Security-und Safety-Feldbusse
Das Wie und Warum von Security-Maßnahmen

Max Perner, infoteam Software AG

Security auf Feldbussen ist notwendig, möglich und sinnvoll. Der theoretische Ansatz von „Security by Design“ und das Konzept „Defense in Depth“ wird in der Praxis häufig vernachlässigt, obwohl vor allem bei eingebetteten Systemen im Bereich von Industriesteuerungen die Angriffssicherheit derzeit stark in den Fokus gerückt ist. Grund dafür sind sowohl neue „Security Standards“ als auch seit langem etablierte Normen der Funktionalen Sicherheit.

Motivation
Normen der Funktionalen Sicherheit (Safety), wie die IEC 61508 als auch Normen des Angriffsschutzes (Security) wie die IEC 62443, fordern den Ansatz „Security by Design“. Häufig findet dann allerdings eine Ausklammerung der Komponentenlieferanten im Bereich der OT (Operational Technology) statt. Gleichzeitig wird der Versuch unternommen, Netzwerksicherheit durch Kapselung mithilfe von Firewalls zu erreichen [1]. Am Beispiel von Feldbussen soll aufgezeigt werden, dass alle Komponenten einer Industrieanlage einen Beitrag zur Gesamtsicherheit leisten können.

(Safety)-Feldbusse in der Anwendung
Feldbusse dienen der Vereinheitlichung von Infrastrukturen. Sie wurden eingeführt, um Parallelverdrahtung und analoge Signalübertragung zu ersetzen und Vorteile der digitalen Übertragung zu nutzen [2]. Aufgesetzte Protokolle wie PROFIsafe ermöglichen Sicherheitsfunktionen durch das Erkennen zufälliger Veränderungen am Datenstrom. Der Security-Aspekt wird an dieser Stelle bisher nur in Ausnahmefällen berücksichtigt [3] .

Ein Angreifer, der über einen Feldbus gezielt Schadcode in ein Unternehmensnetz bringen will, wird das verwendete Übertragungsprotokoll beachten, verwenden und missbrauchen. Ohne Security-Maßnahmen können die Empfänger in diesem Fall nur von einem legitimen Sender ausgehen, da keine Möglichkeit besteht, den Angriff als solchen zu erkennen.

Ziel der Security
Das Ziel von Security bezieht sich immer auf andere Systemkomponenten, deren Funktionalität geschützt werden muss. Es werden die Anforderungen an die zu schützenden Komponenten eines Systems analysiert und unter dem Blickwinkel böswilliger Absicht auf Verwundbarkeiten untersucht. In der Folge können Maßnahmen getroffen werden, die diese Verwundbarkeiten „mindern“. Auf diese Weise können Lücken geschlossen oder Schwachstellen überbrückt werden.

CIA - Triade
Abstrakte Schutzziele helfen es, in konkreten Situationen den Überblick über das System zu behalten. Sie helfen, getroffene Maßnahmen zu klassifizieren und strukturiert vorzugehen. Ein häufiges Beispiel ist die CIA-Triade [4].

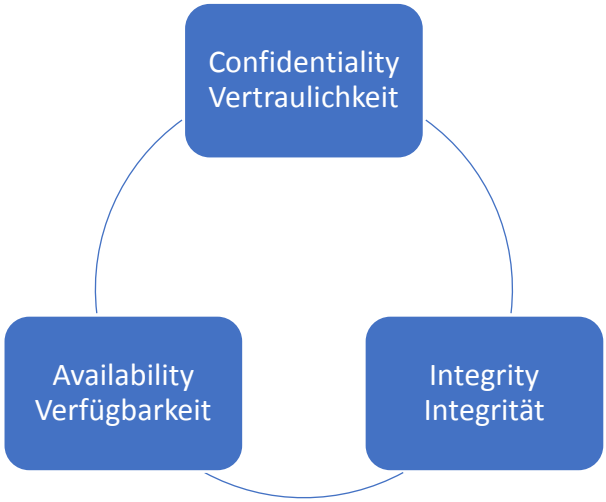

Abb. 1: CIA Triade [4]

Zu klassifizieren wären zum einen Assets [5], also materielle und immaterielle Werte, die bedroht sein können und schützenswert sind. Dies wären z. B. Produktionsdaten (genauer: die Vertraulichkeit von Produktionsdaten). Auch Schutzmaßnahmen wie Authentifizierungscodes zur Integritätssicherung von Daten können so eingeordnet werden, und auch Angriffe z. B. „Denial of Service“ durch falsche Dienstanfragen auf die Verfügbarkeit.

Foundational Requirements
Die DIN IEC 62443 [6] als Norm für System Security auf Industrie Netzwerken erweitert die drei sehr abstrakten Schutzziele der CIA-Triade, um für ein besseres Verständnis der Security-Anforderungen an IACS (Industrial Automation and Control Systems) zu sorgen. Von diesen sieben Foundational Requirements leitet diese Norm dann konkrete Sicherheitsanforderungen an die betrachteten Systeme ab.

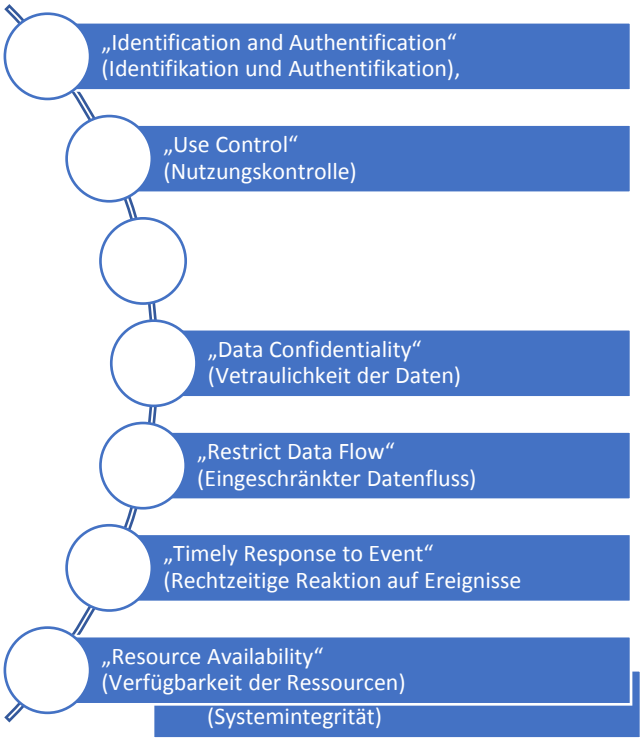

Abb. 2: Foundational Requirements [4]

Defense in Depth
Das Entwurfskonzept „Defense in Depth“, zu Deutsch „geschachtelte Verteidigung“, besteht aus zwei Mustern: Zum einen soll jedes Schutzziel auf jeder Ebene eines Systems möglichst unabhängig gesichert werden, zum anderen können Schwächen auf einer Ebene durch andere Ebenen aufgefangen werden.

Security auf Feldbussen
Im Fall von Feldbussen wird deutlich, wie diese von Normen [5] [7] geforderten Abstraktionen Realität werden:
Einerseits gibt es einen Teilbereich, der möglicherweise sinnvoll an die Vertrauensgrenze des Feldbussystems zur angeschlossenen IT-Infrastruktur delegiert werden kann: der Schutz der Vertraulichkeit. Beispielsweise in der Fertigung sollten alle an einem Werkstück beteiligten Akteure wissen, woran sie arbeiten und in welchem Kontext die Meldungen der Sensoren zu interpretieren sind. In Fällen, in denen der Schutz vertraulicher Informationen auf dem Feldbus für nötig befunden wird, gilt dies nicht, z. B. beim Prototypen-Schutz im Hinblick auf Industriespionage [8] .
Anderseits sollten Gefahren im Hinblick auf Verfügbarkeit und Integrität prinzipiell nicht ignoriert werden. Ein Angreifer, der Zugriff auf einen Feldbus in einer Fertigungsanlage oder in der Prozessindustrie hat, kann Schaden an einzelnen Produkten anrichten und möglicherweise auch Menschen, Maschinen und Umwelt gefährden. Aus diesem Grund sollten Datenströme auf dem Feldbus, zumindest teilweise, authentifiziert werden.

Authentizität
Authentizität bezeichnet zum einen den Schutz der Identität der Kommunikationsteilnehmer. Konkret bedeutet das: ein Adressat kann nicht unbemerkt durch einen anderen ersetzt werden. Zum anderen soll auch gesichert werden, dass der Adressat tatsächlich legitime Rechte besitzt. Im CIA-Paradigma soll also die Integrität der Adressierung geschützt werden. Für den Aktor auf dem Feldbus bedeutet dies zu prüfen, ob die Steuerbefehle tatsächlich von der SPS (Speicherprogrammierbare Steuerung) stammt, die befugt ist mit dem Aktor zu kommunizieren und nicht etwa ein Angreifer, der über das Netzwerk Zugang zum Feldbus erlangt hat.

Datenflussintegrität
Datenflussintegrität bezeichnet den Schutz der Integrität der übermittelten Daten, also die Absicherung gegen illegitime Veränderung der Daten. Möglicherweise könnte ein Angreifer nämlich die Botschaft eines legitimen Absenders ändern. Ein funktional sicheres Protokoll würde grundsätzlich eine Integritätsprüfung vornehmen, da aber diese zyklische Redundanzprüfung (CRC) für den Angreifer transparent und vorhersagbar ist, kann dieser auch die Prüfsumme fälschen. In diesem Fall ist Funktionale Sicherheit nicht gewährleistet.

Auswahl von Security – Maßnahmen
Um diese konkreten Schutzziele umzusetzen werden kryptographische Maßnahmen [9] [10] ergriffen. Diese Maßnahmen müssen auf das konkrete Szenario abgestimmt werden: Im Bereich IIoT (Industrial Internet of Things) begrenzen die Leistungsfähigkeit der Prozessoren in den Endgeräten und die verfügbare Bandbreite die Auswahl der verwendbaren Methoden. Am unteren Ende für 8 Bit Microcontroller [11], können einfache Heartbeat-Protokolle [12] mit kryptographischen Funktionen aufgewertet werden, um ein Mindestmaß an Schutz durch Authentifizierung zu erreichen. Am anderen Ende der Skala kann mit TLS [11] [13] dieselbe Sicherheit wie beim Online-Banking erreicht werden.

Erfüllung von Security Objectives – Security by Design
Das Ziel von Maßnahmen ist es, dem System zu ermöglichen, die Sicherheitsanforderungen zu erfüllen. Hierzu müssen die entsprechenden Angriffsflächen erkannt, auf Schwachstellen analysiert und im Anschluss die identifizierten Probleme gelöst werden. Verglichen mit Desktop-Systemen ist die Komplexität der verwendeten Hard- und Software von eingebetteten Systemen üblicherweise niedrig. Wird in diesem Fall die Sicherheit nicht beachtet, existiert eine Angriffsfläche im Kern eines Unternehmens, von dem aus die gesamte IT und Fabrikation angreifbar sein kann. Eine niedrige Komplexität bietet Chancen: die Härtung der Komponenten zum Schutz vor Angriffen ist mit deutlich weniger Ressourcenaufwand zu erreichen als bei komplexen Office-IT-Systemen.

Fazit
Reagieren Feldbusgeräte ausschließlich auf gesicherte und authentifizierte Kommunikation, wird es deutlich schwieriger, diesen Bereich eines Netzwerkes anzugreifen. Durch konsequente Härtung der Einzelkomponenten in einem System kann so ein Angriff bereits im Vorfeld verhindert werden.

Literaturverzeichnis

[1] C. Romeo, „www.iot-inc.com,“ 2017. [Online]. Available: https://www.iot-inc.com/the-s-in-iot-stands-for-security-article/.

[2] Wikipedia, „Feldbus,“ 2018. [Online]. Available: https://de.wikipedia.org/w/index.php?title=Feldbus&oldid=179337515.

[3] IEC 61508-1:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements, Geneva: IEC, 2010, pp. IEC 61508-1-1 7.5.2.2.

[4] S.-P. Oriyano, CEHTM v9 Certified Ethical Hacker Version 9 Study Guide, Indianapolis: Wiley, 2016.

[5] *IEC/TS 62443-1-1:2009-07: Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models,* Geneva: IEC, 2009.

[6] *IEC DIN EN 62443-4-2:2017-10;VDE 0802-4-2:2017-10 - Entwurf Industrielle Kommunikationsnetze - IT-Sicherheit für industrielle Automatisierungssysteme - Teil 4-2: Anforderungen an Komponenten industrieller Automatisierungssysteme,* Berlin: Beuth Verlag, 2017.

[7] K. Wallace, „Common Criteria and Protection Profiles,“ 2003. [Online]. Available: https://www.sans.org/reading-room/whitepapers/standards/common-criteria-protection-profiles-evaluate-information-1078 p.8. [Zugriff am 23 08 2018].

[8] C. . Sydow, „BND-Affäre: NSA spähte noch 2013 deutsche Firmen aus,“ , . [Online]. Available: http://www.spiegel.de/politik/deutschland/bnd-affaere-nsa-spaehte-noch-2013-deutsche-firmen-aus-a-1032049.html. [Zugriff am 5 9 2018].

[9] B. Schneier, Applied Cryptography, 20th Anniversary Edition, Wiley, 2015.

[10] J. Schwenk, Sicherheit und Kryptographie im Internet Theorie und Praxis, Wiesbaden: Springer, 2014.

[11] M. Welschenbach, Kryptographie in C und C++, Berlin: Xpert.press, 2001.

[12] O. Pfeiffer, „Scalable CAN security for CAN, CANopen and other protocols in CAN in Automation, iCC 2017,“ [Online]. Available: https://www.can-cia.org/fileadmin/resources/documents/conferences/2017_pfeiffer.pdf. [Zugriff am 03 11 2017].

[13] R. u. a. Bless, Sichere Netzwerkkommunikation. Grundlagen, Protokolle und Architekturen, Berlin: Springer, 2005.