherheitszustands. Dies ist vor allem wichtig, weil die zunehmende Vernetzung auch die übertragenen Datenmengen und deren Komplexität erhöht – bei gleichzeitiger Reduzierung der Transparenz der Kommunikationsflüsse. Eine vorherige Absicherung wird dadurch immer schwieriger und muss durch ein nachgelagertes Monitoring mindestens ergänzt werden.

Lokal auf den Trusted Edge Plattformen installierte Monitoring-Systeme sammeln hierzu Daten aus dem Netzwerkverkehr, analysieren diese und stellen sie in Form von Zustandsberichten dar. Anhand von vordefinierten Schwellenwerten und Regeln können diese Systeme frühzeitig auf mögliche Probleme oder Bedrohungen hinweisen. Die festgestellten Probleme werden dann in Form von Warnungen angezeigt und erfordern eine manuelle Überprüfung und gegebenenfalls das Einleiten weiterer Maßnahmen. Im Idealfall können die Maßnahmen direkt wieder über die Plattform ergriffen werden – z. B. die Isolation eines auffälligen Systems über die Firewall.

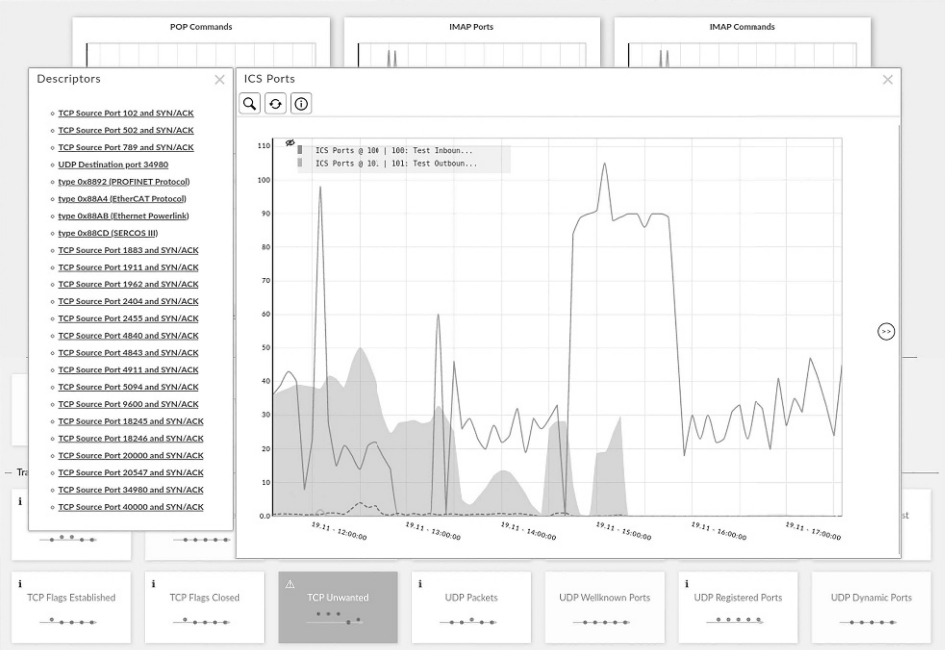
6.8 Anomalieerkennung

Lokal installierte Monitoring-Systeme zur Kontrolle und Überwachung des Datenflusses basieren meist auf relativ starren, vor-

Abb. 9 | Regelbasierte Erkennung von automatisiert generierten Domainnamen, wie sie durch Angreifer eingesetzt werden

```
Standard query response 0x83f4 A fqsdyirlwpk.ws A 38.102.150.27 A 104.244.14.252
Standard query response 0xe4b9 A ginxzzyfeqv.cn A 157.122.62.194
Standard query response 0x4722 A hfimsktquo.cn A 157.122.62.194
Standard query response 0x2e6d A hlpambj.ws A 38.102.150.27 A 104.244.14.252
Standard query 0x2ef3 A crwyxnoqjv.ws
Standard query 0x726f A avilfizb.ws
Standard query 0x6018 A hnhjh.ws
Standard query response 0xc2b4 A jjuelowzz.cn A 157.122.62.194
Standard query response 0x2ef3 A crwyxnoqjv.ws A 38.102.150.27 A 104.244.14.252
Standard query response 0x726f A ayllfjzb.ws A 104.244.14.252 A 38.102.150.27
Standard query response 0x6018 A hnhjh.ws A 38.102.150.27 A 104.244.14.252
Standard query 0xc3f6 A zhtthraz.ws Standard query 0x9f73 A loksmepbq.ws
Standard query response 0xc3f6 A zhtthraz.ws A 38.102.150.27 A 104.244.14.252
Standard query response 0x9f73 A loksmepbq.ws A 104.244.14.252 A 38.102.150.27
Standard query 0xc234 A jycelukrlp.ws
Standard query 0xc33c A ydqxko.ws
Standard query response 0xc33c A ydqxko.ws A 38.102.150.27 A 104.244.14.252
Standard query response 0xc234 A jvcelukrIp.ws A 104.244.14.252 A 38.102.150.27
Standard query 0x81c6 A kgzvnwcnsgt.ws
Standard query response 0x81c6 A kozvnwcnsgt.ws A 38.102.150.27 A 104.244.14.252
```

Abb. 10 | Anomalieerkennung, die auf Netzwerkverkehrsmetriken zurückgreift



definierten Regeln, die auf Basis realer Ereignisse regelmäßig überprüft und angepasst werden müssen. IT-Sicherheitsexpertise zählt jedoch häufig nicht zur Kernkompetenz der Hersteller oder der Betreiber von Maschinen und Anlagen. Zudem ist die Pflege der Regelwerke und Interpretation einzelner Alarme zeitintensiv und bei fehlendem Know-how fehleranfällig. Aus diesem Grund sollte das Prinzip der Trusted Edge Plattformen auch eine automatisierte Erkennung von Anomalien enthalten.

Anomalien sind z. B. Abweichungen von einem Normalzustand oder -verhalten. Um Anomalien zu erkennen, muss dieser Zustand – beispielsweise eines Produktionsnetzwerks, eines Mikrosegments oder einer einzelnen Maschine – erst über eine Lernphase erhoben werden. Auf dieser Basis kann in der Folge anormales Verhalten – also das erstmalige Vorkommen von abweichenden Ereignissen – automatisch erkannt werden. Die kombinierte Verwendung der Funktionen ‚Abschirmung', ‚Segmentierung', ‚Monitoring' und ‚Anomalieerkennung' gepaart mit einem optionalen Sicherheits-Retrofit für unsichere Brownfield-Systeme schafft schlussendlich die nötige präventive und detektive Sicherheit in IIoT- und Industrie 4.0-Netzwerken. Aus architektonischer Sicht lassen sich all diese Funktionen gut mit Trusted Edge Plattformen als einzelne aber miteinander integrierte Anwendungen realisieren. Aufgrund der Positionierung eines solchen Sicherheitssystems als Koppelelement kann dieses insbesondere den ein- und ausgehenden Datenfluss zur bzw. von der Maschine oder Fertigungszelle kontinuierlich erfassen.

7 Fazit

Wer seine Brownfields digitalisieren will oder Expeditionen in der neuen Welt der Digitalisierung beginnt, der braucht am Edge eine zum Digitalisierungsbedarf passende Aufstellung. Diese muss sicher integriert werden, da zunehmende Konnektivität immer auch steigende Sicherheitsanforderungen mit sich bringt. Aus diesem Grund werden umfassend gehärtete Trusted Edge Plattformen, die zudem auch kontinuierlich aktualisiert und effizient kuratiert werden müssen, unverzichtbar – auch mit Blick in Richtung Feldebene. Ist dies alles auch umfassend zertifiziert und kommt aus einem vertrauenswürdigen Herkunftsland wie Deutschland, hat man nach dem heutigen Stand der Technik das Wichtigste getan, was man für die zuverlässige und sichere Anbindung im industriellen Umfeld tun kann. Ein solcher Lösungsansatz eignet sich sogar für den Einsatz in den Kritischen Infrastrukturen nach Definition des Bundesamts für Sicherheit in der Informationstechnik (BSI). Interessanterweise sind viele der dort behandelten Themen deckungsgleich mit den Themen in den größten Wachstumsmärkten des Edge Computings.

Abb. 11 | Sektoren und Branchen Kritischer Infrastrukturen[9]

Literatur

[1] Torsten Redlich: Whitepaper – Trusted Platform at the Edge (2020)
[2] secunet: Factbook secunet edge – Gesamtlösung (2020)

9 https://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/Sektoren/sektoren_node.html