

SAFETY & SECURITY FÜR M2M KOMMUNIKATION

Christoph Schmittner, Erwin Schoitsch

Kurzfassung: *Safety&Security für Machine-to-Machine Kommunikation ist ein wichtiges Thema für industrielle System und neue Anwendungsfälle. Durch die zunehmende Vernetzung entstehen neue Risiken. Im vorliegenden Beitrag wird ein Überblick über Herausforderungen und Stand der Technik gegeben sowie anhand eines Anwendungsfalls aus der Praxis eine mögliche Lösung vorgestellt.*

Schlüsselwörter: M2M Kommunikation, Safety, Security, Reliability, Industrie 4.0

1. EINLEITUNG

Die Digitalisierung, also die Integration und virtuelle Abbildung von Produkten, Systemen und Lösungen ist ein wichtiges Wachstumsfeld für die Industrie. Zusammengefasst als Industrie 4.0, beschreibt es eine zunehmende Verflechtung von realer und virtueller Welt, einschließlich der Abbildung realer Güter, Systeme und Prozesse als digitale Zwillinge.

Eine wichtige Rolle spielt dabei die Machine-to-Machine (M2M) Kommunikation zwischen Maschinen oder Maschinen und zentralen Systemen. Während in der Vergangenheit Kommunikation und Vernetzung von Maschinen kabelgebunden und lokal erfolgte, sind neue Systeme zunehmend mit Anbindungen an kabellose Netzwerke ausgestattet. Diese Vernetzung führt auch zu einer teilweise Aufweichung der klassischen hierarchischen Kommunikationsarchitektur. Bislang nur über eingeschränkt angebundene Systeme werden in IP-basierte Netzwerke eingebunden. Damit einhergehend ist Security, zusätzlich zu Reliability und Safety, eine neue Herausforderung bei Design und Entwicklung (Schmittner, et al., 2015).

Während neue Systeme bereits mit Security und Intelligenz ausgestattet werden und eigene sowie fremde Daten kombinieren um remote Access oder remote Maintenance unterstützen stellt dies für existierende Systeme eine große Herausforderung dar. Meist werden relevante Sensorwerte zwar erfasst, aber es existiert keine Historie oder ein Konzept für den Fern-Zugriff. Im Folgenden wird anhand eines industriellen Use Case beschrieben wie diese Herausforderungen gelöst werden können.

2. SICHERE M2M KOMMUNIKATION

Vernetzung von Systemen und Öffnung zum Internet ohne Berücksichtigung von Security führte bereits zu einer Vielzahl von Sicherheitslücken. Während bei Industrieanlagen bisher nur Vorfälle bei einer iranischen Nuklearaufbereitungsanlage, einem deutschen Stahlwerk und einer Wasseraufbereitungsanlage bekannt wurden, wurden im weiteren Bereich vom Internet der Dinge (IoT) und M2M bereits eine Vielzahl an Sicherheitslücken identifiziert. Diverse Systeme, von Fahrzeugen bis GPS-Trackern, Insulin-Pumpen, Smart Meter und intelligenten Überwachungskameras wurden erfolgreich angegriffen. Einer der schwerwiegendsten Angriffe auf die Infrastruktur des Internets wurde von Kameras, Glühbirnen und Haushaltsgeräten ausgeführt (Schuster, 2016). Ähnlich wie Safety muss Security bereits beim Design von Funktionen, Architekturen und der Implementierung beachtet werden.

2.1 Stand der Technik

Derzeit beschäftigen sich einige Standardisierungsgruppen mit dem Thema sichere M2M Kommunikation und allgemein sicheres (also safe and secure) Industriesysteme. Das European Telecommunications Standards Institute (ETSI) beschäftigt sich mit M2M Secure Kommunikationsstandards. Aktivitäten sind dabei nicht auf Maschinen und Industrie beschränkt sondern umfassen M2M für IoT allgemein in allen Domänen, von

Industriesystemen, Smart Grids bis Smart Cities. IEC 62443 ist eine derzeit in der Veröffentlichung befindliche Normenreihe für „Industrielle Kommunikationsnetze - IT-Sicherheit für Netze und Systeme“. Dabei wird nicht nur die M2M Kommunikation sondern allgemein die Netzwerkarchitektur betrachtet.

Weitere Aktivitäten sind z.B. IEC TC65 WG20, „Industrial-process measurement, control and automation– Framework to bridge the requirements for safety and security“ welche sich mit der gemeinsamen Betrachtung von Safety und Security beschäftigen.

Im Bereich der Kommunikationsprotokolle gab es eine ähnliche Entwicklung hin zur Berücksichtigung von Security und weiteren Funktionalitäten. Während etablierte Protokolle für die M2M Kommunikation Security nur ungenügend unterstützten und für direkte Kommunikation ausgelegt waren unterstützen neue M2M Protokolle wie OPC-UA, MQTT oder CoAP ein publish/subscribe Modell sowie Benutzerauthentifizierung. Dadurch ist die Einbindung von bestehenden Systemen in neue Servicemodelle eine große Herausforderung bezüglich Sicherheit und Zuverlässigkeit.

2.2 Szenario

Als Szenario betrachten wir einen Teststand im Produktionsnetzwerk einer Firma. Für Wartung und Erfassung des Systemzustands möchte der Hersteller des Teststands mit dem System kommunizieren.

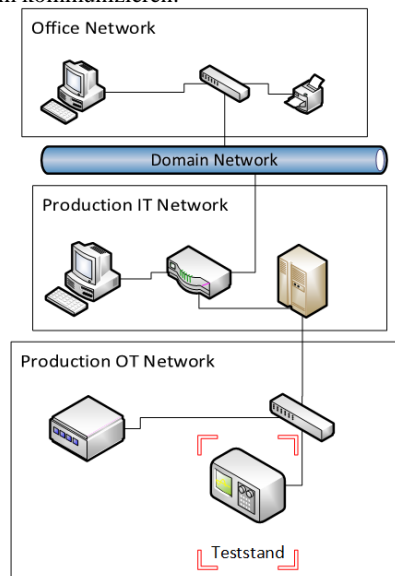


Abb. 1: Systemarchitektur, Ausgangslage

Abb. 1: Systemarchitektur gibt einen vereinfachten Überblick über die Ausgangsbasis. Der Teststand (markiert in der Abbildung mit den hervorgehobenen Ecken) soll mit einem anderen, extern liegenden, System vernetzt werden. Der Hersteller möchte Zustands- und Nutzungsstatistiken des Systems erfassen um dem Betreiber Zuverlässigkeitsgarantien und eine bessere Planung der Wartungs- und Stillstandszeiten anbieten zu können.

Eine erste Risiko- und Assetanalyse ergab einen hohen Schutzbedarf. Ein Stillstand des Teststands kann einen hohen finanziellen Schaden verursachen, im Produktionsnetzwerk sind wertvolle Firmendaten verfügbar und Fehlfunktionen im System können potentiell Schaden an Geräten und Personen verursachen.

Zudem sind im Produktionsnetzwerk Systeme teilweise noch mit älterer Software mit bekannten Sicherheitslücken ausgestattet und das Netzwerk ist allgemein für einfache Kommunikation ausgelegt.

2.3 Lösungsansätze

Abstrakt betrachtet kann dieses Problem auf drei Arten gelöst werden.

1. Umstellung des Produktionsnetzwerk auf eine neue und sichere Netzwerkarchitektur
2. Vernetzung und Absicherung auf einer überliegender Ebene
3. Direkte Kommunikation zwischen Maschine und Hersteller

Alternative 1 ist am flexibelsten, verursacht aber auch die höchsten Kosten. Es sind teilweise Neuanschaffungen von Maschinen notwendig und bei historisch gewachsenen Systemen kann bereits der erste Schritt, die Erfassung des bestehenden Systems mit Datenflüssen und Kommunikationen eine Herausforderung darstellen.

Alternative 2 ist sinnvoll wenn eine Firma generell eine Erfassung von Zustandsdaten ihrer Maschinen ermöglichen will. Eine zentrale Sammlung mit eingeschränktem Zugriff für die Hersteller kann dazu dienen die Wartung zu optimieren und Unterschiede zwischen einzelnen Produktionsstätten zu erfassen.

Alternative 3 kann potentiell einen neuen Angriffsvektor auf das Gesamtsystem öffnen wenn die Kommunikation nicht auf das Zielsystem beschränkt ist und die Zugriffsmöglichkeiten eingeschränkt sind. Vorteilhaft ist das bei ausreichender Trennung kein Einfluss auf das sonstige Firmennetzwerk möglich ist.

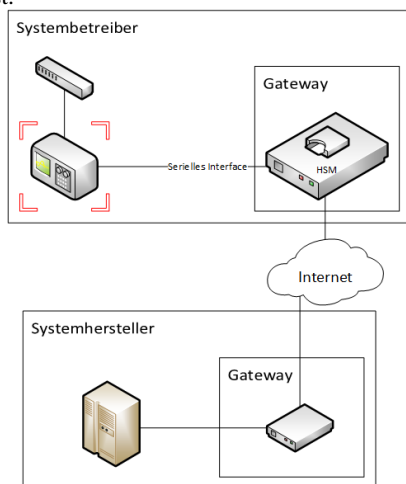


Abb. 2 Kommunikationsarchitektur

Um dies sicherzustellen wird ein Gateway eingesetzt das mittels einer seriellen Schnittstelle mit dem Teststand kommuniziert. Im Gateway selber steht ein Hardware-Security-Modul (HSM) von Infineon (Lesjak, et al., 2014) zur Verfügung. Abb. 2 Kommunikationsarchitektur zeigt die gewählte Kommunikationsarchitektur. Durch die serielle Vernetzung zwischen Gateway und Teststand ist bereits nur ein eingeschränkter Zugriff auf das Restsystem möglich. Zusätzlich sind bei dieser Architektur keine Eingriff oder Anpassungen im Firmennetzwerk des Maschinenbetreibers notwendig.

AUTOR

Christoph Schmittner



AIT Austrian Institute of Technology GmbH, Digital Safety & Security Department
Donau-City-Straße 1 | 1220 Vienna | Austria | +43 664 88256009 | Christoph.schmittner.fl@ait.ac.at

Kurzer Lebenslauf: Christoph Schmittner hat einen Abschluss in technischer Informatik (B.Sc.) und Elektrotechnik (M. Sc). Am AIT forscht er an Methoden, Tools und Systemen für sichere und zuverlässige Systeme.

2.4 Entwicklungsprozess

Für die Entwicklung des Systems und des Sicherheitskonzepts wurde ein iterativer Entwicklungsprozess angewandt. Systemzuverlässigkeit und Cybersicherheit wurde gemeinsam betrachtet und ein ganzheitliches Sicherheitskonzept und Design erstellt.

Basierend auf den Anforderungen und der Systemarchitektur wurde eine Safety & Security Analyse durchgeführt. Die Ergebnisse der Safety & Security Analyse wurden für die Erstellung eines Safety & Security Konzepts verwendet. Das Konzept wurde reviewet und dann für die Erstellung eines verfeinerten Design genutzt.

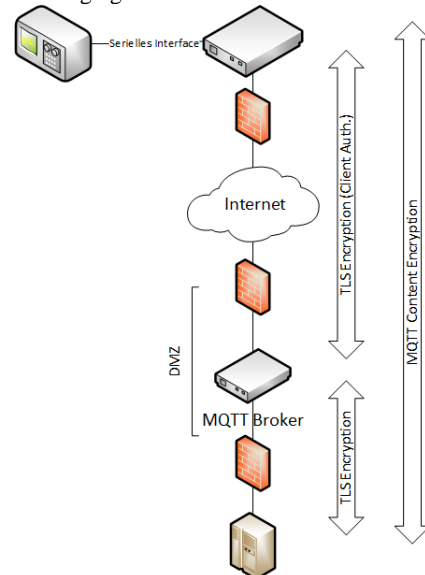


Abb. 3: Sicherheitskonzept

3. ZUSAMMENFASSUNG UND AUSBLICK

Abb. 3: Sicherheitskonzept zeigt das Ergebnis des iterativen Designprozesses. Die Vernetzung von bestehenden Systemen und die Verteilung von Funktionen über das Internet sind Herausforderungen die nicht nur bei Industrieanlagen sondern in vielen technischen Anwendungsfeldern entstehen. Ein Gateway mit einem HSM kann dabei ein Safety & Security Design als „Trust Anchor“ unterstützen. Nächste Schritte sind die Ausweitung des Konzepts auf andere Domänen und Anwendungsfälle

4. LITERATURVERZEICHNIS

Lesjak C [et al.] A Secure Hardware Module and System Concept for Local and Remote Industrial Embedded System Identification [Konferenz] // Proceedings of the 2014 IEEE Emerging Technology and Factory Automation (ETFA). - 2014.

Schmittner Christoph, Zhendong Ma und Gruber Thomas Combining Safety and Security Engineering for Trustworthy Cyber- Physical Systems [Journal] // ERCIM News. - 2015. - 102. - S. 19 - 20.

Schuster Johannes Frustrierter PlayStation-Spieler legte Teile des Internets lahm [Online] // Heise. - 20. 11 2016. - <https://heise.de/-3492276>.