Datensicherheit von Produktionsanlagen

Prof. Dr. Axel Zimmermann

Zusammenfassung

Die fortschreitende Digitalisierung der industriellen Produktion wirft die Frage auf, wie eine weitgehend vernetzte Fabriklandschaft vor unbefugtem Zugriff, Spionage oder Sabotage geschützt werden kann. Eine Reihe von Vorkommnissen hat gezeigt, dass selbst gut geschützte Anlagen nicht vor Angriffen sicher sind. Derzeit sind mehrere hundert ernst zu nehmende Angriffe von Cyber-Kriminellen auf Fabriken und Infrastruktur pro Jahr festzustellen, mit stark wachsender Tendenz.

Produktionsanlagen sind besonders anfällig gegenüber Angriffen aus dem Internet, da sie häufig sehr kleine und wenig leistungsfähige Computer einsetzen. Oft läuft darauf auch noch ein veraltetes Betriebssystem und keine Anti-Virus Software. Eine großflächige Vernetzung solcher Anlagen ohne weitergehende Schutzmaßnahmen stellt damit ein Sicherheitsrisiko dar.

Gerade in Deutschland wird die Sicherheit der Daten im Produktionsumfeld als wesentlicher Hinderungsgrund für die zügige Einführung von Industrie 4.0 Methoden in kleinen und mittleren Unternehmen angesehen. Ein wichtiger Baustein zur erfolgreichen Umsetzung ist die fundierte Information über Chancen und Risiken, die ein solcher Wandel mit sich bringt.

1. Der Sicherheitsbegriff in der Industrie

Jede große industrielle Entwicklung hat das Thema Sicherheit massiv beeinflusst. Ende des 18. Jahrhunderts im Zeitalter der ersten industriellen Revolution war es vor allem der Konflikt zwischen Arbeit und Kapital, der die Sicherheit der Arbeitsplätze und im Gegenzug die Sicherheit der Produktionsanlagen in aufkommenden Fabriken gefährdete (Mirow, 1996). Die zweite industrielle Revolution brachte es mit sich, dass Menschen im Takt von Maschinen arbeiten mussten und damit die Sicherheit am Arbeitsplatz relevant wurde (Hahn, 2005). Der Einsatz von Robotern und anderen Automatisierungssystemen verlagerte im Zuge der dritten industriellen Revolution gefährliche Arbeiten weg von den Menschen, brachte jedoch neue Gefahren durch eine direkte Zusammenarbeit mit Maschinen. Der Begriff „Safety“ für die funktionale Sicherheit von technischen Anlagen wurde geboren. Die vierte industrielle Revolution geht noch einen Schritt weiter (Hillenbrandt, 2012). Die massive Digitalisierung von Produktionsprozessen fügt eine Datenschicht zwischen Mensch und Maschine, die eine direkte Interaktionen in den Hintergrund treten lässt. Daten sind Überträger von Steuerbefehlen und Messwerten und die Verarbeitung erfolgt in der Internet-Cloud. Sicherheit betrifft jetzt vor allem die Daten und der Begriff „Security“ fasst dies zusammen. Dabei geht es im Wesentlichen um drei Bereiche der Datensicherheit. Authentische Daten gewährleisten, dass der Urheber der Daten bekannt ist. Unverfälschte Daten stellen sicher, dass keine Manipulationen von Anlagen erfolgen. Und schließlich muss auch der Transportweg für Daten gegen Diebstahl abgesichert sein (Eckert, 2012).

Obwohl die Datensicherheit als zentraler Bestandteil der Digitalisierung angesehen wird, steigt die Zahl der bekannt gewordenen sicherheitsrelevanten Vorfälle. 2010 zerstöre „Stuxnet“ Zentrifugen in iranischen Atomanlagen, 2012 legt „Shamoon“ 30.000 Computer in saudischen Raffinerien lahm, 2013, infizierte „Havex“ flächendeckend SCADA Systeme in Kontrolleinrichtungen und seit 2015 ist eine massenhafte Ausbreitung von sogenannten Erpressungs-Trojaner im Umlauf, die zum Teil sensible Daten verschlüsseln und nur gegen Zahlung von Lösegeld wieder frei geben. Die Zahl solcher Sicherheitsvorfälle in Deutschland stieg von 2014 auf 2015 um etwa 30% und im Jahr 2015 summierte sich nach einer Schätzung des BSI der wirtschaftliche Schaden angerichtet durch Wirtschaftsspionage, Datendiebstahl, Sabotage und Erpressung auf ca. 51Mrd EUR. Etwa 61% der KMUs sollen bereits Opfer von Angriffen geworden sein, doch nur 30% verfügen dem nach über ein eigenes Sicherheitskonzept und sogar nur 11% wollen an dieser Situation etwas verbessern (BSI, 2014).

Das Zentrum Industrie 4.0 der Hochschule Aalen setzt genau an dieser Stelle an. Es hat die Aufgabe Kenntnisse, Erfahrungen und Angebote aus der Hochschule nach außen zu bündeln und sichtbar zu machen und neue Kooperationen mit den Unternehmen der Region zu ermöglichen. Mit Information, Beratung und anwendungsbezogener Forschung soll die Wahrnehmung der Datensicherheit als zentraler Aspekt einer Digitalisierungsstrategie unterstützt werden.

2. Angriffe auf Industrieanlagen

Ein Sicherheitskonzept kann nur erfolgreich entwickelt werden, wenn das Gefährdungspotential im eigenen Unternehmen abgeschätzt werden kann.

Eine typische Unternehmensstruktur aus Datensicht ist in Bild 1 dargestellt und besteht aus einer Unternehmensebene, der Leitebene, der Steuerungsebene und schließlich der Feldebene. In der Regel ist nur die Büro-IT direkt mit dem Internet verbunden und über eine Firewall abgesichert. Die

dahinter liegenden Datenbanken der Leitebene sind oft durch eine weitere Firewall getrennt davon. Die Verbindung zur Steuerungsebene ist oft nur über Gateways möglich und dies trifft in noch größerem Maße auch auf die Feldebene zu. Ein solches Netzwerk scheint gut gesichert zu sein, insbesondere wenn es zur Feldebene in manchen Fällen nicht einmal eine direkte Datenverbindung gibt.

In den meisten Fällen erfolgen Angriffe auf Unternehmensnetzwerke über die Büro-IT. Fortgeschrittenes „Social Engineering“ schafft vertrauensvollen Kontakt zu Mitarbeitern mit dem Ziel, dass Email-Anhänge geöffnet und damit Schadprogramme installiert werden können. Eine Firewall kann dies nicht verhindern, da die Aktionen aus dem internen Netzwerk kommen. Sobald ein Büro-Computer infiziert ist, kann er weitere Aktionen auslösen und insbesondere dem Angreifer helfen, den Zugang zu Steuerungs- und Feldebene zu untersuchen. Weitere Schadsoftware wird nachgeladen und kann dann direkt auf den Anlagen eingesetzt werden.

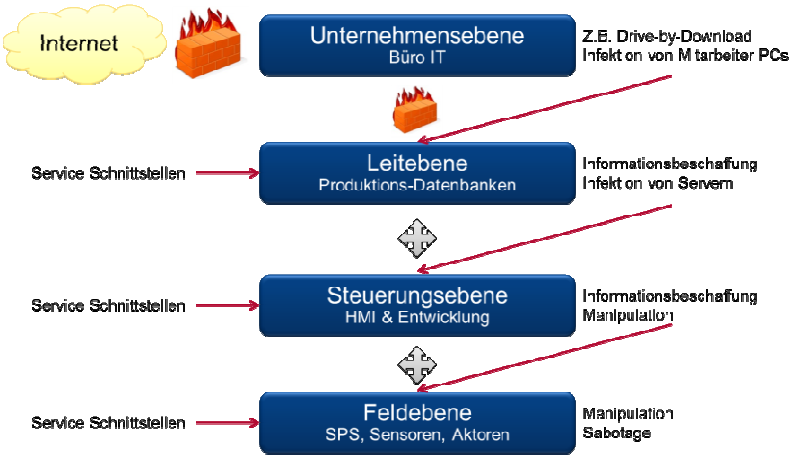

Bild1: Angriffsverlauf in einem Unternehmen aus Datensicht

Service Schnittstellen auf allen Ebenen bieten weitere Einfallstore. Insbesondere ist ein USB Anschluss für Service Computer oft die Ursache für einen Sicherheitsvorfall. Mit Malware infizierte USB-Sticks lassen sich zielgerichtet und mit hoher Erfolgsquote einsetzen. Das ist auch das Ergebnis einer Studie der Universitäten Illinois und Michigan zusammen mit Google. Auf dem Campus-Gelände der Universität Illinois lagen 297 USB-Sticks als Köder aus. 48 Prozent der Finder eines USB-Stick nahmen diesen mit, steckten ihn in einen Computer und öffneten Dateien (Tischer, 2015).

Eine Studie des TÜV-Süd untersuchte das Bedrohungspotential auf kritische Infrastrukturen mit Hilfe eines simulierten Pumpspeicherkraftwerks, das als sogenannter Honeypot an das Internet angeschlossen wurde. Die Anlage erscheint dabei nach außen hin als reales Kraftwerk und überwacht den Datenverkehr zum Internet. Es zeigte sich, dass innerhalb von 8 Monaten ca. 60.000 Zugriffe auf die Anlage erfolgten, die nicht nur über Standardprotokolle der Büro-IT, sondern auch über Industrieprotokolle wie Modbus TCP oder S7Comm erfolgten. Damit ist offensichtlich, dass eventuelle Lücken in der Sicherheitsarchitektur von Steuerungsanlagen entdeckt werden könnten und dass solche Systeme für einen möglichen Angriff anfällig sind (TÜV, 2015).

Es erscheint vor diesem Hintergrund als unrealistisch, industrielle Anlagen mit vertretbarem Aufwand gegen Angriffe von außen weitgehend absichern zu wollen. Die Strategie sollte daher sein, mit Eindringlingen zu rechnen und diese möglichst schnell zu erkennen um Schaden abwenden zu können. Intrusion Detection Systeme bieten hier das geeignete Instrumentarium.

3. Intrusion Detection Systeme

Netzwerk basierte Intrusion Detection Systeme (IDS) sitzen hinter der Firewall und gehen ihrer Arbeit unsichtbar für alle Teilnehmer im internen Netzwerk nach. Auch ein Angreifer hat keine Möglichkeit ein IDS zu erkennen. Es besitzt keine Netzwerkadresse und kann daher nicht direkt angesprochen werden. Seine Aufgabe ist es, jedes Datenpaket unverändert durchzuleiten, dabei aber nach bestimmten Regeln auf eventuelles Gefährdungspotential hin zu untersuchen. Noch weiter geht ein Intrusion Prevention System, das auch aktiv in den Datenverkehr eingreifen und gefährliche Pakete verwerfen kann.

Die Zeit, die ein Paket zum Durchlaufen des IDS benötigt, wird zur Analyse der Paketdaten verwendet. Dabei wird nach Anhaltspunkten gesucht, ob das Paket zum ganz normalen Datenverkehr gehört, oder eventuell von einem Angreifer initiiert wurde. Falls ein Angriff vorliegt, muss ein Alarmsignal generiert werden, oder im Falle des IPS wird das Paket verändert oder ganz blockiert.

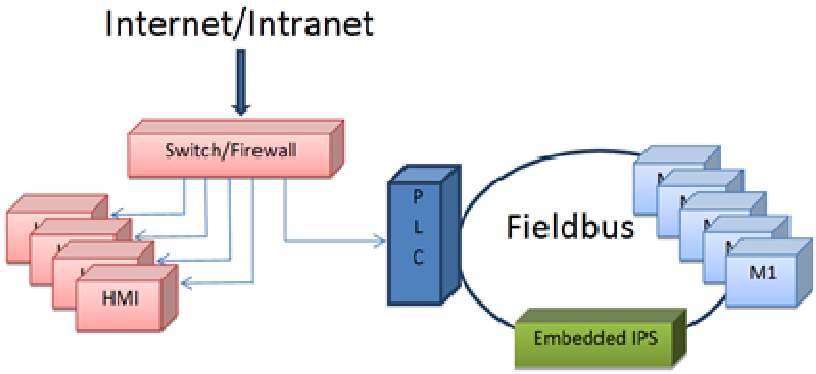

Bild 2: Informations- und Kommunikations Netzwerk Architektur im industriellen Umfeld

Es gibt eine ganze Reihe von verschiedenen Gründen, warum ein Angreifer in ein Netzwerk eindringen will. Im einfachsten Fall will er nur Lauschen, d.h. Datenpakete abfangen um diese unabhängig vom Datenverkehr weiter zu verarbeiten und möglicherweise sensible Daten zu stehlen. Oft wird aber passiv mitgehört, um darauf folgende Angriffe vorzubereiten. Die gewonnenen Erkenntnisse können dann dazu eingesetzt, aktiv am Netzverkehr teilzunehmen und dessen Aufbau sowie die Funktionsweise voll zu verstehen. Z.B. könnte durch den Lauschangriff ein Gerät ausgemacht werden, das für die Kontrolle einer bestimmten Ressource zuständig ist. Der Angreifer testet dann verschiedene Zugangsmöglichkeiten, um die Kontrolle über das Gerät und damit die Ressourcen zu gewinnen.

Eine andere Möglichkeit ist, das Netzwerk durch sinnlose Anfragen zu überlasten und damit die Bandbreite für den eigentlichen Netzbetrieb zu reduzieren. Das kann auch effektiv betrieben werden, wenn Geräte im Netzwerk erkannt werden, für die es Informationen zu Softwarefehlern gibt. Diese lassen sich dann ausnutzen, um Geräte vollständig lahm zu legen. Schließlich gibt es auch eine Reihe von Zugangsdaten, die im Netzwerk an verschiedenen Stellen abgespeichert sind. Ein Angreifer kann sich nach erfolgter Inspektion daran machen, Passwörtern und Schlüssel zu stehlen bzw. zu aufzulösen um dann selbst weiter aktiv zu werden.

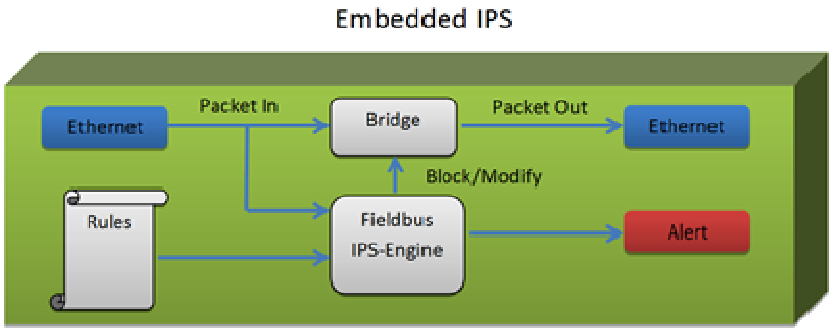

Bild 3: Überblick eines Intrusion Detection Systems für industrielle Anwendungen

Für die Vielzahl möglicher Angriffsvektoren existieren grundsätzlich zwei Techniken zu deren Erkennung: die regelbasierte Analyse und die Erkennung von Anomalien im Datenverkehr.

Ein auf Regeln aufgebautes Analysesystem arbeitet vergleichbar zu einem Antivirusprogramm. Es greift auf eine Sammlung von Informationen zu Angriffen aus der Vergangenheit zurück und sucht nach den spezifischen Merkmalen, die ein Angriff dabei hinterlassen hat. Das sind meist Signaturen im Datenpaket, also Muster von zusammenhängende oder lose verknüpfte Bytes. Es können auch bestimmte Adressen oder Kommunikationsports sein, die dabei benutzt werden. Manchmal kann man einen Angriff auch erst erkennen, wenn das Muster über mehrere Pakete hinweg verfolgt wird. Ein Angriff läuft dabei über verschiedene Phasen, die für sich genommen unauffällig und regelkonform sein können.

Ein einfaches Beispiel ist der sogenannte Syn-Flood Angriff, der sich den normalen Aufbau einer Kommunikation über das Transport Control Protokoll (TCP) zu Nutze macht. Bild 4 veranschaulicht das.

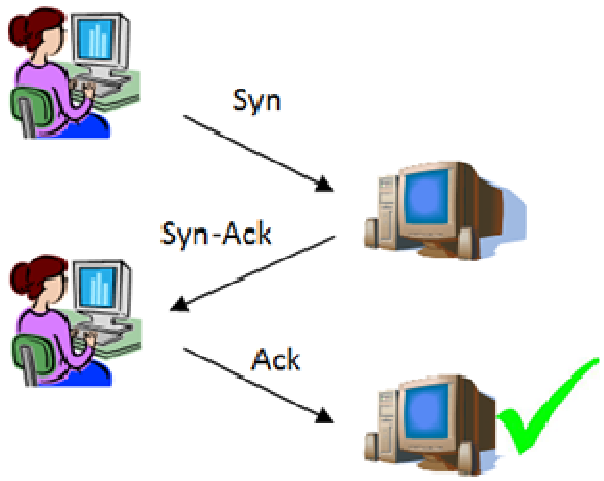

Bild 4: 3-Wege Handshake beim TCP Protokoll

Aus Gründen der Sicherheit verwendet TCP einen sogenannten 3-Wege Handshake, um eine Verbindung zwischen zwei Teilnehmern im Netz aufzubauen. Ein Teilnehmer signalisiert dabei einem

anderen Gerät mit dem speziellen SYN Paket, dass er mit ihm sprechen möchte. Das Gerät registriert den Wunsch und merkt sich die Adresse des Teilnehmers sowie den Port, über den dieser erreichbar ist. Dann sendet es zum Teilnehmer ein SYN-ACK Paket, zum Zeichen dass es bereit für die Verbindung ist. Auch der Teilnehmer speichert sich jetzt die Verbindungsdaten und bestätigt den Empfang des SYN-ACK Paketes mit einem abschließenden ACK Paket. Damit ist die Verbindung auf beiden Seiten aufgebaut und es können Daten ausgetauscht werden.

Ein Syn-Flood Angriff nutzt das TCP Protokoll dahingehend aus, dass in schneller Abfolge und großer Zahl Verbindungswünsche per SYN Paket an eine Gegenstelle gesendet werden. Die vom diesem Gerät gesendeten SYN-ACK Pakete werden dagegen ignoriert, d.h. es werden keine ACK Pakete zurückgeschickt. Die Folge ist, dass das Gerät eine Vielzahl von offenen Verbindungsdaten bereithalten muss und damit irgendwann an die Grenze kommt, also keinen Platz mehr für weitere Verbindungsanfragen mehr bereitstellen kann. Will jetzt ein anderer Netzwerkteilnehmer Kontakt zu dem Gerät aufnehmen, dann bekommt es keine Antwort mehr. Das Gerät ist damit faktisch ausgeschaltet. Bild 5 veranschaulicht den Angriff.

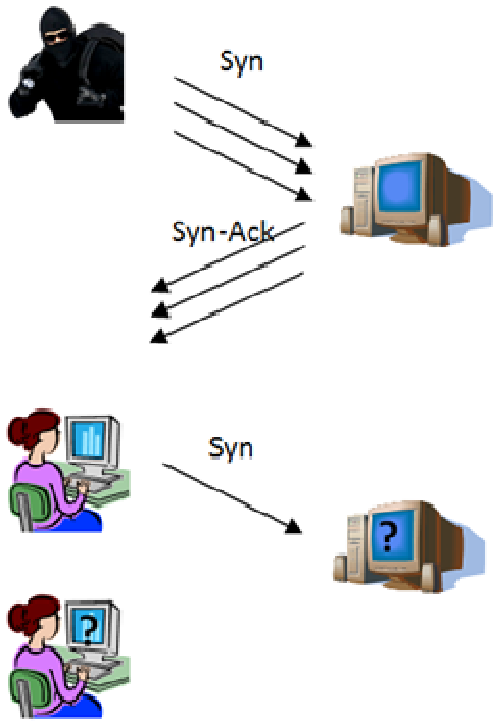

Bild 5: Syn-Flood Angriff auf einen Netzwerk Server

Einen Syn-Flood Angriff in einem regelbasierten Intrusion Detection System zu erkennen ist noch relativ einfach. Das IDS überwacht dazu den Status der Verbindungen in einem Netzwerk und meldet sich, wenn zu viele offene Verbindungen existieren.

Für fast alle bekannten Angriffsszenarien lassen sich Regeln finden, die eine Erkennung sehr zuverlässig ermöglichen. Das Problem ist, dass es zum einen sehr viele verschiedene Angriffe gibt und damit der Aufbau einer Datenbank mit deren Merkmalen sowie die Erstellung der erforderlichen Regeln zur Erkennung einen erheblichen Aufwand erfordern. Auf der anderen Seite kann man natürlich nicht voraussetzen, dass alle Angriffe bereits irgendwo einmal geschehen sind. Für Industrielle Netzwerke gibt es im Gegenteil fast kein Wissen über vergangene Angriffe, weil das

Thema einfach zu neu ist. Man kann sich also nicht nur auf regelbasierte IDS verlassen und greift daher auf Anomalie Erkennung.

Ein Anomalie-basiertes IDS überwacht Parameter, die den Zustand eines Netzwerkes und den Datenverkehr als normal oder nicht normal klassifizieren. Werden entsprechende Parameter entdeckt und eine Auslösebedingung erfüllt, dann schlägt das IDS Alarm.

Parameter können zum Beispiel sein, wieviel Pakete zwischen den einzelnen Teilnehmern pro Zeiteinheit ausgetauscht werden, wie lang diese sind, wie schnell sie aufeinander folgen und welche Richtung dabei gilt. Komplexere Modelle berechnen Wahrscheinlichkeiten, mit denen ein Netz von einem Zustand in einen anderen übergehen wird und erkennen Abweichungen von diesen Wahrscheinlichkeiten als potentiellen Angriff.

Ein Anomalie-basiertes IDS kann nur funktionieren, wenn es den normalen Zustand, die normalen Parameter bzw. die normalen Übergangswahrscheinlichkeiten kennt. Diese Parameter sind für nahezu jedes Netzwerk unterschiedlich und daher muss ein IDS immer erst auf das Zielnetzwerk trainiert werden. Danach kann es prinzipiell jede Abweichung von der Norm erkennen und damit auch Angriffe, die bisher völlig unbekannt sind.

Der Nachteil dabei ist, dass es in einem Netzwerk immer zu Abweichungen von einer Norm kommen kann. Sei es, dass ein neues Gerät integriert wird, oder dass ein Benutzer neue Nutzungsmöglichkeiten einführt. Die Norm ist also mit einer gewissen Unschärfe versehen. D.h. eine hohe Erkennungsrate für Abweichungen führt zu einer guten Erkennung von Angriffen, aber auch zu einer großen Zahl von nur scheinbaren Angriffen, die in Wirklichkeit unbedenklich sind. Will man diese sogenannte Falsch-Positiv Rate senken und macht dazu die Erkennung unschärfer, dann sinkt auch die Rate für die erkannten richtigen Angriffe auf das Netz. Ein Dilemma, das sich z.B. mit der Kombination aus einem Anomalie-basierten IDS und einem regelbasierten IDS deutlich abmildern lässt. In letzter Zeit werden auch vermehrt Neuronale Netze dazu eingesetzt, den Datenverkehr in einem Netzwerk zu überwachen. Neuronale Netzte sind sehr gut geeignet, aus dem Verhalten eines Netzwerks auf ein neues Verhalten in bisher unbekannten Zusammenhängen zu schließen. Diese Generalisierungsfähigkeit macht man sich beim Einsatz als IDS Kern zu Nutze. Grundsätzlich ist aber auch hier eine Kombination von regelbasiertem Ansatz mit einem Neuronalen Netz zielführend.

4. Spezielle Anforderungen der industriellen Daten Kommunikation

Intrusion Detection Systeme sind schon seit vielen Jahren auf dem Markt und sie werden nach wie vor häufig vor allem in Rechenzentren eingesetzt. Selbst im IT Bereich ist die Firewall alleine nicht ausreichend, um ein Netzwerk vor unerwünschten Eindringlingen zu schützen. Neben den kommerziellen Systemen gibt es OpenSource Systeme wie SNORT, die recht gut an die jeweiligen Anforderungen anpassbar sind. Allerding nur solange, wie man einen leistungsfähigen Rechner als Plattform zur Verfügung hat. Systeme für die Industrie sind bisher noch praktisch unbekannt.

Die wichtigsten Anforderungen sind hier:

- Ein Intrusion Detection System muss neben den Internet Protokollen wie TCP/UDP/ICMP auch Protokolle wie EtherCat, Profinet, CAN, FlexRay und AVB verstehen können

- Neben regelbasierten IDS sind auch Anomalie basierte IDS wünschenswert, da sehr wenig Historie zu bekannten Angriffen vorhanden ist

- Die Embedded Rahmenbedingungen wie geringe Größe, geringe Kosten und geringer Stromverbrauch sind einzuhalten

Diese Anforderungen sind mit normalen Embedded Microcontrollern nicht gleichzeitig realisierbar. Sie erfüllen zwar die Rahmenbedingungen, haben aber viel zu wenig Rechenleistung um ein IDS aufzubauen. Eine Applikationscontroller Plattform mit leistungsfähiger CPU wäre dazu in der Lage, ist aber nicht flexibel genug um auf die wechselnden Anforderungen vor allem bezüglich spezieller Schnittstellen einzugehen. Außerdem sprengt ein solcher Ansatz leicht die Embedded Rahmenbedingungen. Notwendig ist eine Controller Architektur, die sowohl flexible Interfaces als auch hohe und vor allem skalierbare Performance aufweist. Derzeit ist das z.B. mit der XCORE Architektur von XMOS machbar (May, 2009)

Bild 6: MicroIDS

XMOS bezeichnet seine xCORE Multicore Bausteine als neue Klasse von Microcontrollern. Insbesondere deshalb, weil sie mehrere unabhängige Controller Kerne auf einem Baustein bereitstellen, deren Arbeit zeitlich exakt vorhersehbar ist und die auf sehr flexible I/Os zugreifen können.

Der Unterschied zu anderen Multicore Controller Bausteinen auf ARM oder x86 Basis ist die Technik, in der die Controller Kerne aufgebaut sind. Diese sind nämlich nicht physikalisch vorhanden sondern vielmehr logisch existent und bilden zusammen mit der Ablaufsteuerung ein in Hardware gegossenes Echtzeit-Betriebssystem. Die Verteilung der Tasks auf die parallel arbeitenden virtuellen Prozessoren ist in der Software einfach zu steuern und wir auf Wunsch auch vom Tool visualisiert. Eine typische Taskverteilung in einem System mit zwei Ethernet Ports ist in Bild 7 dargestellt.

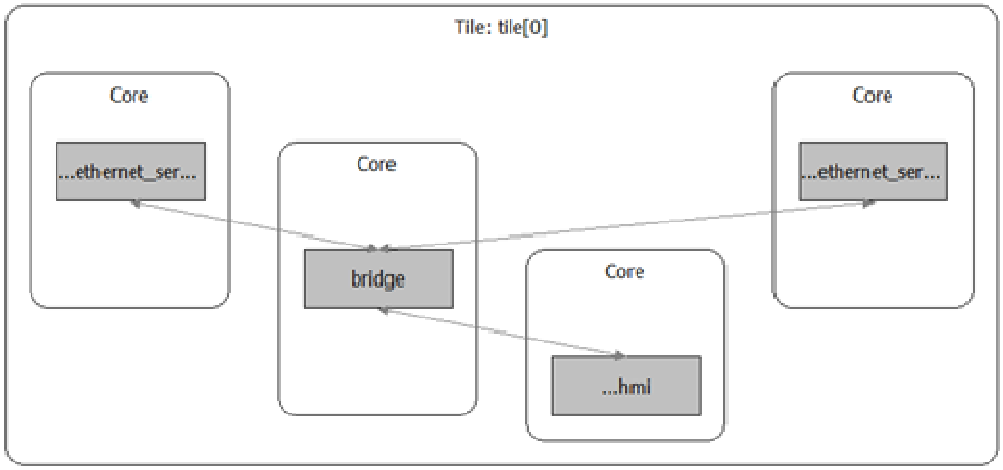

Bild 7: Task Verteilung auf 4 virtuelle Cores der xCORE Bausteine

Der große Vorteil einer solchen Architektur ist zum einen der sehr geringe Verbrauch von kostbarem Silizium und zum anderen ein bisher nicht da gewesener Freiheitsgrad bei der Programmierung von parallelen Prozessen. Die genaue Anzahl der eingesetzten Prozessorkerne lässt sich flexibel steuern, ohne dass nicht genutzte Kerne Platz und Leistung verschwenden würden. Natürlich gibt es in der Realität doch ein paar Einschränkungen, aber trotzdem ist diese Architektur sehr Ressourcen und damit Kosten sparend. Ein idealer Prozessor für Embedded Applikationen also.

Eine weitere Besonderheit versteckt sich in den GPIOs, den flexiblen Ein- und Ausgängen. Diese sind nicht einfach nur Pins, die auf bestimmte Signalpegel geschaltet werden können bzw. ein externes Signal in einem Register für die CPU zugänglich machen. Die xCORE GPIOs können sowohl kombinatorisch als auch taktgesteuert verwendet werden und beinhalten Schieberegister zum einfachen serialisieren und deserialisieren von Datenströmen. Als Eingang geschaltet können sie sogenannte Events auslösen, die direkt auf die Programmsteuerung einwirken. Im Unterschied zu anderen Microcontrollern gibt es zumindest in der Basis Familie praktisch keine Standardschnittstellen auf dem Baustein. UART, I2C, Ethernet oder sonstige Interfaces werden dagegen je nach Bedarf als vorgefertigte Software-Module implementiert. Die schnellen und flexiblen I/Os machen es möglich, nahezu beliebige Schnittstellen aufzubauen und die Ansteuerung entsprechend der Schnittstellen Protokolle übernimmt die Software.

Die xCORE Architektur ähnelt damit eher einem FPGA (Field Programmable Gate Array) nur mit dem entscheidenden Vorteil, dass die Hardware statt in VHDL oder Verilog in ganz normalem C programmiert werden kann. Ein xCORE Baustein kostet auch nur ein Bruchteil eines vergleichbaren FPGAs und verbraucht viel weniger Leistung.

XMOS Prozessoren eigenen sich sehr gut zur Implementation von Intrusion Detection Systemen. Die grundlegende Herausforderung bei einem solchen System ist die große Menge an Daten und die zeitlich kritische Abarbeitung von vielen unabhängigen Operationen auf einem Datenpaket. Die XMOS Architektur ermöglicht die Parallelisierung dieser Operationen ohne dabei die Gesamtverarbeitungszeit wesentlich zu erhöhen.

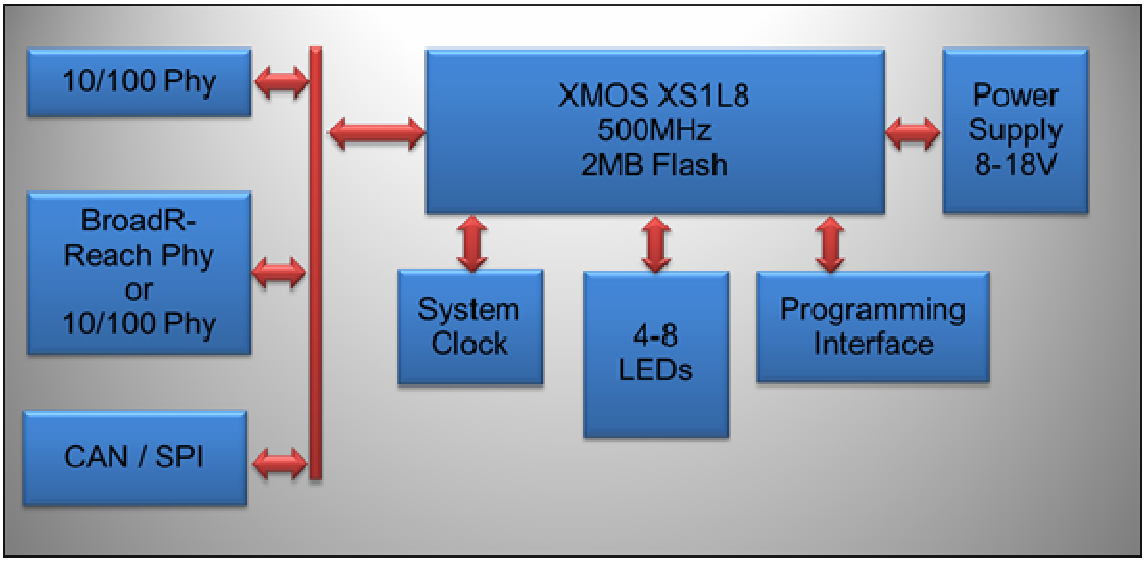

Bild 8: Ethernet Gateway System Architektur

Auf der Schnittstelleseite gibt es zwei Ethernet Ports, die je nach Konfiguration den 10/100 Standard oder das relative neue BroadR-Reach Format von Broadcom unterstützen. BroadR-Reach ist ein Transportprotokoll, das sich derzeit im Automotive Umfeld etabliert und auch für Industrie Anwendungen attraktiv ist (OPEN, 2017). Als Medium wird z.B. eine ungeschirmte Zweidrahtleitung eingesetzt, die sehr kostengünstig realisiert werden kann.

Bild 9: Portables Ethernet Protokoll-Analyse Gerät

Das Gateway stellt als dritten Port ein CAN oder SPI Interface zur Verfügung, das zur Signalisierung von Events oder als Schnittstelle zu einer HMI eingesetzt werden kann. In der kleinsten Gateway Variante wird ein 8-Core Baustein von XMOS verwendet, der intern mit 500MHz getaktet ist. Er hat genug Verarbeitungsleistung, um neben den Schnittstellen auch Applikationen wie CAN-Ethernet Routing, Netzwerkanalysator mit graphischer HMI (Bild 9) oder ein regelbasiertes Intrusion Detection System zu integrieren.

Durch den Einsatz paralleler Rechnerarchitekturen und optimierter Software ist es gelungen, eine Plattform für Intrusion Detection Systeme speziell für den industriellen Einsatz zu entwickeln. Derzeit beschäftigen sich mehrere Forschungsprojekte mit Algorithmen, die eine effektive Erkennung von Angriffen mit Hilfe solcher verteilter Systeme ermöglichen.

5. Literatur

BSI (2016). Die Lage der IT-Sicherheit in Deutschland. Bundesamt für Sicherheit in der Informationstechnik . Godesberger Allee 185–189. Bonn

Eckert, Claudia (2012): IT-Sicherheit. Konzepte – Verfahren – Protokolle. Oldenbourg Verlag

Hahn, Hans-Werner (2005). Die industrielle Revolution in Deutschland Band 49 von Enzyklopädie deutscher Geschichte. Oldenbourg Verlag

Hillenbrandt, Martin (2012). Funktionale Sicherheit nach ISO 26262 in der Konzeptphase der Entwicklung von Elektrik/Elektronik Architekturen von Fahrzeugen. KIT Scientific Publishing, Karlsruhe

May, David (2009). The XMOS XS1 Architecture, XMOS Limited

Mirow, Jürgen (1996). Geschichte des deutschen Volkes: Von den Anfängen bis zur Gegenwart, Bd. 1.

OPEN (2017). OPEN Alliance Special Interest Group, www.opensig.org

Tischer, M., Durumeric, Z., Foster, S., Duan, S., Mori, A. & Bailey, M., (2015). Users Really Do Plug in USB Drives They Find. University of Illinois, Urbana Champaign

TÜV (2015). Potenzielle Angreifer sind überall. TÜV Süd, Interne Studie

Prof. Dr. Axel Zimmermann studierte an der Universität Stuttgart Elektrotechnik und promovierte anschließen am Institut für Informatik der Universität Stuttgart. Im Anschluss daran arbeitete er über 20 Jahre in der Halbleiterindustrie unter anderem für die Unternehmen Xilinx, Lattice und Altera. 2015 folgte er dem Ruf an die Hochschule Aalen und vertritt dort seither die Bereiche Produktionsautomatisierung und Elektrotechnik. Er ist Leiter des Zentrums Industrie 4.0 der Hochschule Aalen sowie einer der Geschäftsführer der Transferplattform Industrie 4.0 des Steinbeis Innovationszentrums.
Kontakt: axel.zimmermann@hs-aalen.de