Gibt es sichere Software?

Dr. Thomas Liedtke, Prof. Dr. Bernhard Hohlfeld

thomas.liedtke@ics-ag.de,
bernhard.hohlfeld@ics-ag.de

Abstract: Steigender Komplexität in Industrie 4.0- und Big Data-Themen erfordern neue Lösungskonzepte. So werden Security-Themen normativ größtenteils noch stiefmütterlich behandelt. Der Vortrag beleuchtet Konzepte der IT-Security (Angriffssicherheit) in Abgrenzung zu Safety (Betriebssicherheit).

Der Vortrag ist in drei Blöcke strukturiert. Nach einer Motivation mit Beispielen wird auf den Unterschied zu Safety eingegangen. Am Ende soll der derzeitig Stand des Themas Security bei Mensch und Technik zusammengefasst werden, insb. das Umfeld und Ziele der z.Zt. entstehenden Normen..

1 Motivation

Spätestens seit dem SCADA-Maroochy-Abwasserunfall in Australien, der erfolgreichen Attacke auf Autos durch Malware-behaftete MP3-Dateien, den ersten von einem Kühlschrank versendeten Spam-E-Mails, ist in unserer Gesellschaft das Bewusstsein allgegenwärtiger IT-Security sprunghaft gestiegen. Der menschliche Faktor den Wert von Sicherheit (erst) dann zu erkennen, wenn sie nicht mehr gewährleistet ist, treibt auch hier den Stand der Technik.

Für Industrie 4.0-Anwendungen werden Anforderungen an technische Systeme stetig komplexer:

- Dezentralisierung von Steuerungen: Energiegewinnung/-verteilung, wachsender Einsatz "SMARTer"/unterschiedlichster Endgeräte, MES, Car2x, einfachste Funktionen werden über mehrere Steuergeräte verteilt, Steuergeräte kommunizieren über immer mehr Kommunikationskanäle/Busse miteinander, ...

- Neuartige unterschiedlichste Endgeräte und Bedienungskonzepte: Flexible Tablet-Steuerung einer begehbaren Maschine, …

- Erhöhte Anzahl von Sicherheitslücken. Jede neue Technologie, die Sicherheitslücken schließt, bringt neue mit sich. Anlagensteuerungen/-wartungen über Cloud-Rechenzentren

- Anlagenlebenszeiten werden länger, umgekehrt zu Software und Betriebssystemen

2 IT-Security und/ oder Safety

Je nach Domäne, Anwendungsfall und erfüllender (Sicherheits-) Funktion spricht man der Software einen bestimmten Safety Integrity Level zu. Das jetzt noch enthaltene Restrisiko wird (vom Mensch) akzeptiert. Bei Security spricht man von einem Evaluation Assurance Level, der die kriminelle Energie, die notwendig ist um ein System zu gefährden berücksichtigt. Zielwerte bei Safety und Security sind untereinander abhängig und tlw. sogar orthogonal (z.B. geschlossene Türen in Auto und Flugzeug).

Safety braucht Security. Umgekehrt darf Security Safety nicht stören. Was z.B. wenn bei einem Störfall eines weit entlegenen dezentralen Energiekraftwerks dem helfen wollenden Servicetechniker im Stress Passwort und Schlüssel für den entsprechenden Zugriff entfallen sind?

3 IT-Sicherheit

Spricht man von IT-**Sicherheit** meint man i.d.R. IT-**Security**. Im Gegensatz zu Safety gelten für Security tlw. ganz andere Randbedingungen:

- Schutzziele müssen zunächst definiert werden. Diese sind nicht automatisch gleich Mensch, Leib, Leben und Umwelt, sondern können z.B. auch Geld, zu schützendes Wissen und ein ausfallfrei laufender Online-Service sein (s. DoS).

- Eine Sicherheitslücke in der IT-Sicherheit wird – einmal bekannt – mit großer Wahrscheinlichkeit auch ausgenutzt werden. Bekannte Lücken müssen also schnell geschlossen werden und können nicht statistisch erfasst werden (i.G. zur Regelmäßigkeit eines Tsunamis der Stärke acht…)

- Eine Gefährdung wirkt nicht zufällig vom System auf seine Umwelt (z.B. der Airbag, der ohne Aufprall während einer Fahrt aufgeht), sondern die Umwelt (z.B. ein Mitarbeiter mit entsprechendem Knowhow und Motivation) attackiert ein System absichtlich um es zu „überlisten“.

- Fehlverhalten sind meist Ergebnisse von Angriffen über mehrere (Zwischen-) Stufen und nicht unabhängig. Sie können deshalb mit konventionellen Safety-Methoden nicht offenbart werden

- Ein attackiertes System soll unter allen Umständen weiterhin funktionieren. Ein sicherheits-gerichtetes System (im Sinne von Safety) muss einen sicheren Zustand erreichen (Flugzeug landet, Zug hält auf offener Strecke, ...).

Im Gegensatz zu Normen, die seit vielen Jahren die Sicherheit in Bezug auf Safety regeln (insb. IEC 61508, abgeleitete, sowie RTCA DO 178B/C et. al.) sind Normen

bezugnehmend auf Security erst noch im Entstehen. So gibt es derzeit vielfältige Ansätze aus unterschiedlichen Blickwinkeln:

- Common Criteria (ISO/ IEC 15408) versucht international Kriterien zur Sicherheits-Evaluierung von IT-Technik zu harmonisieren. Inzwischen ist ein umfangreicher Katalog zur Spezifikation von Sicherheitsanforderungen entstanden, der eine Vergleichbarkeit der Ergebnisse von Evaluierungen herstellen soll (Bsp. Bahntechnik)

- Entwicklungsprozessreife. Ähnlich wie SPICE oder CMMI gibt es Ansätze notwendige Prozesse für die IT-Sicherheit zu definieren (SAMM, BSIMM, SDL, …) und deren Erfüllung einer Reifegradstufe zuzuordnen

- Zertifizierungen: Beim BSI kann man Organisationen und Produkte basierend auf den Normen 27k ähnlich zur ISO-9000 zertifizieren lassen

- ISA 99/ IEC 62443 versucht einen Ansatz analog zu SIL-Einstufungen SAL (Security Assurance Level) vorzunehmen. Parameter sind hier Angriffe/ Hilfsmittel/ Wissen/ Ressource und Motivation.

Derzeit verfolgte Lösungskonzepte betreffen insbesondere

- konsequente(re)s "Security by Design" (durch Norm geregelt)

- Standardisierung von Protokollen wie z.B. OPC UA

- Schulung/ Know-How- und Bewusstseinserhöhung

Am Ende des Vortrags wird beispielhaft die Methodik CORAS (Cost Risk Analysis) vorgestellt, mit der sich ganzheitlich ein Prozess von der Definition von Schutzzielen bis zur Identifikation und Priorisierung von Risiko-Maßnahmen grafisch modellieren lässt. Sie visualisiert Risikobewertungen und hilft damit ein gemeinsames Verständnis zu bekommen.