Mit Sicherheit in der Fertigung kommunizieren

Die Kommunikationstechnologie OPC UA ist ein Standard, der Geräte und Dienste verschiedener Hersteller miteinander verbindet. Der durchgängige Datenfluss von smarten Sensoren, Steuerungstechnik und anderen Geräten der Produktionsebene ist untereinander, aber insbesondere auch zu IT-Systemen der Unternehmensleitebene möglich. OPC UA bietet dabei aus einer generischen Architektur heraus vertikale und horizontale Kommunikation für die gesamte Fabrik und ist deshalb in der Referenzarchitektur Rami 4.0 als einziges Protokoll gesetzt. Darüber hinaus bietet der Standard auch für das Industrial Internet of Things Lösungen, die von Cloud-Anbindung bis zum deterministischen Datentransfer zwischen Steuerungen (SPS) reichen.

Unabhängig vom Datentransport bietet OPC UA ein Informationsmodell. Hierbei handelt es sich um eine Datenbeschreibung basierend auf einem Metamodell, über das sich der Inhalt der Daten standardisieren lässt. Dies ermöglicht unter anderem die Standardisierung von verschiedenen Geräteklassen, zum Beispiel Spritzgussmaschinen oder CNC-Fräsen beziehungsweise deren Repräsentation im Informationsmodell. Weiterhin werden über die Gremien und Branchenverbände – auch außerhalb der klassischen Fabrikautomation – die Informationsmodelle inklusive ihres spezifischen Dateninhalts vereinheitlicht. Dies schafft die Voraussetzung für eine reibungslose Vernetzung aller Systeme, vom Sensor bis zur Cloud.

Zentrale Rolle

Die allgegenwärtige und umfassende Kommunikation zwischen Komponenten spielt in Industrie 4.0-Szenarien eine zentrale Rolle. Für die Absicherung dieser Kommunikation ist der Einsatz eines sicheren Kommunikationsprotokolls wie OPC UA unabdingbar. Das Sicherheitskonzept von OPC UA ist tief in der Architektur verankert. Mit einer Ende-zu-Ende-Verschlüsselung und Signierung wird Datensicherheit und -integrität auf der Transportebene sichergestellt. Hierbei werden asymmetrische (AES) und symmetrische Verfahren (RSA) verwendet und über Zertifikate Vertrauensstellungen von Anwendungen untereinander sowie von Bedienern der Anwendungen abgebildet. Hierfür kommen in der IT etablierte und bekannte Technologien zum Einsatz: PKI mit CAs und x509. Neben der reinen Absicherung des Transports definiert OPC UA zusätzlich auf Applikationsebene weitere Sicherheitsmechanismen. Diese reichen bis hinunter auf einen einzelnen Datenpunkt, für den rollenbasiert Zugriffsrechte vergeben werden können. Das BSI hat jüngst einen Bericht veröffentlicht, indem die Sicherheitsmechanismen von OPC UA geprüft und als sicher beurteilt wurden. Die Software Development Kits (SDK) von Unified Automation bilden die Basis für alle Applikationen, die eine OPC UA-Schnittstelle in ein Gerät oder eine Software integrieren wollen. Die Implementierung der Sicherheitsfunktionen ist in den SDKs als abstrakte Schnittstelle umgesetzt und bietet damit die maximale Flexibilität. Hier lassen sich einschlägige, softwarebasierte Cryptobibliotheken andocken. Es können aber auch hardwarebasierte Varianten mit sicherem Speichermedium bis hin zu kompletten Crypto-Chips angebunden werden, die neben dem sicheren Speicher auch die Cryptoalgorithmik selbst berechnen sowie eine gute Entropiequelle zur Verfügung stellen.

Vielfältige Anforderungen

Wie bei allen Technologien, die als sicher gelten, wird oftmals nicht die Verschlüsselung selbst geknackt, sondern lediglich der Schlüssel gestohlen. Der Faktor Mensch ist die Angriffsfläche, aber auch sein Verhalten bei der Konfiguration und bei der Nutzung von sicheren Systemen. Passwörter sind so lang und kompliziert, dass sie auf einen Zettel geschrieben werden, der am Monitor klebt. Was nützt das dickste Vorhängeschloss, wenn der Schlüssel unter der Fußmatte liegt? Allein durch die richtige Wahl eines sicheren Kommunikationsprotokolls ist eine umfassende Sicherheit noch nicht gewährleistet. Auch wenn der eigentliche Kommunikationsfluss abgesichert stattfindet, muss eine Risikoabschätzung einen unerlaubten Zugriff aus der Ferne berücksichtigen. Auch ein kurzzeitiger physischer Zugriff auf ein Endsystem stellt einen Angriffsvektor dar, der in Industrie 4.0-Szenarien betrachtet und abgeschätzt werden muss. Um diesen hohen Sicherheitsanforderungen gerecht zu werden, wurde die am Markt für IT- und Embedded-Systeme bereits etablierte Schutztechnologie Codemeter von Wibu-Systems erweitert und in die Frameworks zur OPC UA-Softwareentwicklung von Unified Automation integriert. Somit steht nun neben der reinen softwarebasierten Lösung mit Berechnung und Ablage im Dateisystem beziehungsweise in einem speziellen Bereich des Betriebssystems zusätzlich auch eine hardwarebasierte Lösung bereit.

Schlüssel in der Hardware

Der Schutz des eingesetzten kryptografischen Materials stellt einen wichtigen Schritt bei der Absicherung gegen Angriffe dar. Insbesondere die sichere Verwahrung von privatem Schlüsselmaterial steht hier im Vordergrund. Durch den Einsatz von CodeMeter-Hardware-Sicherheitsmodulen kann dies gewährleistet werden. Sogenannte CmDongles können in vielfältigen Bauformen wie USB, (Micro-)SD-Card, CFast, CF oder auch direkt als ASIC in das System integriert werden. Durch eine Speicherung des privaten Schlüsselmaterials im CmDongle ist sichergestellt, dass diese Daten nicht wieder vom Dongle ausgelesen werden können. Im Vergleich zu einer Speicherung des privaten Schlüsselmaterials direkt im System stellt dies eine erhebliche Steigerung der Sicherheit des Gesamtsystems dar. Das private Schlüsselmaterial kann somit nur dann entwendet werden, wenn auch der physische CmDongle entwendet wird.

Software und Konfiguration

Betrachtet man jedoch einen Angreifer, der lokale Administratorrechten oder gar kurzzeitigen physischen Zugriff erlangt hat, so kann dieser dennoch erheblichen Schaden verursachen. Einfache Änderungen an den lokal vorhandenen Konfigurationsdaten, wie zum Beispiel der Liste der vertrauenswürdigen Systeme, können die Sicherheit des Gesamtsystems gefährden. Neben einfach zu entdeckenden Angriffen mit direktem Schaden sind aber auch langfristig angelegte Angriffe durch schwer entdeckbare Manipulationen am System denkbar. Mittels des Softwareschutzes der CodeMeter-Technologie kann dieser Angriffsvektor ausgeschlossen werden. Die so manipulationsgeschützte Anwendung kann eine Überprüfung der Integrität und Authentizität ihrer Konfigurationsdaten durchführen. Der Manipulationsschutz stellt hierbei ein entscheidendes Detail der Sicherheitslösung dar, denn bei einer nicht manipulationsgeschützten Applikation kann die Prüfung auf Integrität und Authentizität von Konfigurationsdaten einfach umgangen oder entfernt werden.

Security-in-Depth

Die OPC UA-Technologie bringt mit ihrem Security-in-Depth-Konzept alle Voraussetzungen mit, um in Industrie 4.0-Anwendungen einen durchgängigen und sicheren Informationsaustausch zu gewährleisten. Die Vielfältigkeit der Anforderungen und Einsatzszenarien vor allem unter der Berücksichtigung des ‘Faktors Mensch’ erfordert es, die Beherrschbarkeit der Sicherheitsfunktionen für den Anwender möglichst einfach zu gestalten. Die OPC UA-SDKs von Unified Automation bieten die Flexibilität, neben reiner Software auch Mischvarianten oder gar vollständige Hardware - Kryptographie umzusetzen, je nach Anwendungsfall und Einsatzzweck. Wibu-Systems liefert mit seiner CodeMeter-Technologie und dem CmDongle einen sicheren Speicher für private Schlüssel und Trustlisten, wie sie OPC UA-Anwendungen verwenden. Mit der Erweiterung der Schnittstellen ist nun eine Kombination von Unified Automation SDK mit dem Dongle möglich, der die Nutzbarkeit und Beherrschbarkeit der Zertifikate in einer PKI deutlich erleichtert und dabei gleichzeitig eine deutlich erhöhte Sicherheit bietet, da die Schlüssel sicher gespeichert sind.

Die Autoren: Dr.-Ing. Sören Finster arbeitet bei der Wibu-Systems AG und Gerhard Gappmeier arbeitet bei der Unified Automation GmbH.

Internet: www.wibu.com

IT&PRODUCTION, PRODUCTION Oktober 2016 Blickpunkt Automation-IT

Lesen Sie auch:

Sichere Informationstechnologie
Was braucht die Cloud?
Sie ist der Wegbereiter für die digitale Wirtschaft: die Cloud. Flexible IT-Services on demand können Flexibilität und Kosteneffizienz schaffen. Ganze Prozessketten basieren mittlerweile auf Cloud-Infrastrukturen ...

Pragmatische Lösungen gefragt
Security-Konzepte für Automatisierung und Produktion
Das Thema Security ist in der Automatisierung und Produktion angekommen. Doch vielfach werden punktuelle Aspekte und Maßnahmen fokussiert. Die Herausforderung bei der Sicherstellung der Informationssicherheit ...