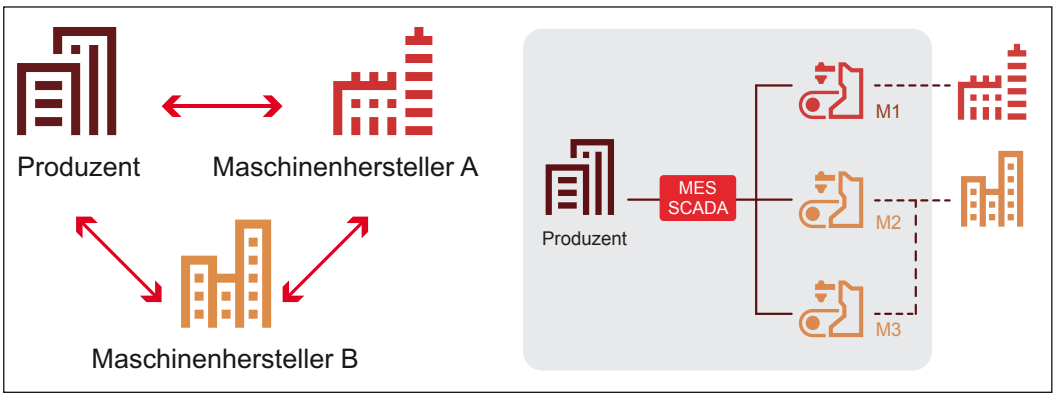
IT Retrofit – Secure IoT für existierende Maschinen und Anlagen

Die Vernetzung von Maschinen und Anlagen, die bereits seit Jahren in Betrieb sind und noch viele weitere Jahre zuverlässig ihren Dienst leisten können, ist eine Voraussetzung für eine erfolgreiche und effiziente Umsetzung von Digitalisierungsstrategien gerade in mittelständischen Unternehmen



Fallbeispiel 1: Wertschöpfungsnetzwerk (links) auf Infrastruktur-Netzwerk (rechts)

Dieses White Paper entwickelt ein Konzept zur sicheren Anbindung von Maschinen und Anlagen an Unternehmensprozesse. Die Umsetzung des Konzepts wird nachfolgend anhand der von der Janz Tec AG entwickelten Secure Appliance OSIRIS vorgestellt.

Secure IoT – Basis für neue Geschäftsmodelle

Die Eröffnung von Zukunftsmärkten für den deutschen Maschinen- und Anlagenbau wird durch die Fähigkeit, Geschäfts- und Vertriebsmodelle zu adaptieren, geprägt sein. Die in diesem Zusammenhang diskutierten Ansätze beruhen auf einer qualitativ weitergehenden Einbindung der Hersteller in Service- und Betriebsprozesse. Dabei übernimmt der Hersteller z.B. die komplette Verantwortung für die Verfügbarkeit bzw. Zuverlässigkeit der von ihm gelieferten Maschinen und Anlagen oder stellt diese in Betreibermodellen (Production as a Service) zur Verfügung. Die sich dabei bildenden Wertschöpfungsnetzwerke zwischen Herstellern, Betreibern, Produzenten und ggf. Servicedienstleistern sind „gekennzeichnet … durch komplexe wechselseitige Beziehungen zwischen autonomen, rechtlich selbstständigen Akteuren. Es bildet eine Interessengemeinschaft von potenziellen Wertschöpfungspartnern, die bei Bedarf in gemeinsamen Prozessen interagieren. Die Entstehung von Wertschöpfungsnetzwerken ist auf nachhaltigen ökonomischen Mehrwert ausgerichtet.“[1] Diese sind charakteristisch für die Produktion im Umfeld von Industrie 4.0.

Integration

Die Umsetzung adaptierter Geschäfts- und Vertriebsmodelle ist dabei wesentlich von der Integration der Maschinen und Anlagen in die digitale Infrastruktur jener Organisationen, die das Wertschöpfungsnetzwerk bilden, abhängig. Das so entstehende Infrastruktur-Netzwerk ist die technische Abbildung des Wertschöpfungsnetzwerkes und überschreitet die jeweiligen Organisationsgrenzen. Die Auslegung des Infrastruktur-Netzwerks muss den Anforderungen und grundlegenden Interessen von autonomen, rechtlich selbstständigen Akteuren hinsichtlich der Sicherheit ihrer privaten Informationen genügen.

Fazit

IT-Sicherheit und Digitalisierung von Geschäftsmodellen sind untrennbar verbunden. Der Schutz von privaten Informationen, unabhängig davon ob diese auf Personen, Prozesse oder Maschinen bezogen sind, ist Basis für die vernetzte Produktion.

IoT – Ansätze und Risiken

Im nachfolgenden Fallbeispiel werden eine einfache Umsetzung eines Wertschöpfungsnetzwerkes, das charakteristisch für die Produktion im Industrie-4.0-Umfeld ist, gezeigt und mögliche Risiken hinsichtlich der IT-Sicherheit diskutiert.

Wenn Risiken frühzeitig erkannt und entsprechend berücksichtigt werden, eröffnet die Nachrüstung von existierenden Maschinen und Anlagen mit gesicherten IT-Komponenten die Möglichkeit, mit vergleichsweise geringen Investitionen den Schritt in Richtung Industrie 4.0 zu realisieren. Konzepte für die Nachrüstung müssen neben den Anforderungen der IT-Sicherheit auch eine einfache Integration in bestehende Maschinen und Anlagen berücksichtigen.

Fazit

Die Planung der Umsetzung einer digitalisierten Produktion muss von Beginn an einen Prozess zur Erkennung und Behandlung möglicher Risiken im Bereich der IT-Sicherheit etablieren.

Fallbeispiel 1

Wertschöpfungsnetzwerk mit Einbindung von Maschinenherstellern in die Betriebsprozesse

Die Abbildung illustriert ein Wertschöpfungsnetzwerk zwischen drei Partnerunternehmen: Der Produzent setzt innerhalb der Produktion Maschinen von Hersteller A und B ein. Beide Maschinenhersteller sind für den Betrieb ihrer Maschinen M1 bis M3 zuständig und benötigen daher dedizierten, sicheren Zugriff auf diese. Das Infrastruktur-Netzwerk zeigt die notwendigen Netzwerkverbindungen. Allerdings kann eine direkte Umsetzung dieser Netzwerktopologie unter Umständen zu gravierenden Problemen führen. Dies sind beispielsweise:

- Unautorisierter Zugriff auf Produktionsdaten vom Produzenten durch Maschinenhersteller A und B an den jeweiligen Maschinen M1 bis M3
- Man-in-the-Middle-Angriff auf die Verbindungen der Maschinenhersteller in die Fabrik. Folgen eines gelungenen Angriffs können sein:
- Mithören von Daten, Erlangen von Betriebsdaten und Konfigurationen
- Einschleusen von Schadcode bzw. manipulierten Betriebsdaten
- Einbruch in das MES (Manufactoring Execution System) von M1, M2 und M3 aus.

IoT – Integrationskonzept

Hilfestellung sowohl bei der Konzeption der Integration als auch bei der Auswahl bzw. dem Design der notwendigen IT-Komponenten gibt die IEC 62443 „Industriellen Kommunikationsnetze – IT-Sicherheit

Autor:

Dr. Markus von Detten (li), Leiter Systems Engineering und Dr. Harald Hoffmann (re), Bereichsleiter Industrial Security und Senior Consultant, beide Janz Tec AG

Ereignis	Folge des Ereignisses	Schadens-potenzial	SIL (Safety Integrity Level)	Begründung für Schadenspotenzial
Abschalten der Maschine per Einschleusen des „Aus"-Signals von außen	Abschalten – Ausfall der Maschine	gering	1	1h Materialpuffer beim Übergang zum nächsten Produktionsschritt → geringe Auswirkung einer kurzzeitigen Abschaltung
Manipulation des Programmcodes der Steuerung	Indikation komplizierte Störung, z.B. Überhitzung Drehmomentwandler – Ausfall der Maschine	hoch	2	Produktionsausfall, Nichteinhaltung von Lieferzusagen
Einschleusen einer falschen Konfiguration von außen – Angriff auf Verbindung	falsche Konfiguration	hoch	–	Qualitätsmängel oder Produktionsausfall, Nichteinhaltung von Lieferzusagen
Abhören der übermittelten Konfiguration – Angriff auf Verbindung	Erlangen der Konfiguration	hoch	–	Abfluss von Firmen Know-how
Manipulation des Programmcodes der Steuerung	Ausfall des Magnetspannfutters im Betrieb	sehr hoch	4	Lebensgefahr für Personal im direkten Umfeld, Beschädigung der Maschine

Tabelle 1: Schadenspotenziale

für Netze und Systeme" [2]. Diese definiert eine Reihe von Standards, welche speziell auf die IT-Sicherheit von Steuerungs- und Automatisierungssystemen (= Industrial Security) abzielen.

Bestandsaufnahme und Analyse von Schadenspotenzialen

Ausgangspunkt des Integrationskonzepts ist eine Bestandsaufnahme der zu schützenden Bereiche in einer Organisation (Fabrik, Anlage) sowie darauf abbildbarer Bedrohungsszenarien. Es wird eine Einschätzung des Schadenspotenzials, welches bei Ausfall bzw. Störung des jeweiligen Bereiches eintreten kann, vorgenommen. Dabei sind bei der Bestandsaufnahme die Lokalisierung von Equipment, dessen Konnektivität (LAN, WLAN, WWAN) etc., die Funktion im Betriebsprozess und damit einhergehenden Szenarien zu berücksichtigen. Dies führt zu einer Festlegung von Zonen. Hilfestellung bei der Schätzung des Schadenspotenzials geben unter anderem die Betrachtungen zur funktionalen Sicherheit (FMEA – Failure Mode and Effects Analysis, FHA – Functional Hazard Assessment) eines Systems in Zusammenhang mit den Normen IEC 61508 und IEC 62061 [3] [4]. Führt der Ausfall bzw. Fehlfunktion eines Systems z.B. zu einer lebensgefährlichen Situation für den Bediener einer Anlage, ist dies unbedingt zu berücksichtigen. Darüber hinaus sind weitere schützenswerte Güter zu benennen und das relevante Schadenspotenzial zu bestimmen. Ein schützenswertes Gut kann z.B. spezielles Firmen-Know-how sein, welches in Maschinenkonfigurationen, Rezepten oder Designdaten abgelegt ist.

Fallbeispiel 2 zeigt eine entsprechende Analyse.

Aus dem Schadenspotenzial und den Eintrittswahrscheinlichkeiten werden die IT-Security Level (SL) für den jeweiligen Bereich festgelegt. Dafür stehen unterschiedliche Methoden zur Verfügung. Neben dem Vorgehensmodell der IEC 62443-3-2 seien hier Microsoft STRIDE/DREAD [5] oder OCTAVE [6] genannt.

Fazit

Die Einschätzung von Risiken erfolgt auf Basis der möglichen Schadenspotentiale und der Eintrittswahrscheinlichkeit. Die Risikoeinschätzung ist Ausgangspunkt für die Etablierung von Strategien für die Gewährleistung der IT-Sicherheit. Die Aufteilung einer Organisation in Zonen annähernd gleichen IT-Risikolevels führt dabei zu einer vereinfachten und besser handhabbaren Struktur.

Fallbeispiel 2

Bestandsaufnahme der zu schützenden Bereiche und relevanter Bedrohungsszenarien

Die im Fallbeispiel 1 definierte Fabrik wurde in einer ersten Analyse in die Bereiche Management, MES/SCADA, M1, M2 und M3 zerlegt. Die Tabelle 1+2 erfassen die Schadenspotenziale für den Bereich M1 und ein abstraktes Bedrohungsszenario.

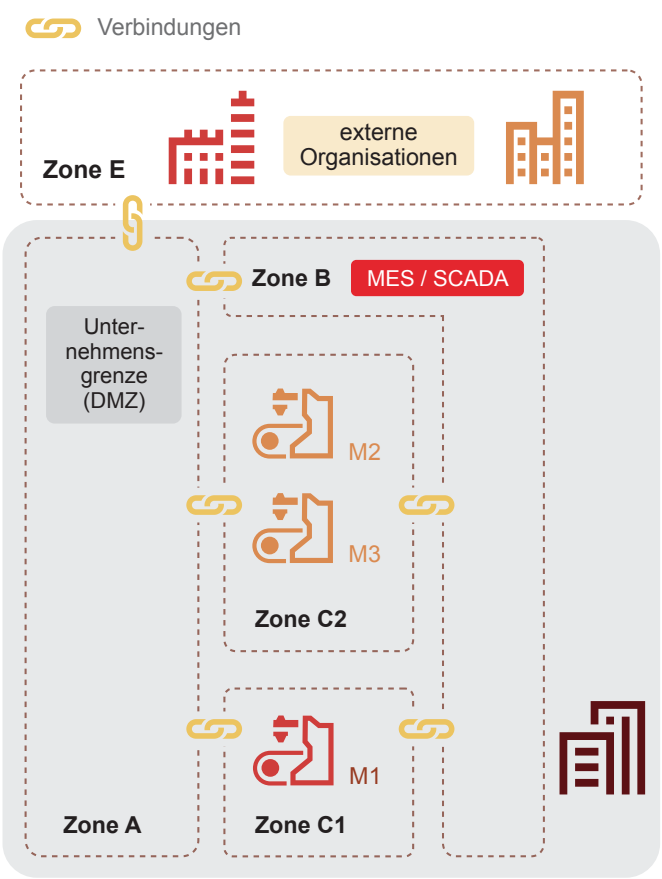
Aus der Betrachtung ergeben sich drei Bedrohungsszenarien, die hinsichtlich Eintrittswahrscheinlichkeit, Schadenspotenzial, Minimierungsmöglichkeiten, damit verbundener Reduktion des Schadenspotenzials und dem Erreichen des Schutzziels zu bewerten sind.

Analyse der IoT-Kommunikationsinfrastruktur

In einem zweiten Schritt werden die Verbindungen (Conduits), d.h. der Informations- und Datenfluss zwischen den Zonen, betrachtet. Dies führt zu einer Kommunikationsinfrastruktur/Netzwerktopologie. Die Topologie selbst ist zunächst maßgeblich von der Tiefe der horizontalen (Kommunikation auf Maschinen-Ebene) und der vertikalen (Kommunikation Maschine zu übergeordneten bzw. entfernten Instanzen) Integration abhängig. Ansätze für Fernwartung und -konfiguration durch die

Bedrohungsszenario	Schadens-potenzial	Eintrittswahr-scheinlichkeit	Minimierungsmöglichkeiten	Ziel SL (IT Security Level nach IEC 62443)	Schutzziel
Angriff auf Verbindung	hoch	hoch	Einsatz kryptografischer Verfahren bei der Übertragung	2	Vertraulichkeit Integrität/ Authentizität
Manipulation des Programmcodes der Steuerung	sehr hoch	gering	Sicherung Programmcode etc. als vertrauliche Daten (BackUp); Vergleich BackUp – Einsatzdaten über Hashes	2	Verfügbarkeit Integrität/ Authentizität
Diebstahl/ Erlangen von Konfigurationen/ Rezepten	sehr hoch	hoch	Verschlüsselung von Konfigurationen, Programmcode etc. und Ablage in manipulationssicheren Systemen	3	Verfügbarkeit Integrität/ Authentizität

Tabelle 2: Bedrohungsszenarien



Nach eingehender Analyse wurden folgende Zonen innerhalb der im Fallbeispiel 1 definierten Fabrik festgelegt:

Zone A: Abgrenzung der Fabrik nach außen durch eine geeignete Infrastruktur. Aufgabe: Sicherung nach außen, Management des eingehenden/ausgehenden Verkehrs. Integrität und Verfügbarkeit als Schutzziele.

Zone B: MES/SCADA System. Verfügbarkeit, Authentizität und Integrität als Schutzziele.

Zone C1: Maschine M1. Verfügbarkeit, Authentizität und Integrität als Schutzziele. SL 3 wurde bereits bestimmt (Fallbeispiel 2).

Zone C2: Maschine M2 und M3. Redundante Maschinenanordnung. Verfügbarkeit, Authentizität und Integrität als Schutzziele. Die Zerlegung der Zone C2 in zwei Sub-Zonen (C21 und C22) ist zu untersuchen.

Zone E: Externes Netzwerk (Internet und Netzwerke anderer Organisationen).

Fallbeispiel 3: Analyse der Datenzonen und ihrer Verbindungen

Hersteller der genutzten Maschinen und Anlagen führen speziell bei gemischten Maschinenparks zu Topologien, die nicht mehr zu klassischen, hierarchischen Ansätzen bei der Kommunikation zwischen Zonen passen. In Fallbeispiel 1 entspricht die produzenteninterne Infrastruktur der klassischen Automationspyramide [3]. Die Fernwartung durch die Maschinenhersteller A und B erfolgt im Fallbeispiel 1 aber an dieser Infrastruktur vorbei. Dies schwächt in der aktuellen Organisation die Security-Situation des Produzenten.

Die IT-Administration der Organisation und der einzelnen Zonen sollte von zentraler Stelle aus erfolgen, um Zugriffe auf die Zonen und dem darin lokalisierten Equipment zentral zu verwalten. Dies ist insbesondere für Fernwartungsstrategien von eminenter Bedeutung, da hier die Verwaltung des Zugangs eines außerhalb der Organisation stehenden Nutzers zeitlich befristet realisiert werden muss.

Fazit

Conduits verbinden die Zonen und bilden das grundlegende Kommunikationsnetzwerk ab. Die Auslegung des Kommunikationsnetzwerkes sollte bereits in diesem Stadium die Möglichkeit der Segmentierung in Teilnetzwerke und die Isolation (Separierung) von kritischen Zonen (Zugänge über WLAN, Internetzugänge etc.) berücksichtigen.

Analyse der Zonen und ihrer Verbindungen

Final müssen Zonen und ihre Verbindungen hinsichtlich der notwendigen Schutzmaßnahmen/-ziele weiter analysiert werden. Daraus ergeben sich eine Reihe spezieller Anforderungen aus Richtung der IT-Sicherheit, die bei der Auswahl des IT-Equipment im konkreten Anwendungsfall berücksichtigt werden müssen. Die IEC 62443-1-1 definiert dabei Basisanforderungen, welche, abhängig vom IT-Security-Level, durch die IEC 62443-3-3 weiter untersetzt werden.

Neben diesen IT-Security relevanten Anforderungen muss das Equipment die innerhalb der jeweiligen Zone vorhandenen Schnittstellen zu Maschinen und ggf. Sensoren bzw. Aktoren implementieren. Die Anzahl und der Typ der verwendeten Protokolle wird wesentlich durch die Komplexität der in der Zone angesiedelten Maschinen, Sensoren und Aktoren bestimmt. Das Nebeneinander unterschiedlicher Standards führt speziell bei der Integration des IT-Equipments zu Problemen, da eine Implementierung aller möglichen Schnittstellen schon aus Kostengründen nicht möglich ist. Bei der Auslegung des IT-Equipments sind also von vornherein Anforderungen hinsichtlich Erweiterbarkeit, Komponentenbildung und Modularität sowie Portierbarkeit zu berücksichtigen, um die spätere Interoperabilität bei der Integration in den Zonen überhaupt realisieren zu können.

Fallbeispiel 3

Fallbeispiel 3 zeigt die Aufteilung in Zonen und Verbindungen für das in Fallbeispiel 1 definierte Wertschöpfungsnetzwerk. Es legt vier interne Zonen fest und identifiziert mehrere Verbindungen zwischen diesen. Im nächsten Schritt ist nun zu klären, wie dieses Infrastrukturkonzept umzusetzen ist.

Fazit

Die für jede Zone zu definierenden Schutzziele bestimmen die Anforderungen an das IT-Equipment. Allgemeine Anforderungen sind

1. Identifizierung und Authentifizierung
2. Nutzungskontrolle
3. Systemintegrität
4. Vertraulichkeit der Daten
5. Eingeschränkter Datenfluss
6. Rechtzeitige Reaktion auf Ereignisse
7. Ressourcenverfügbarkeit.

Definition der Sicherheitsarchitektur

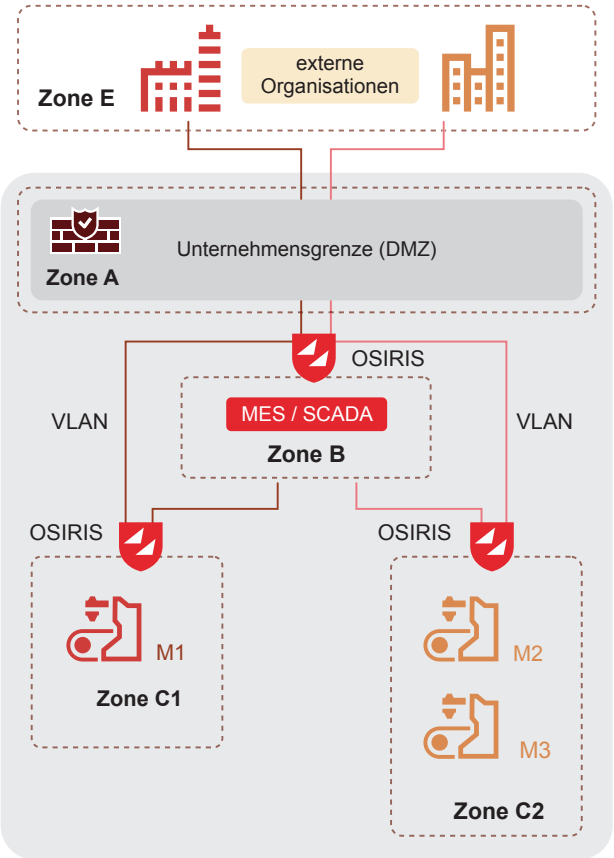
Fallbeispiel 4 zeigt den Übergang von Zonen und Verbindungen in eine Netzwerkinfrastruktur. Innerhalb dieser Struktur kommt dem Schutz der Zonen eine besondere Bedeutung zu.

Die Zone A beherbergt die DMZ (De-Militarized Zone) und stellt damit eine allgemeine Schutz- und Zugriffsmanagementfunktion für das gesamte Unternehmen sicher. Hier können Standard-IT-Komponenten zum Einsatz kommen. Die innerhalb des Unternehmens gebildeten Zonen müssen nunmehr entsprechend ihres SL nochmal separat abgesichert werden.

Dafür steht mit Janz Tecs Secure Appliance OSIRIS eine spezielle Architektur bereit, die nachfolgend erläutert wird.

Sicherheitsarchitektur

Fallbeispiel 4 verdeutlicht den Einsatz von OSIRIS zur Realisierung von Zonen. Die allgemeinen technischen Anforderungen, die aus Richtung der IT-Sicherheit an ein solches Equipment gestellt werden, wurden bereits hergeleitet. In der Tabelle 3 sind diese gemeinsam mit Umsetzungen, welche für OSIRIS gewählt wurden, zusammengefasst. OSIRIS realisiert ein mehrstufiges und



Das Fallbeispiel zeigt ein Szenario, welches auf eine Anbindung von Anlagenteilen und Maschinen abstellt, die jeweils eine geschlossene Zone realisieren. Dabei wird innerhalb der Zone eine komplett private, d.h. organisationsinterne Struktur, über OSIRIS realisiert. Der Zugriff auf die Zone wird zentral gesteuert (freigegeben/gesperrt). Typische Anwendungsfälle sind die Freigabe von dedizierten lokalen Ressourcen (gespeicherte Fehlerinformationen, Nutzungszyklen etc.) für Vor-Ort-Wartungsvorgänge oder die Freigabe bestimmter Informationen für Cloud- oder Fernwartungsdienste.

Eine über OSIRIS mögliche Erweiterung erlaubt es, ein in der Zone C1 oder C2 gebildetes VLAN in einem Tunnel bis zur Organisationsgrenze (Zone A, Übergang zu öffentlichen Netzen) zu führen. Nunmehr kann über die zentrale Administration der Zugriff auf dedizierte, über das VLAN erreichbare Services und Daten gesteuert werden. Ein Fernwartungszugriff von extern wird somit zentral entgegengenommen und in das entsprechende VLAN geroutet.

Fallbeispiel 4: Neue Sicherheitsarchitektur basierend auf vorab definierte Zonen und Verbindungen

in Abhängigkeit von der Anwendung adaptierbares Sicherheitskonzept. Auf der untersten Ebene sind Maßnahmen angesiedelt, die eine Manipulation der Firmware bzw. das Einschleusen fremder Software ausschließen. Auf Basis dieses Ansatzes kann über spezielle Maßnahmen auch eine Manipulation der Hardware verhindert werden.

Um die Anzahl möglicher Angriffsvektoren auf das System zu minimieren, wird ein minimales Betriebssystem genutzt, welches für die jeweilig genutzte Hardware und den angeforderten Funktionsumfang konfiguriert wird.

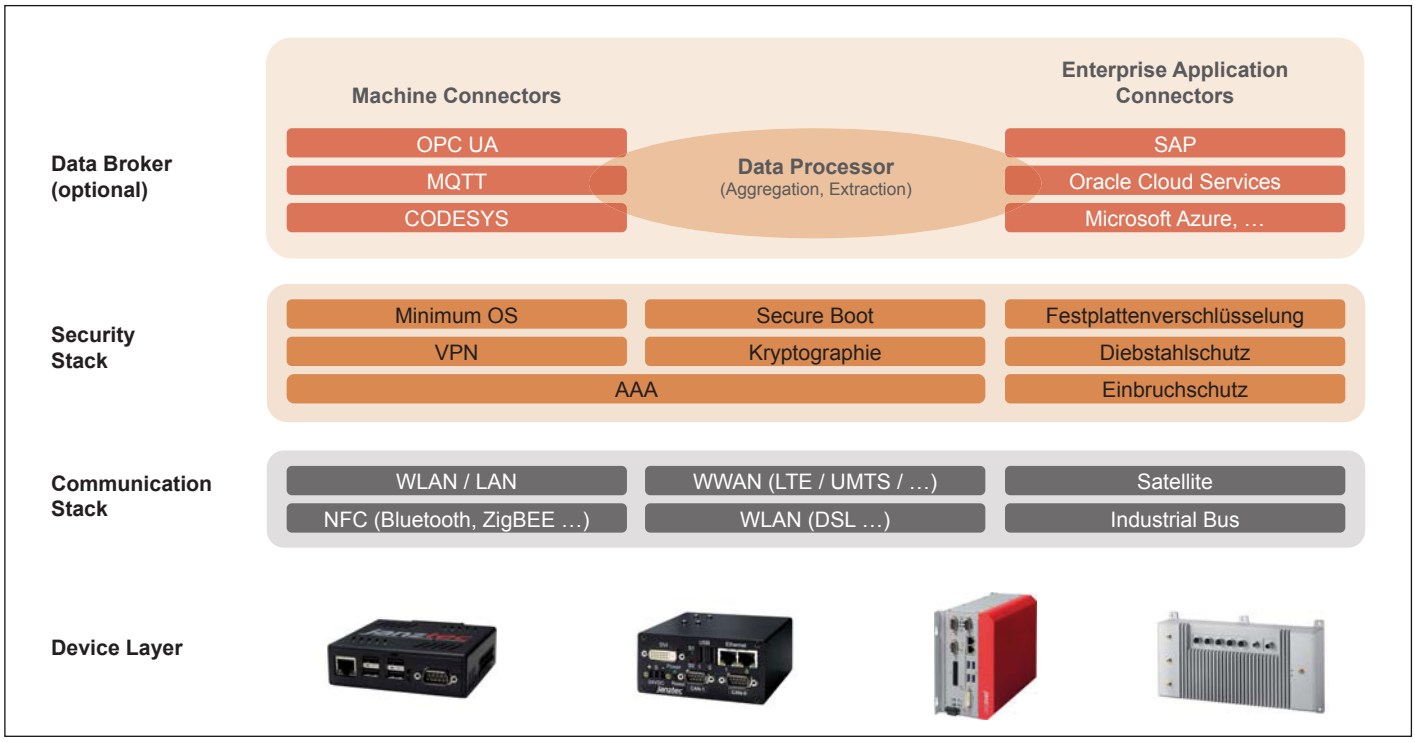
Zur Absicherung der Kommunikation zwischen Zonen bzw. zu zentralen Einrichtungen kommen Standard-VPN-Implementierungen zur Sicherstellung der Vertraulichkeit und Integrität der Daten zum Einsatz. Die Verschlüsselung wird gemäß BSI-Empfehlung konfiguriert. Die Autorisierung erfolgt mit Hilfe von X.509 Zertifikaten (für Client und Server). Mechanismen zur automatisierten Erneuerung von Zertifikaten sind vorgesehen.

Um eine Kapselung der Zonen und somit auch einen autarken Betrieb zu ermöglichen, erweitert OSIRIS die in Zone A befindliche zentral geführte IT-Infrastruktur inklusive des Sicherheitssystems in jeweils lokale Endpunkte bzw. Zonen. Dazu wird stets die entsprechende Untermenge der in Zone A zentral geführten Nutzer- und Geräteinformationen mitgeführt und diese mit den zentralen Informationen synchronisiert sobald Verbindungen dorthin verfügbar sind.

Innerhalb der Zone wird die Authentifizierung und Autorisierung für den (W)LAN-Zugang auf Basis der mitgeführten Nutzer- und Geräteinformationen über das Extensible Authentication Protocol (EAP) realisiert. EAP beschreibt eine vollständige Umgebung zur Authentifizierung und Autorisierung. EAP-Messages können in verschiedene Protokolle eingebunden werden. IEEE 802.1X (EAP over LAN – EAPOL) spezifiziert das Protokoll für die Anwendung auf Netzwerk-Ebene (Layer 3, OSI Modell), welches durch OSIRIS zur Netzwerkzugangskontrolle genutzt wird. Je nach Größe des LAN und interner Policy stellt OSIRIS verschiedene Mechanismen zum Aufbau von Teilnetzen (VLAN) innerhalb des LAN zur Verfügung. Bei Vorhandensein solcher Teilnetze wird der Zugriff auf diese durch den Autorisierungsprozess

Anforderung	Umsetzung – OSIRIS
Identifizierung und Authentifizierung	• Anbindung eines Verzeichnisdienstes zur Identifizierung, Authentifizierung und Autorisierung von Nutzern und Geräten
Nutzungskontrolle	• Authentifizierung aller Kommunikationsteilnehmer auf Zertifikatsbasis
	• Nutzungsmonitoring (mind. Login/Logout-Zeit)
	• Realisierung zeitbeschränkter Zugänge
Systemintegrität	1. Sicherung der (W)WAN Verbindungen – VPN
	2. Sicherung (W)LAN – Network Access Control über 802.1X Implementation (zertifikatsbasiert)
	3. Minimales Betriebssystem
	4. Signatur der Soft-/Firmware (Schutz gegen Manipulation und Schadcode)
	5. Verschlüsselung der Soft-/Firmware (Schutz gegen Ausspähen)
Eingeschränkter Datenfluss	Separierung von Netzen über VLAN, Filterung des Datenverkehrs (Firewall)
Vertraulichkeit der Daten	Zugriffsautorisierung (Dateien, Verzeichnisse), Verschlüsselung, Verteilung und Back-Up des Datenbestandes
Rechtzeitige Reaktion auf Ereignisse	Automatisiertes Systemmonitoring & Auslösen von Schutzmechanismen (IDS/IPS)

Tabelle 3: Umsetzung der Sicherheitsanforderungen der IEC 62443 mit der Secure Appliance OSIRIS



abgebildet. Damit können innerhalb der Zone weitere LAN-Enklaven mit unterschiedlichen Zugriffsrechten geschaffen werden. Ist OSIRIS von der zentralen Infrastruktur getrennt, stellt es Netzwerk- und Anwendungsdienste lokal bereit. Dabei ist der Umfang der lokalen Bereitstellung von Diensten von den verfügbaren Ressourcen abhängig. Die Funktionsfähigkeit der durch OSIRIS bereitgestellten lokalen Endpunkte für die dort angeschlossenen Nutzer/Maschinen ist auch bei Ausfall der Verbindung zur zentralen Infrastruktur gewährleistet. Wird OSIRIS für die Speicherung von Daten (Maschinenkonfigurationen, Rezepte etc.) genutzt, werden diese verschlüsselt abgelegt. Zugriffe auf Daten werden über die in OSIRIS implementierte Authentifizierungs- und Autorisierungsstruktur geregelt.

Fazit

OSIRIS erfüllt hinsichtlich der Sicherheitsarchitektur alle Anforderungen der IEC 62443 und stellt gleichzeitig Mechanismen für die Integration in existierende Infrastrukturen bereit.

Architektur

Die OSIRIS Architektur lässt sich in vier Schichten zerlegen:

1. Device Layer – stellt die Hardware zur Verfügung. Je nach Anforderung können unterschiedliche Plattformen der Janz Tec AG genutzt werden.

2. Communication Stack – stellt ein Set von Kommunikationstechnologien zur Verfügung, die je nach Auslegung in Nutzung genommen werden können.

3. Security Stack – integriert ein modulares Sicherheitskonzept, welches die Hardwareeigenschaften, die genutzten Kommunikationstechnologien und implementierte Anwendungen berücksichtigt.

4. Optionaler Data Broker – stellt die Interoperabilität mit unterschiedlichen Schnittstellen und Protokollen sicher. Der Data Broker ist eine separate und erweiterbare Schicht in der OSIRIS Architektur. Über den Data Broker wird das Anmelden von Schnittstellen und die Zuordnung von Treibermodulen realisiert.

Fazit

Eine modulare, den jeweiligen Erfordernissen anpassbare Architektur ist OSIRIS zugrunde gelegt. Damit können skalierbare und hinsichtlich der Sicherheitsinfrastruktur angepasste Lösungen realisiert werden. Unterschiedliche Anforderungen bei der Integration werden erfüllt.

Zusammenfassung

Das Retrofit von existierenden Anlagen und Maschinen muss die Erfordernisse hinsichtlich des IT-Schutzes und einer effizienten Integration berücksichtigen.

Mit OSIRIS besteht ein IT-Equipment, das diesen Anforderungen genügt und für Neubau- und Nachrüstprojekte zur Verfügung steht. Es fungiert als in seiner Funktion skalierbarer mobiler „Mini- Server“, der die IT-Dienste der bestehenden Infrastruktur innerhalb jeder Zone zur Verfügung stellen kann und diese gleichzeitig von der Umgebung abgrenzt.

Literatur

[1] Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0, Abschlussbericht des Arbeitskreises Industrie 4.0 (2014)
[2] IEC 62443 Industrial communication networks – Network and system security
[3] IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems
[4] IEC 62061, Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems
[5] https://msdn.microsoft.com/en-us/library/ff648644.aspx
[6] http://www.cert.org/resilience/products-services/octave/index.cfm

■ *Janz Tec AG*
mail@janztec.com
www.janztec.com

https://www.janztec.com/white-paper-secure-iot/