Ergebnisvermerk: Workshop „IT-Sicherheit“ am 18.06.2014

Ort: Neue Mälzerei, Friedenstraße 91, 10249 Berlin

Agenda

1. **Zusammenfassung HMI-Workshop und Zielsetzung des Tages** (Dr. Daniel Willkomm, [Institut für Innovation und Technik])
2. **IT-Sicherheit in vernetzten Produktionssystemen und CPS – Aktuelle Erfahrungen und Herausforderungen (**Dr. Carsten Rudolph, [Fraunhofer SIT])
3. **Bisherige Ansätze der IT-Sicherheit (und erste Erfahrungen) in den Autonomik 4.0-Projekten: Use Cases, Risiken und Maßnahmen, Technologien, Standards, offene Fragen**
4. **Vorschlag für die Erstellung eines Leitfades**

---

1. Zusammenfassung HMI-Workshop und Zielsetzung des Tages

Siehe Vortragsfolien.

2. IT-Sicherheit in vernetzten Produktionssystemen und CPS – Aktuelle Erfahrungen und Herausforderungen

Siehe Vortragsfolien.

Diskussion:

Use cases

Die Komponenten sind autonome Geräte. Legacy-Geräte mit einem Alter von 20–30 Jahren müssen berücksichtigt werden. Maschinenadressen (MAC) können gefälscht werden und liefern per se keine nicht fälschbare Identitäten.
Es werden alle üblichen Kommunikationsarten der Büro- und der Industrial IT genutzt, Netzwerktopologien ändern sich spontan, z. T. gibt es Vernetzungen mit der Büro-IT.

Risiken & Maßnahmen

Derzeit gibt es keinen allgemeinen Katalog der Sicherheitsrisiken autonomer Systeme in der Produktion. Beispiel: Im Landmaschinenbau dienen die Log-Daten der Maschinen als Nachweis gegenüber der EC für die Gegenleistungen zu Subvention. Diese Dateien können gefälscht werden, eigentlich wäre ein digitaler Nachweis der Log-Dateien notwendig.

Technologien

Viele Standardtechnologien sind für den Einsatz in autonomen Produktionssystemen nicht geeignet. Beispiel: In den USA vertreibt ein Hersteller drahtlose Router für den Einsatz in Produktionsumgebungen, obwohl sie nicht für Ad-hoc-Netze geeignet sind.

Die Abgrenzung des Perimeters zwischen drinnen und draußen ist bei Firewalls und VPN ein tragendes Konzept, kann in Produktionssystemen aber teilweise nur schwer definiert werden (Beispiel Fernwartung).

Beim Virenschutz ist ein „black-listing-Ansatz“ nicht geeignet, notwendig wäre eher ein „white-listing“ der erlaubten Systeme.

Intrusion Detection: Gegenüber heutigen Systemen in Büroumgebungen gibt es andere Nutzungsmuster und andere Geräte. Zum Teil sind auch andere Reaktionen verlangt. Beispiel: Es ist ggfs. günstiger, ungefährliche Banking-Viren auf einem Produktionssystem zu belassen als die Produktion für die Reinigung zu unterbrechen.

Trusted computing könnte eine geeignete Basis für eine Hardware-basierte IT-Sicherheit einschließlich der Identifikation sein.

Standards

OPC UA deckt nur die Kommunikationsschicht ab, andere Schichten werden nicht berücksichtigt.

<u>Offene Fragen:</u>

- Es fehlt derzeit ein Katalog an typischen Sicherheitsanforderungen
- Ebenso fehlen Engineering-Prozesse für das security by design
- Notwendig wäre eine Referenzplattform (oder Referenzgeräte)
- Methodisch ist offen, ob echtzeitfähige Systeme (Sensorik und Aktuatorik in der Produktion) mit nichtechtzeitfähigen Systemen (Backend in der Cloud) sicherheitstechnisch integriert werden können
- Die internationalen Rechtssysteme definieren zum Teil unterschiedliche Anforderungen, z. B. den Grad der erlaubten Überwachung von Arbeitnehmern
- Der Austausch zwischen Unternehmen zu Sicherheitsangriffen ist noch unzureichend organisiert.

3. Bisherige Ansätze der IT-Sicherheit (und erste Erfahrungen) in den Autonomik 4.0-Projekten: Use Cases, Risiken und Maßnahmen, Technologien, Standards, offene Fragen

Projekt FTF out of the box

Use case ist die innerbetriebliche Logistik mit Staplern. Das Fahrzeug erhält den Transportauftrag per Gestensteuerung vom Bediener und fährt die Route autonom. Es gibt keinen externen Zugriff auf das System, die Routen werden auf dem Fahrzeug berechnet.

Risiken sind die Sabotage des Systems, z. B. durch High-jacking des Fahrzeugs, der innerbetriebliche Zugriff auf das System, der Zugriff auf personenbezogene Daten des Bedieners oder anderer Mitarbeiter, die zufällig erfasst werden, der Diebstahl von Datenbanken und Software.

Es werden nur Standardtechnologien eingesetzt, insbesondere Middleware-Systeme wie z. B. ROS.

Offene Fragen

- Kann das Prototypsystem mit ROS später auch im Operativbetrieb verwendet werden?
- Wie ist der Zusammenhang zwischen IT-Sicherheit und funktionale Sicherheit?

Wunsch wäre ein Leitfaden mit technischen und organisatorischen Umsetzungsmöglichkeiten.

Projekt CoCos

Use case ist das standort- und unternehmensübergreifende plug-and-play von Maschinen mit dynamischen Netztopologien. Vordringliche Aufgabe ist die Beherrschbarkeit der komplexen Situation in Fehlerfällen und die Abwehr von Komponenten, die unerlaubt eindringen.

Es werden Standardtechnologien eingesetzt. Der Einsatz von software defined networks ist angedacht.

<u>Offene Frage:</u>

- Bei software defined networks drohen neue Angriffsszenarien

Projekt SmartSite

Use case ist die Cloud als Kommunikationsplattform, die Asphaltswerk, LKW, Verdichtungswalze, etc. ad-hoc-vernetzt. Es gibt mobile Apps für Poliere und andere Mitarbeiter. Die Maschinen werden z. T. ferngewartet, einige Maschinen agieren teilautonom , z. B. die Walzen bei der Asphaltaufbringung.

Darüber hinaus gibt es eine Vernetzung mit externen Planungs- und CAD-Systemen. Hier ist der Schutz der Kalkulation- und Planungsdaten vor anderen Unternehmen wichtig.

Die Cloud-Lösung wird vom Projekt AutoBauLog übernommen. Es gibt im Projekt noch keine spezifischen Sicherheitskonzepte.

Projekt Speedfactory

Speedfactory ist für adidas ein strategisches Projekt über den Zeitraum von fünf bis zehn Jahren, das zu einer Disruption der Fertigungstechnik führen kann. Daher steht der Know-how-schutz im Kern des Projekts.

Relevante Risiken sind Hackerangriffe und eine zu enge IT-Vernetzung mit anderen Unternehmen, die z. T. unerwünscht ist.

Eingesetzt wird Sharepoint, die externen Partner werden über VPN angebunden. Adidas Global IT setzt ein internes Team auf, um die IT-Sicherheit für den IP-Schutz in Speedfactory zu analysieren und Lösungsansätze zu formulieren.

Projekt Innocyfer

Relevante Risiken sind Angriffe auf vernetzte Systeme, um einen allgemeinen Zugriff auf vernetzte Systeme zu gewinnen, um gezielt IP abzugreifen (auch relevant für das Querschnittsthema Recht) oder um den Open-Innovation-Prozess zu stören.

Absichtlich falsch designte Produkte können die Fertigungsanlagen schädigen.

Gefälschte Beteiligungen im Prozess können auch darauf abzielen, Kapazitäten und andere Betriebsgeheimnisse der Fertigung auszuforschen.

Projekt GEMINI

Use case ist eine Plattform für die Verteilung von Aufträgen an einen Pool von additivem Fertigungsmaschinen.

Risiken sind die üblichen Sicherheitsrisiken bei Cloud-Systemen gefälschte Identitäten von Maschinen die Abfrage von Kapazitäten (wie bei Innocyfer)

Projekt Smartface

Use case ist die dezentrale Produktionsplanung. Später angedacht sind autonome Fertigungsstationen und Cloudservices.

Projekt OPAK

Use case ist das funktionsorientierte Engineering von Automatisierungsanlagen. Dabei wird Software auf allen Ebenen eingesetzt, vom Sensor bis zur Fertigungszelle.

Zentrales Risiko sind die Identifikation und Authentifizierung der Komponenten, damit z. B. nicht gefälschte Ersatzkomponenten in das System kommen. Ebenso ist der IP-Schutz der Software auf den Komponenten gefährdet.

Im Kern werden Automatisierungsgeräte mit Software eingesetzt. Es wird über eine TPM-Lösung nachgedacht, um eine Authentifizierung der Komponenten zu erreichen. Denkbar ist auch eine Zertifizierung der Komponenten.

4. Vorschlag für die Erstellung eines Leitfades

Ein Leitfaden sollte sich insbesondere an die Zielgruppe Mittelstand richten. In die Arbeiten sollten auch andere Leitfäden, etwa der Plattform Industrie 4.0, mit einbezogen werden. Auch der Industrie 4.0-Leitfaden von der Acatech, inklusive der dortigen Struktur der use cases sollte aufgegriffen werden.

Der Austausch zu IT-Sicherheit ist Aufgabe der Projekte. Die Begleitforschung moderiert diesen Prozess wenn sich besondere Bedarfe ergeben, sie erstellt aber keine spezifische Lösung für einzelne Projekte.

Notwendig erscheint eine gemeinsame Sicherheitsanalyse der Projekte.

Alle Projekte befinden sich jetzt in Analyse- und Konzeptionsphase, die Arbeiten werden zeitnah erfolgen. Auch die jetzt nicht vertretenen Projekte sollen nach Möglichkeit zur Mitarbeit in der Gruppe bewegt werden.