PLATTFORM INDUSTRIE4.0

LEITFADEN

Security in RAMI4.0

Mit den vielen neuen Chancen von Industrie 4.0 sind auch viele Herausforderungen verbunden. So wird auch „Security-by-Design“ zum unverzichtbaren Element der Industrie 4.0-Entwicklungs- und Konzeptarbeiten. In vielen Fällen wirkt Security als Enabler neuer Geschäftsmodelle.

Security wirkt wie ein Gerüst, das alle Strukturelemente des RAMI4.0 und damit auch das Design der Industrie 4.0-Komponente trägt und zusammenhält. Im Folgenden wird daher auf die Security-Aspekte des RAMI eingegangen, um diese dem Leser deutlich zu machen. Konkrete Security-Maßnahmen werden anhand einiger Beispiele für alle drei Achsen des RAMI4.0 beschrieben.

RAMI4.0 – Referenzarchitekturmodell für Industrie 4.0

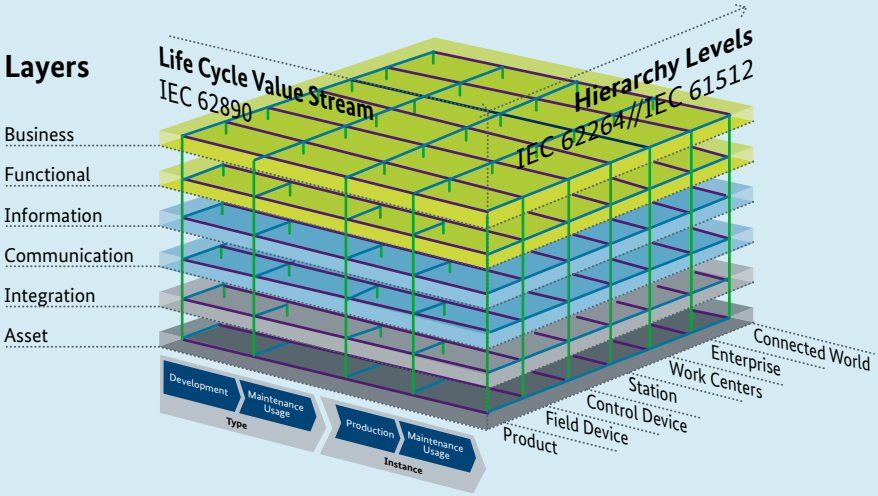
RAMI4.0 beschreibt strukturiert die wesentlichen Elemente eines Objekts/Assets mittels eines aus drei Achsen bestehenden Schichtenmodells[1]. Komplexe Zusammenhänge können so in kleinere, überschaubare Abschnitte aufgegliedert werden, indem durch Kombination aller drei Achsen zu jedem Zeitpunkt im Lebenslauf eines Assets der jeweils relevante Aspekt dargestellt wird. Die drei Achsen sind:

- Architektur-Achse (Layers) mit sechs Schichten zur Darstellung der für die Rolle des Assets relevanten Informationen;
- Verlauf-Achse (Value Stream) zur Darstellung des Lebenslaufs eines Assets und des Wertschöpfungsprozesses in Anlehnung an die Norm IEC 62890;
- Hierarchie-Achse (Hierarchy Levels) zur Zuweisung funktionaler Modelle zu einzelnen Ebenen in Anlehnung an die Normen DIN EN 62264-1 und DIN EN 61512-1.

Referenzarchitekturmodell Industrie 4.0 (RAMI4.0)

Layers:
Security betrifft alle Ebenen. Risiken müssen ganzheitlich betrachtet werden.

Value Stream:
Security muss über den ganzen Lebenszyklus der Objekte durch den Besitzer betrachtet werden.



Hierarchy Levels:
Alle Objekte/Assets sind Gegenstand der Security-Betrachtungen (Risiko-Analyse) und müssen für ihre Aufgabe und den Schutz relevante Security-Eigenschaften besitzen bzw. bereitstellen.

Quelle: Plattform Industrie 4.0 und ZVEI

Die Abbildung links zeigt die Einbettung der Security im RAMI4.0 in allen drei Achsen und verdeutlicht den integralen Charakter der Security. Sie stellt keine separate Schicht oder zusätzliche Hierarchie-Ebene dar, sondern ist über den gesamten Lebenszyklus auf allen Schichten und Hierarchie-Ebenen wirksam. Vergleichbar mit einem Gebäude, das mit Stahl armiert wurde, gewährleistet die Security damit die Stabilität von RAMI4.0 und schützt gegen mögliche Angriffe.

Hierarchy Levels

Die Hierarchie-Achse bildet im Kern die Automatisierungspyramide mit den unterschiedlichen Komponenten, dem Produkt und der Außenwelt (Connected World) ab. Sowohl in Bezug auf die einzelnen Aspekte als auch für das Gesamtsystem gilt es einen angemessenen Schutzbedarf zu ermitteln. Um dies gewährleisten zu können, muss zunächst eine Risikoanalyse durchgeführt werden. Dazu werden die Bedrohungen und deren Gefährdungspotentiale bestimmt. Aus den Ergebnissen lassen sich Security-Maßnahmen für die jeweilige Industrie 4.0-Komponente ableiten.

Exemplarisch sei eine Maschine (Station) in einer Produktions- oder Prozessumgebung (work unit) genannt. Diese muss eine korrekte und störungsfreie Verarbeitung gewährleisten und die Möglichkeit zum Schutz der Prozesslogik vor unberechtigten Veränderungen, Zugriffen und Auslesen bieten.

Es müssen Bediener identifiziert und dafür ein Berechtigungskonzept mit unterschiedlichen Eingriffsmöglichkeiten spezifiziert werden. Auf Produktionsumgebungsebene gilt es die Mitarbeiter und deren Berechtigungen oder aber auch mehrere Maschinen zu verwalten, entsprechende Aufträge sicher zu übermitteln und deren Abarbeitung zu überwachen.

Value Stream

Security betrifft den gesamten Lebenszyklus, dargestellt als Verlauf-Achse innerhalb RAMI4.0. Sie umfasst die Planung und Entwicklung und setzt sich über die Produktion bis hin zum Einsatz sowie zur Pflege und Wartung fort.

„Security-by-Design“ betrifft alle Beteiligten: Hersteller, Integrator und Betreiber, je nach deren Verantwortlichkeit. Bei der Definition von Standards und bei der Entwicklung von Komponenten muss Security von Beginn an geplant und bedarfsgerecht realisiert werden. Dies betrifft sowohl technische als auch organisatorische Maßnahmen (Prozesse).

Bereits bei der Planung gilt es die notwendigen Security-Funktionen zu berücksichtigen, die aufgrund einer Risikobetrachtung oder als Anforderungen durch andere Komponenten erforderlich sind. Während der Entwicklung und Produktion gilt es konsequent Fehler zu vermeiden, z. B. in Anlehnung an den Security Development Lifecycle (SDL) von Microsoft[2].

Beim Einsatz von Komponenten und Systemen geht es neben der Erfüllung der vorhandenen Security-Anforderungen auch um die Beseitigung von potenziellen Schwächen im laufenden Betrieb. Erforderliche Aktualisierungen müssen zeitgerecht entwickelt, an die Beteiligten verteilt und integriert werden.

1 Referenzarchitekturmodell Industrie 4.0 (RAMI4.0). DIN SPEC 91345.

2 https://www.microsoft.com/en-us/sdl/

Layers

Die sechs Schichten der Architektur-Achse ermöglichen eine systematische Betrachtung verschiedener Aspekte im Rahmen der Herleitung von Security-Anforderungen. Exemplarisch gilt dies für Kommunikations- und Business-Schicht wie folgt: Die Analyse der Geschäftsmodelle auf der Business-Schicht liefert relevante Security-Bedrohungen und -Anforderungen. Auf der Kommunikations-Schicht müssen dann ggf. Maßnahmen zur Verschlüsselung auf der Basis sicherer Identitäten ergriffen werden. Für die Entscheidung, welche Kommunikationsverbindungen schutzbedürftig sind, muss klar sein, welche Informationen darüber übertragen werden.

Zusammenwirken

An allen Schnittpunkten der verschiedenen Ebenen spielt Security eine Rolle. Das heißt, dass sich für jeden Punkt zunächst Anforderungen (Requirements) aus der Analyse ergeben, die auf Basis des konkreten Anwendungsfalls mit entsprechenden Funktionalitäten (Capabilities) seitens der involvierten Industrie 4.0-Komponenten zu beantworten sind. Hersteller, Integrator und Betreiber sind gemeinsam gefordert, um ein holistisches Security-Konzept umzusetzen, das technische und organisatorische Maßnahmen verbindet. Das Design von Security in RAMI4.0 ermöglicht die Umsetzung jeglicher Security-Anforderung für alle denkbaren Anwendungsfälle.

RAMI4.0 ermöglicht die Einbeziehung bereits existierender Security-Standards, insbesondere VDI/VDE 2182 und IEC 62443. In der VDI/VDE 2182 wird z. B. die Rückkopplung der Anforderungen von den verschiedenen Prozessbeteiligten bereits adressiert. Dort wird die Kommunikation zwischen Hersteller, Integrator und Betreiber als wesentlicher Bestandteil für Security beschrieben, so dass die jeweiligen Anforderungen weitergegeben und umgesetzt werden. IEC 62443 skizziert ein Referenzmodell für industrielle Kommunikationsnetze und zeigt auf, wie auf dieser Basis Sicherheitsanforderungen erhoben und Sicherheitstechnologien identifiziert werden können. Sowohl VDI/VDE 2182 als auch IEC 62443 unterstützen ein holistisches Security-Konzept, das sich mit den sogenannten Protection Levels bewerten lassen könnte.

AUTOREN:

Michael Jochem, Robert Bosch GmbH | Wolfgang Klasen, Siemens AG | Lukas Linke, ZVEI | Lutz Jaenicke, Phoenix Contact Cybersecurity AG | Thomas Gamer, ABB AG | Mario Stolz, NXP Semiconductors Germany GmbH | Jens Mehrfeld, Bundesamt für Sicherheit in der Informationstechnik | Andreas Teuscher, Sick AG | Wolfgang Fritsche, IABG GmbH

Impressum

Herausgeber
Bundesministerium für Wirtschaft und Energie (BMWi)
Öffentlichkeitsarbeit
11019 Berlin
www.bmwi.de

Redaktionelle Verantwortung
Plattform Industrie 4.0
Bertolt-Brecht-Platz 3
10117 Berlin

Gestaltung und Produktion
PRpetuum GmbH, München

Bildnachweis
GKSD – Fotolia

Stand
April 2016

Druck
Silber Druck oHG, Niestetal