Halle 10.0
Stand 314

Bild: David Goffin

Sichere Feldgeräte in der Industrie auch 'secure'?

Die Zeiten, in denen Industrieanlagen monatelang unverändert vor sich hin arbeiteten, sind vorbei: heute sollen Prozessdaten kontinuierlich über das Internet überwacht und in die Cloud transportiert, Prozessparameter kontinuierlich modifiziert und optimiert werden. Wenn sich Automatisierungssysteme zur Welt öffnen, entstehen neue Gefahren: Neben Spionage und Sabotage, können auch Leib und Leben bedroht werden. Dieser Artikel geht der Frage nach, wie sich das Thema 'Security' auf funktional sichere Komponenten auswirkt, die solche Gefährdungen verhindern sollen. Gibt es bei dem Thema 'Industrial Security' Fragen, die besonders die Entwicklung funktional sicherer Komponenten betreffen?

Auszug aus der EMBEDDEDDESIGN, Smarte Systeme für das Internet of Things, Ausgabe 6/2016.

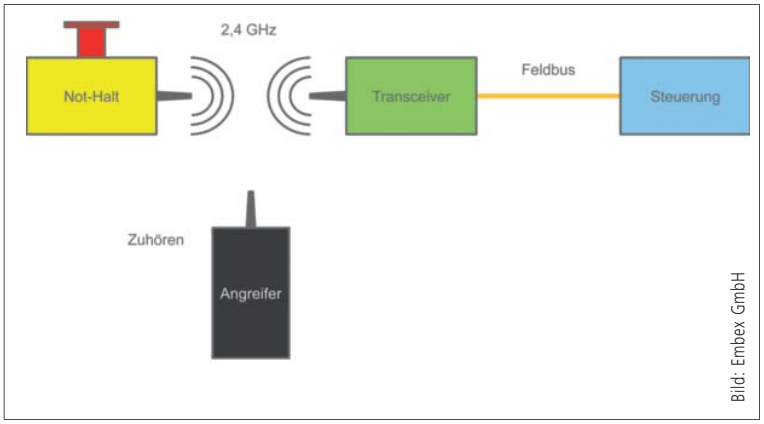

Abb. 1: Funk-Nothaltschalter im Normalbetrieb: Der Angreifer hört der Kommunikation zu, ohne selbst aktiv zu sein.

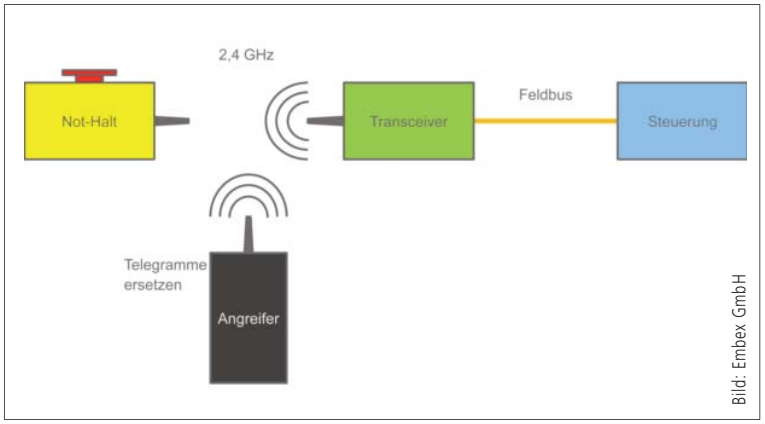

Abb. 2: Funk-Nothaltschalter gedrückt: Der Angreifer sendet nun weiter die vom Transceiver erwarteten Nachrichten.

Authentifizierung

Inzwischen gibt es eine Vielzahl von Untersuchungen und Veröffentlichungen zur Bedrohung von industriellen Automatisierungssystemen durch Angriffe Dritter. Auffällig daran ist, dass bei den allermeisten theoretischen Szenarien wie tatsächlich geschehenen Angriffen Authentifizierungsmaßnahmen unzureichend vorhanden oder nicht genutzt wurden. So funktioniert z.B. der in [1] beschriebene Wurm nur, wenn eine Authentifizierungsabfrage in der betroffenen SPS deaktiviert ist (was leider defaultmäßig der Fall ist). Für die Designer und Entwickler funktional sicherer Komponenten bedeutet dies vor allem, für die Änderung von sicherheitskritischen Parametern oder für Firmwareupdates zwingend mindestens eine Passwortabfrage zu implementieren. Für solche Komponenten wäre es beispielsweise eine sinnvolle Maßnahme, die Übertragung von sicherheitskritischen Messsignalen oder die Aktivierung sicherheitsrelevanter Ausgänge erst dann zuzulassen, wenn das Defaultpasswort geändert wurde. Weitere Maßnahmen, die zu erwägen sind, wären

- Rechtegranulierung
- Zweifaktorenauthentifizierung, wenn das Gerät auch per Internet parametrierbar ist

Zu beachten ist in jedem Fall, dass eine Bedrohung nicht nur über das Internet besteht. Ein Angreifer kann sich möglicherweise auch Zugang zu einer Geräteschnittstelle verschaffen, um sicherheitsrelevante Parameter zu manipulieren. Auch für solche Schnittstellen (z.B. USB) muss ein Passwortschutz implementiert werden.

Man-in-the-middle-Attacken

Unter einer Man-in-the-Middle-Attacke versteht man einen Angriff, bei dem der Angreifer Nachrichten abfängt und sie, ohne

dass das für den eigentlichen Empfänger erkennbar ist, mitliest (was zunächst keine unmittelbare Gefährdung bedeutet), ändert oder sogar eigene Nachrichten erzeugt, die für den Empfänger als echt erscheinen. Besonders anfällig für eine solche Bedrohung sind Kommunikationsmedien (wie Funk oder das Internet), die per se zumindest physikalisch für andere zugänglich sind. Ein Beispiel für einen solchen Angriff soll im Folgenden skizziert werden. Es handelt sich dabei um einen Funk-Nothaltschalter, wie er z.B. bei der Wartung von Maschinen eingesetzt werden könnte, bei denen der Wartungstechniker nicht immer einen festverdrahteten Nothaltschalter erreichen kann. Die Funktion dieses Nothaltschalters ist denkbar einfach. Solange der Schalter nicht gedrückt ist, sendet das Gerät kontinuierlich vordefinierte Telegramme an einen Transceiver, der daraufhin über einen Feldbus ein OK-Signal an eine (Sicherheits-)SPS schickt. Wird der Schalter gedrückt, hört das Gerät auf, Telegramme zu senden und nach einer definierten Timeout-Zeit sendet der Transceiver ein Stop-Signal an die SPS. Ein Angriff wäre nun folgendermaßen vorstellbar: ein Angreifer hört im Normalbetrieb die vom Nothaltmodul gesendeten Signale mit (siehe Abbildung 1). Die Nachrichten enthalten wahrscheinlich eine laufende Nummer und mindestens eine Sender- und/oder Empfängeradresse. Deren Struktur ist relativ leicht zu identifizieren. Wenn der Wartungstechniker nun den Nothaltknopf betätigt, weil eine akute Gefährdung besteht, so hört das Nothaltgerät auf, Nachrichten zu senden. Gleichzeitig kann aber der Angreifer, der die Struktur der vom Transceiver erwarteten Nachrichten kennt, diese Nachrichten seinerseits weitersenden (siehe Abbildung 2) – die Maschine läuft weiter. Der Aufwand für einen solchen Angriff ist überschaubar: es muss lediglich eine solche 'Angriffsbox' in der Nähe der angegriffenen Maschine installiert werden. Dieser Angriff macht sich eine spezifische Eigenschaft funktional-sicherer Geräte zunutze: wenn sie einen Fehler erkennen (oder, wie im Beispiel, eine Anforderung der Sicherheitsfunktion aufgetreten ist), nehmen sie einen sicheren Zustand ein. In der Regel bedeutet das auch: sie hören auf zu kommunizieren. Ein Angreifer kann sich dies zunutze machen, indem er, wie im Beispiel, auf die Anforderung der Sicherheitsfunktion wartet, oder indem er gezielt das Gerät in seinen sicheren Zustand versetzt, um gleichzeitig dem Empfänger seinerseits gültige Nachrichten zu senden. Die Maßnahme gegen einen solchen Angriff wäre eine sichere Signatur oder eine kryptographische Prüfsumme, d.h. eine Information, die sich durch das Abhören der Kommunikation nicht in endlicher Zeit reproduzieren lässt. Nach heutigem Stand der Technik hätte diese Signatur eine Länge von mindestens 128, besser 256bits. Dies setzt dann sowohl eine höhere Bandbreite als auch einen erhöhten Rechenaufwand bei Sender und Empfänger voraus. Oder, wenn, wie im Beispiel, Übertragungsweg und Batteriegröße gegeben sind: die Laufzeit des Gerätes wird geringer und die Fehlertoleranz und/oder die sichere Reaktionszeit des Systems verschlechtert sich.

Safety vs. Security

Mit funktionaler Sicherheit (Safety) und Security treffen Welten aufeinander: in der Zeit, die es braucht, funktional sichere Software zu verifizieren und abschließend zu zertifizieren, bekommt Ihr Windowsrechner zu Hause mindestens 20 Securityupdates. Fast täglich werden Schwachstellen in den verbreiteten IT-Systemen (Windows, Android, iOS) bekannt, und es ist nur eine Frage der Zeit, bis ein ähnlicher Effekt auch bei den industriellen Systemen (Feldbus-Stacks, Steuerungen der großen SPS-Hersteller) eintritt. Das heißt, in Zukunft werden die SPS-Hersteller, die Anbieter von Feldbusstacks in immer kürzeren Zyklen Updates ihrer Firmware ihren Kunden anbieten müssen. Dass in gleichem Maße der Aufwand abnimmt, um funktional sichere Software zu verifizieren und zertifizieren, ist nicht anzunehmen. Das kann nur eines bedeuten: in funktional sicheren Geräten müssen Safety und Security konsequent getrennt werden. Es muss möglich sein, die Kommunikationskomponenten monatlich, wenn nicht wöchentlich zu aktualisieren, ohne dabei die funktional sicheren Komponenten zu beeinflussen. Im einfachsten Fall heißt das, dass das funktional sichere Gerät ein separates Kommunikationsmodul enthält, das die Kommunikation über einen sicheren Feldbus oder mit dem Internet kapselt. Falls in dem Gerät einer der immer häufiger eingesetzten Safety-Prozessoren eingesetzt wird (die i.d.R. auch über eine Ethernetschnittstelle verfügen), so muss durch die Softwarearchitektur sichergestellt sein, dass ein Update der Kommunikationsschnittstellen keine Auswirkung auf die funktional sichere Software hat. Dies kann auch als Hinweis an die verschiedenen Feldbusnutzerorganisationen verstanden werden, die wahrscheinlich alle derzeit damit beschäftigt sind, Securityprofile zu spezifizieren (auch wenn davon wenig nach außen dringt): so verführerisch der Gedanke sein mag, eine erforderliche Signatur mit der sowieso schon vorhandenen Checksumme der Safety-Protokolle zu verheiraten: hier sollte eine strikte Trennung erfolgen, da ansonsten ein Teil der Sicherheitsfunktion in die Kommunikationslayer des Feldbusses übertragen wird mit allen Folgen bezüglich Verifikation und Zertifizierung, die damit verbunden sind.

Zusammenfassung

- An allen Schnittstellen, an denen funktional sicherheitsrelevante Parameter geändert werden können, müssen wirksame Authentifizierungsmechanismen implementiert werden.
- Sicherheitsrelevante Nachrichten brauchen eine Signatur oder kryptographische Prüfsumme, die sich in endlicher Zeit nicht reproduzieren lässt.
- Kommunikationskomponenten, die Securityfunktionen beinhalten, und funktional sichere Komponenten müssen strikt getrennt werden, da ihre Updatezyklen völlig unterschiedlich sind und sich in Zukunft eher auseinanderbewegen werden. ■

[1] Maik Brüggemann, Ralf Spenneberg:
PLC-Blaster – Ein Coputerworm für PLCs.
https://www.youtube.com/watch?v=9ZvtbsMshnQ
(27.12.2015)

Autor:
Dr. Martin Lange,
Leiter Geschäftsbereich Safety in Automation,
embeX GmbH
www.embex.de

Auszug aus der EMBEDDEDDESIGN, Smarte Systeme für das Internet of Things, Ausgabe 6/2016.