Leitfaden Industrie 4.0 Security

Handlungsempfehlungen für den Mittelstand

in Kooperation mit

accessec
powerful security solutions

Fraunhofer AISEC

protect-ing.de

VDMA

Editorial

Wolfgang Bokämper

Verehrte Mitglieder und Leser,

die Vernetzung und Digitalisierung der Welt schreitet immer weiter voran. Dies gilt natürlich auch für alle Produktionsbereiche. Diese Herausforderung, genannt Industrie 4.0, bedarf – über die Aufgaben der eigentlich technischen Realisierung hinaus – auch der „Secure Einbettung“.

Industrie 4.0 heißt Daten und somit Informationen zu jeder Zeit an jedem Ort nutzen zu können. Aus einer solchen Verfügbarkeit werden sich viele Chancen ergeben, d. h. Informationen und deren Vernetzung werden zu einem bedeutenden Produktionsfaktor. Im Zuge eines derartigen Prozesses werden Unternehmensgrenzen fallen – fallen müssen, denn Produktentstehungsketten sind auch unternehmensübergreifend.

Macht man sich diesen Umstand bewusst, wird sehr schnell klar, dass die Aufgabe „Security“ die reine Office-Welt verlässt und neue Anforderungen stellt. Der Begriff „Verfügbarkeit“ bekommt somit eine andere Dimension. Sollte heute das E-Mail-Programm für einen halben Tag ausfallen, ist das unbequem, aber nicht lebensbedrohlich. Ein solcher Ausfall der Produktion würde aktuell ein Desaster für alle Lieferketten bedeuten. Somit ist Security eine wichtige Basis oder die „Leitplanke“ für Industrie 4.0.

Für mich ist der Trend zu mehr Shopfloor-IT schon heute klar erkennbar. Auch der Begriff „künstliche Intelligenz“ ist bis zu den Fabrikhallen vorgedrungen. Logistik, Mobilität – alles ist vernetzt und benötigt entsprechende Informationen. Eine ganzheitliche Betrachtung ist hierfür wesentlich und unabdingbar. Dabei wird natürlich klar, dass diese Aufgabe weder isoliert betrachtet noch gelöst werden kann. Alles ist Teil der Kette: angefangen bei der Komponentenherstellung über die Integration bis hin zum Betrieb der Anlagen.

Zu dieser Kette, die oft vorrangig technisch betrachtet wird, gehören aber selbstverständlich auch die Menschen. Sie heißen Entwickler, Automatisierer, Betreiber, Anwender usw. Die wichtige Aufgabe des Managements besteht darin, die Security Awareness bei den Mitarbeitern als Teil des täglichen Arbeitslebens zu integrieren.

Gehen wir also Industrie 4.0 „secure“ an und der Erfolg wird uns recht geben.

Wolfgang Bokämper

Vorsitzender des VDMA-Arbeitskreises Industrial Security,
Bereichsleiter Beschaffung, Organisation & Qualitätssicherung,
Kolbus GmbH & Co. KG, Rahden

Inhaltsverzeichnis

Management Summary

Der zuverlässige und dauerhaft sichere Betrieb von weltweit vernetzten Maschinen und Anlagen ist eine elementare Herausforderung für eine erfolgreiche Umsetzung von Industrie 4.0. Der dafür geläufige deutsche Begriff „Sicherheit“ ist irreführend, da er im Maschinen- und Anlagenbau vornehmlich im Sinne der „Safety“, also der Funktionalen Sicherheit, etabliert ist. Demgegenüber steht in diesem Leitfaden der aus dem Englischen stammende Begriff der “Security“ im Fokus. Die Security beschreibt grundsätzlich die Absicherung von IT-Systemen. Um eine klare Abgrenzung zur Absicherung der Büroinformationstechnik („IT-Security“) zu erhalten, sprechen wir bei der Absicherung von Informationstechnik in industriellen Anlagen, Maschinen und Systemen von „Industrial Security“. Werden diese Systeme nun durch die Integration von Industrie 4.0 vernetzt, so müssen sich sowohl Hersteller als auch Betreiber Gedanken darüber machen, wie sie diese unternehmensübergreifende Vernetzung dauerhaft sicher (im Sinne von „secure“) gewährleisten können. Das ist der Kern von „Industrie 4.0 Security“. Nur mit der zuverlässigen Absicherung moderner Produktions- und Prozesssysteme wird die Transformation der Industrie ermöglicht.

Ziel der „Industrie 4.0 Security“ ist es, die Security von zukünftigen Maschinen und Anlagen über den gesamten Lebenszyklus gewährleisten zu können, statt wie aktuell ein nachgeschaltetes Hinzufügen („Anflanschen“) einer Security-Funktionalität notwendig zu machen. Security muss zukünftig als integraler Aspekt bereits von Beginn an in den gesamten Produktentwicklungsprozess seitens der Maschinen- und Anlagenbauer mit einfließen („Security by Design“). Die Integration der Security erfordert es, diese schlussendlich als funktionalen Bestandteil von zukünftigen Anlagen und Systemen zu betrachten, und somit die „Security as a Function“ zu etablieren.

Dieser Leitfaden dient Maschinen- und Anlagenbauern als Einstieg und Orientierungshilfe, welche Themenbereiche, Technologien und Prozesse für eine Erhöhung der Security komplexer Anlagen berücksichtigt werden sollten. Der Fokus liegt auf der Sicht der Hersteller und Integratoren, zusätzlich werden Anforderungen an notwendige Eigenschaften oder Funktionen gestellt, die zukünftig durch Lieferanten bereitgestellt werden müssen. Die branchenspezifische Fokussierung auf den Blickwinkel des Maschinen- und Anlagenbaus ermöglicht eine angemessene Abdeckung des Anforderungsspektrums und bietet den notwendigen Tiefgang, um konkrete Handlungsoptionen aufzeigen zu können.

Um die Ziele für die Bereitstellung nachhaltig und dauerhaft sicherer Anlagen für Industrie 4.0 zu erreichen, beschreibt der Leitfaden die Berücksichtigung der Security als gleichrangiges Ziel bereits im Entwicklungs- und Konstruktionsprozess. Weiterführend umfassen die Anforderungen an „Industrie 4.0 Security“ eine Betrachtung von Gefährdungen und Risiken vor Inbetriebnahme, ein Management von Cyberrisiken während des Betriebs und eine Aufrechterhaltung der Securityfunktion im gesamten Produktlebenszyklus von vernetzten Maschinen und Anlagen. Die Risikobetrachtung bereitet Hersteller und Integratoren auf aktuelle und zukünftig zu erwartende Bedrohungslagen vor. Mit der Inbetriebnahme kann dem Betreiber gegenüber zudem ein Mindestmaß an Security gewährleistet werden. Während des Produktlebenszyklus ist die Etablierung eines Prozesses zur Annahme, Beurteilung und Reaktion auf relevante Securitybedrohungen notwendig.

Erste Hilfe zur Unterstützung bietet der Leitfaden mit dem Industrie 4.0 Werkzeugkasten des VDMA, unterstützt durch eine Online-Selbsteinschätzung.

Zur Verwendung des Leitfadens

Der Leitfaden bietet die Möglichkeit, sich gezielt bestimmte Aspekte herauszugreifen und diese autark zu betrachten. Es empfiehlt sich jedoch, zunächst mit den organisatorischen und analytischen Themen wie Lebenszyklus der Anlage zu beginnen, bevor eher technische Themen wie Benutzerkonten, Passworte und Netzsegmentierung angegangen werden. Jeder Abschnitt für sich enthält hilfreiche Handlungsoptionen, diese sollten jedoch im Rahmen eines durchgängigen Security Managements bewertet werden, um Prioritäten richtig zu setzen. Nur so lassen sich nachhaltige Veränderungen im Produktentstehungsprozess bewirken und wiederkehrende Kosten für die Bereitstellung von Security-Funktionen minimieren. Hierbei ist zwingend erforderlich, alle Beteiligten einzubinden und Entwicklung als auch Konstruktion gleichermaßen in die Pflicht zu nehmen. Zur sprachlichen Vereinfachung werden diese Begriffe im Folgenden synonym verwendet. Als weitere sprachliche Vereinfachung wird der Begriff „Komponente“ synonym für „Systemteil“ verwendet und umfasst somit alle Bauteile und deren Kombinationen, mit Hilfe derer eine Anlage konstruiert wird.

Der Begriff „sicher“ bezieht sich, wenn nicht explizit anders angeben, ausschließlich auf Security und nicht auf Safety (Funktionale Sicherheit).

Zur Abgrenzung gegenüber der funktionalen Sicherheit wird zur Klarstellung bevorzugt der Begriff „Security“ anstelle von „Sicherheit“ verwendet. Da dies jedoch nicht durchgängig möglich ist, bezieht sich der Begriff „sicher“, wenn nicht explizit anders angeben, ausschließlich auf Security und nicht auf Safety (Funktionale Sicherheit).

Die ausklappbare Seite am Schluss zeigt die Funktionsklassen des „VDMA-Werkzeugkasten Industrie 4.0 – Produkte“. Innerhalb der Klassen (hier A bis F genannt) wird auf einer fünfwertigen Skala der Grad der Industrie 4.0 Funktionalität angezeigt. So beziehen sich die Einträge in der linken Spalte auf eine Maschine der klassischen Produktion, während Funktionen der rechten Spalte der vollen Vision von Industrie 4.0 entsprechen.

Handlungsempfehlungen und Mindestanforderungen

Im Folgenden werden grundlegende Handlungsempfehlungen und Mindestanforderungen für Schutzmaßnahmen ausgesprochen, die einen gewissen Grundschutz für die Maschine ermöglichen. Jeder Empfehlung wird zudem eine entsprechende Produktfunktion zugeordnet, so dass bei der Entwicklung lediglich die für die jeweilige Maschine relevanten Schutzmaßnahmen identifiziert werden müssen. Dieser Kompromiss bedeutet einen hohen Sicherheitsgewinn für Unternehmen auf dem Weg zur Industrie 4.0.

Den Handlungsempfehlungen werden Produktfunktionen zugeordnet, um damit anzudeuten, ab welchem Grad auf der fünfstufigen Industrie 4.0 Skala eine Handlungsempfehlung in eine Mindestanforderung übergeht. Anders gesagt: ab welcher Funktionalität eine Schutzmaßnahme notwendigerweise umgesetzt werden soll. Hierzu wird der „VDMA-Werkzeugkasten Industrie 4.0 – Produkte“ als Skala verwendet.

Um den Lesern den Einstieg für die eigene Positionsbestimmung zu erleichtern, findet sich unter

www.i40-security.de

ein Online-Fragebogen. Die (anonyme) Beantwortung ermöglicht eine schnelle Selbsteinschätzung und verweist auf einzelne Abschnitte des Leitfadens, in denen auch ohne Risikoanalyse passende Handlungsempfehlungen für die Verbesserung der eigenen Situation angeboten werden.

Beispielsweise bedeutet folgende Grafik, dass, sobald das Produkt zumindest über Feldbusschnittstellen oder über Datenspeicher zum Informationsaustausch verfügt, die Maßnahme eine Mindestanforderung ist (Abbildung 1).

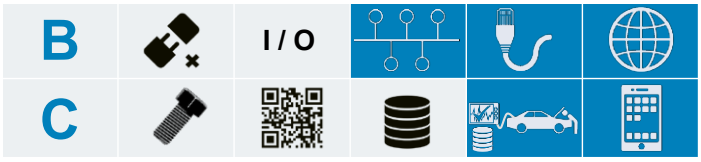


Abbildung 1: Beispiel einer Handlungsempfehlung

Bei mehreren Kennzeichnungen sind diese als „oder“ zu verstehen.

Manche Handlungsempfehlungen sind immer eine Mindestanforderung. Diese sind durch folgende Grafik gekennzeichnet (Abbildung 2):

Abbildung 2: Hinweis auf eine Mindestanforderung

Ferner kennzeichnen wir den Abschnitt des Produktlebenszyklus, in dem die Handlungsempfehlung (oder respektive Mindestanforderung) umgesetzt werden soll. Wir unterscheiden hier zwischen der Entwicklungsphase, der Integrationsphase, der Betriebszeit mit Gewährleistung seitens des Herstellers, sowie der Betriebszeit ohne Gewährleistung.

Diese Einordnung bezüglich des Produktlebenszyklus wird durch folgende Symbolik dargestellt (Abbildung 3).

In diesem Beispiel sind die Entwicklungsphase, und die Betriebszeit mit und ohne Gewährleistung relevant.

Abbildung 3: Beispiel einer Einordnung im Produktlebenszyklus

Tabelle:
Übersicht der Handlungsempfehlungen
Die Tabelle auf den Seiten 38 bis 41 gibt einen kompakten Überblick über die Handlungsempfehlungen. Zudem werden die Handlungsempfehlungen eingeordnet in folgende Bereiche:

Die vier Phasen des Produktlebenszyklus:
- Entwicklung
- Integration
- Betrieb mit Gewährleistung
- Betrieb ohne Gewährleistung

Die aus dem Werkzeugkasten Industrie 4.0 stammenden Anwendungsebenen:
- A: Integration von Sensoren/Aktoren
- B: Kommunikation
- C: Funktionalitäten zur Datenspeicherung und Informationsaustausch
- D: Monitoring

Die für die Umsetzung verantwortlichen Kreise:
- Hersteller
- Integrator
- Betreiber

Ein Punkt in den Feldern des Produktlebenszyklus bzw. Umsetzungsverantwortung besagt, dass die Handlungsempfehlung für diese Phase/Verantwortlichen gilt.

Die in den Anwendungsebenen verzeichneten Zahlen von 1 bis 5 zeigen, ab welcher jeweiligen Entwicklungsstufe die Handlungsempfehlung zur Mindestanforderung wird.

1. Risikoanalyse

Verschaffen Sie sich einen Überblick

Zu Beginn der Security-Betrachtung steht die Risikoanalyse, die als integraler Bestandteil des Entwicklungsprozesses der Maschine etabliert werden soll. Schon bei der ersten Anforderungsanalyse zu Beginn der Entwicklung können so Security-Aspekte in das Konzept und den Entwurf der Maschine einfließen.

Die frühe Einbindung einer Risikoanalyse in den Konstruktions- und Entwicklungsprozess bedeutet zwar einen oftmals ungewohnten anfänglichen Mehraufwand, dieser lässt sich jedoch durch strukturiertes, wiederholbares Vorgehen auf ein überschaubares Maß reduzieren. Es hat sich als sinnvoll erwiesen, hierbei im Betrieb etablierte Methoden (wie etwa FMEA – Failure Mode and Effects Analysis) für die Risikobetrachtung zu adaptieren. Vor allen Dingen aber zahlt sich dieser frühe Mehraufwand im weiteren Verlauf der Entwicklung aus, da Security-Funktionen als integraler Bestandteil der Maschine aufgefasst werden können und diese nicht nachträglich teuer nachgerüstet werden müssen.

Alle nachfolgenden Schritte innerhalb der Risikoanalyse sollen während des Entwicklungsprozesses sowie regelmäßig zur Betriebszeit mit und ohne Gewährleistung seitens des Herstellers berücksichtigt werden.

Ein effizientes Vorgehen lässt sich auf die folgenden Punkte reduzieren (siehe auch die Richtlinie VDI/VDE 2182[1]).

1.1. Identifikation der schutzbedürftigen Werte

Zunächst sollte ein Konsens darüber bestehen, welche Komponenten innerhalb der Maschine einen schutzbedürftigen Wert darstellen. Dies können beispielsweise Hardware- und Softwarekomponenten sein, aber auch Daten und Programme, die als geistiges Eigentum einen hohen Wert darstellen. Als erster Schritt ist also die Bewusstwerdung über materielle und immaterielle Werte zu empfehlen, die sich dann in der Identifikation und Auflistung der jeweiligen Komponenten widerspiegelt.

1.2. Ermittlung der Schutzziele

Nun lassen sich für die schutzbedürftigen Werte Schutzziele formulieren. Wurde einer speziellen Komponente innerhalb der Maschine (im ersten Schritt) ein hoher Wert zugemessen, so sollte ein entsprechendes Schutzziel für diese Komponente formuliert werden. Für einen Datensatz innerhalb der Maschine, der als kritisch eingestuft wurde und von dem auch das Funktionieren weiterer verbundener Maschinen abhängt, könnte das Schutzziel beispielsweise lauten: „Garantierte Verfügbarkeit der Daten bei Maschinen-Fernzugriff“.

[1] VDI/VDE 2182, Informationssicherheit in der industriellen Automation – Allgemeines Vorgehensmodell, Blatt 1. (2007).

1.3. Identifikation der Bedrohungen

Hat man die schutzbedürftigen Komponenten der Maschine identifiziert, lassen sich als nächstes Überlegungen zu den zugehörigen Bedrohungen anstellen. Eine Bedrohungsanalyse gibt Aufschluss darüber, mit welchen praktischen Bedrohungen man beim Betrieb der Maschine zu rechnen hat und welchen jeweiligen Schaden man ansetzen sollte. Als Hilfestellung bieten sich hier gängige Zusammenfassungen und Auflistungen aktueller Bedrohungen an, wie z.B. die Zusammenstellung des Bundesamtes für Informationstechnik (BSI)[2].

1.4. Risikobewertung

Es lassen sich nun auf Basis der Bedrohungsanalyse die den Bedrohungen zugeordneten Risiken bewerten. So ist das Risiko einer ausgeführten Bedrohung der mit der jeweiligen Eintrittswahrscheinlichkeit gewichtete Gesamtschaden.

Die Bewertung erfolgt anhand eines vorab zu erstellenden Angreifermodells. In diesem werden die Annahmen zu den Fähigkeiten eines möglichen Angreifers festgehalten.

Eine vollständige Ermittlung aller Risiken und deren Priorisierung führt direkt zur Auswahl geeigneter Schutzmaßnahmen und bildet daher die Grundlage für eine optimale Absicherung der Maschine oder Anlage. Gleichzeitig kann eine umfassende Risikoanalyse sehr umfangreich sein und für ein mittelständisches Unternehmen einen nicht tragbaren Aufwand bedeuten. Deshalb wird empfohlen, den Ansatz einer Risikoanalyse zumindest dahingehend in den Entwicklungsprozess zu integrieren, dass schutzbedürftige Werte erkannt und zugehörige Schutzziele formuliert werden und dass sich die jeweiligen Verantwortlichen in Planung und Entwicklung der Maschine über die gängigen Bedrohungen bewusst sind. In diesem Sinne stellt dieser Leitfaden ein Kompromiss zwischen dem Status quo einer oftmals nicht stattfindenden Security-Betrachtung und der idealen Ermittlung aller Schutzmaßnahmen auf Basis einer detaillierten Risikoanalyse dar.

[2] BSI: Industrial Control System Security – Top 10 Bedrohungen und Gegenmaßnahmen 2014

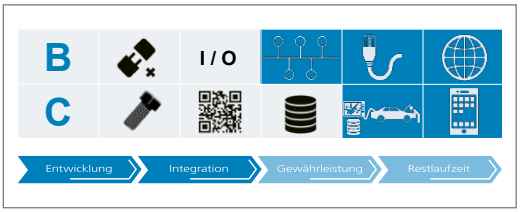
2. Netzsegmentierung

Teile und herrsche!

Die Anlage soll anhand des Schutzbedarfs der einzelnen Systemteile in Zonen aufgeteilt werden. Die verbundenen Maschinen und Komponenten innerhalb einer Zone zeichnen sich hierbei durch ähnlichen Schutzbedarf aus. Die Trennung der einzelnen Segmente sollte durch technische Maßnahmen realisiert sein.

2.1. Definition des Risiko-basierten Schutzbedarfs, der den Anlagen und Komponenten zugeordnet wird

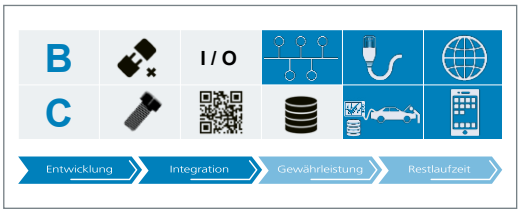
Die Ermittlung des Schutzbedarfs soll anhand gängiger Methoden zur Risikoabschätzung vorgenommen werden. Wie in Abschnitt 1 beschrieben, sollen hierzu zunächst die schutzbedürftigen Werte identifiziert werden. Nach der Ermittlung entsprechender Schutzziele erfolgt dann eine Bedrohungsanalyse. Eine Risikoanalyse liefert dann Aufschluss über den Schutzbedarf der Anlagen und Komponenten. Die Zuordnung des so ermittelten Schutzbedarfs ist Voraussetzung für die Ermittlung von Zonen, d.h. Netzsegmenten mit Komponenten vergleichbaren Schutzbedarfs.



2.2. Zonierung der Dienste

Die verschiedenen Netzbereiche der Produktion (wie z.B. ERP-, MES- oder SCADA-Netz) zeichnen sich insbesondere durch die bereitgestellten Dienste aus. Bei der Zonierung sollen insbesondere auch diese Dienste innerhalb des Produktionsnetzes berücksichtigt werden.

So soll sichergestellt werden, dass sich innerhalb des unmittelbar mit der Maschine verbundenen Netzsegmentes ausschließlich Dienste mit vergleichbarem Schutzbedarf befinden. Dienste können beispielsweise Softwaremodule zur Verarbeitung oder Bereitstellung von Maschinendaten sein, aber auch Konfigurationsmodule, welche Maschinenfunktionen entsprechend einer Konfigurationsdatei zusammenstellen. Bei der Zonierung soll darauf geachtet werden, dass bei Ausfall einer Zone möglichst wenig andere Zonen betroffen sind.



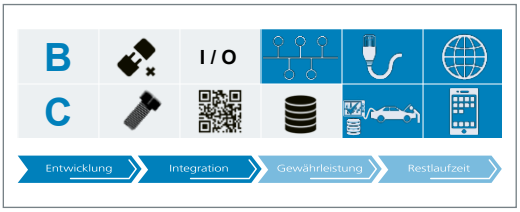
2.3. Einsatz von Isolationsmaßnahmen

Sind den Hardware- und Softwarekomponenten der Maschine Sicherheitszonen zugeordnet, sollen diese durch technische Maßnahmen ausreichend voneinander getrennt werden. Dies soll bei einer Kompromittierung eines Teilbereiches der Maschine die Ausbreitung in das Gesamtsystem erschweren. Mögliche technische Maßnahmen zur Trennung der ausgewiesenen Segmente können z.B. Firewalls oder Datendioden sein. Für die Maschine bedeutet dies insbesondere, dass sie abhängig vom Schutzbedarf nicht nur Filterfunktionen für aus- und eingehende Kommunikation bereitstellen soll, sondern auch für Kommunikation innerhalb der Maschine selbst.

Es wird empfohlen, die Erkennung von Schadsoftware oder Protokollanomalien anhand der Netzwerkkommunikation zwischen den definierten Netzsegmenten durchzuführen. Solche Schutztechnologien kommen oft direkt auf Firewalls zum Einsatz.

Für besonders gefährdete Netzsegmente sollen Datendioden sicherstellen, dass Informationen ausschließlich in eine vordefinierte Richtung fließen. Hierbei ist jenen Lösungen der Vorzug zu geben, bei denen die Isolation durch eine hardwaremäßige Trennung erfolgt. Um Datendioden sinnvoll einsetzen und anpassen zu können, sollen sämtliche Datenflüsse in und aus der Maschine identifiziert werden.

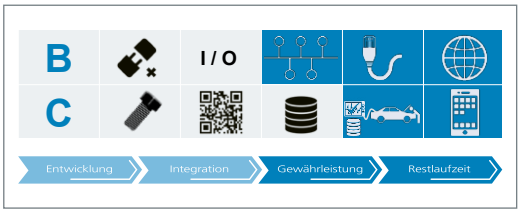
Ferner ermöglichen VPN-Lösungen das Zusammenfassen räumlich getrennter Netze zu einem Segment, um ähnliche oder gleiche Anlagen trotz räumlicher Entfernung gemeinsam verwalten zu können.



2.4. Periodische Überprüfung der Isolationsmaßnahmen auf Effektivität und Patchbarkeit von Filterkomponenten

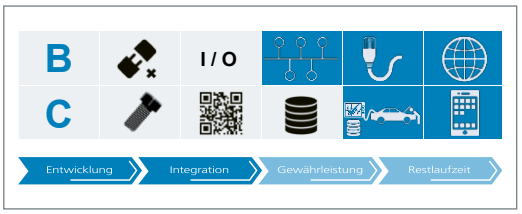
Die technischen Isolationsmaßnahmen sollen regelmäßig hinsichtlich ihrer Effektivität überprüft werden können. Im Falle von Firewalls und anderen Filtertechniken kann eine regelmäßige Überprüfung der Filterregeln notwendig sein. Der Anlagenbauer soll eine Updatefähigkeit gewährleisten, sodass diese Aufgabe entweder vom Betreiber selbst durchgeführt werden kann, oder als Service dem Betreiber angeboten wird. Der zeitliche Abstand zwischen den Überprüfungen hängt dabei sehr stark von der jeweiligen Maschine ab. Während Maschinen mit geringer Konnektivität auch mit relativ statischen Filterregeln sicher konfiguriert werden können, sollten die Filterregeln bei Maschinen mit hoher Funktionsvariabilität und entsprechender Kommunikation häufiger überprüft und angepasst werden. Auch muss davon ausgegangen werden, dass sich der Schutzbedarf einer Anlage durch Produktumstellungen oder Umbau/Umzug ändert, wodurch weitere Anpassungen an der Netz- und IP-Konfiguration notwendig sein können.

Im Falle von bekannt gewordenen Schwachstellen in den Filterkomponenten soll sichergestellt sein, dass die betroffenen Module vom Hersteller zeitnah gepatcht werden können (siehe Abschnitt 9).



2.5. DNS und andere Services pro Zone

Vor dem Hintergrund des zu erwartenden starken Anstiegs von kommunikationsfähigen Komponenten innerhalb der Anlage ist davon auszugehen, dass zentrale DNS-Server mit der Gesamtheit der Anfragen aus der Anlage zunehmend überlastet werden. Deshalb soll die Netzsegmentierung so weit wie möglich auf die DNS-Infrastruktur abgebildet werden. Aufgrund teils sehr komplexer Netze und einer großen Zahl an Netzsegmenten ist hier auch denkbar, mehrere Segmente mit ähnlichem Schutzbedarf einem einzelnen DNS-Server zuzuordnen. Da die DNS-Konfiguration sowohl vom Integrator als auch vom Betreiber vorgenommen wird, sollen die Maschinen und Anlagen die entsprechende Funktionalität zur flexiblen Konfiguration gewährleisten.



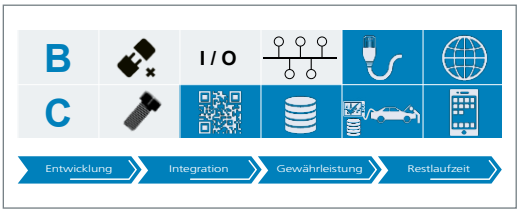
3. Benutzerkonten, Credentials, Authentisierung und Autorisierung

Nicht jeder darf alles machen …

Die Anlage soll das sichere Verwalten von Benutzerkonten und zugeordneter Zugangsdaten (Credentials, z.B. Passwörter, Token, SSH-Schlüssel oder biometrische Authentisierungsdaten) gewährleisten.

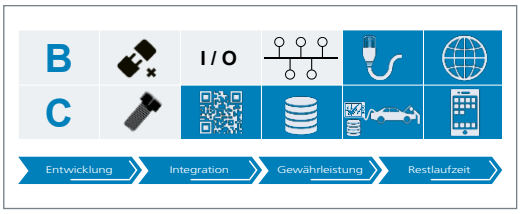
3.1. Individuelle Benutzerkonten

Es sollen individuelle Benutzerkonten für jeden Akteur eingerichtet werden können. Als Akteure sind sowohl mit der Maschine interagierende Menschen gemeint, aber auch andere Maschinen und Systeme, die auf bereitgestellte Dienste zugreifen. Dies bezieht sich sowohl auf Akteure, die via Fernzugriff mit der Maschine interagieren, als auch auf Akteure mit lokalem Zugriff. Nur so kann eine auf den Akteur beziehbare Protokollierung (siehe Abschnitt 7) aller Zugriffe auf die Maschine stattfinden, welche wiederum in die Angriffserkennung und die Untersuchung von IT-Sicherheitsvorfällen einfließt. Hierbei ist zu beachten, dass dem Betreiber die Möglichkeit gegeben werden soll, sämtliche Benutzerkonten von Maschinen zu dokumentieren und diese jeweils einem menschlichen Verantwortlichen zuzuordnen, der über Herkunft und Wirkweise des technischen Kontos informiert ist. Auch sind individuelle Benutzerkonten Grundlage für eine nachfolgende Rechteverteilung auf Individuen und Rollen. Hierbei ist insbesondere zu berücksichtigen, dass es keine Konten für eine Gruppe von mehreren Akteuren geben soll: Benutzerkonten sind nicht nur aufgrund von zugeordneten Rollen, sondern individuell für jeden Nutzer der Anlage zu erstellen.



3.2. Account Management

Die Menge der Akteure kann je nach Einsatzumgebung der Maschine starker Fluktuation unterliegen. Im günstigsten Fall wird die Maschine für lange Zeitabschnitte von derselben Gruppe von Akteuren bedient. Im ungünstigsten Fall wechseln die Akteure sehr oft, mitunter bedienen sie die jeweilige Maschine nur wenige Schichten. Die Maschine soll deshalb eine effiziente Handhabung zur Verwaltung der individuellen Benutzerkonten gewährleisten, insbesondere in Bezug auf das Hinzufügen, Aktivieren, Modifizieren, Abschalten und Beseitigen von Konten. Dies ist oftmals durch eine zentrale Verwaltung der Benutzerkonten zu erreichen. So wird empfohlen, dass die Maschine eine Integration in bestehende Identitätsmanagementsysteme oder die Einbindung der Benutzerkonten in Verzeichnisdienste unterstützt.

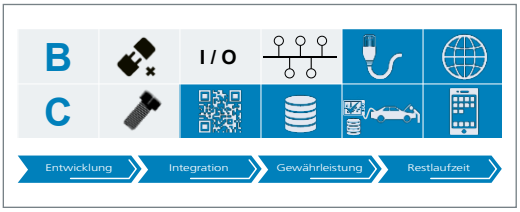


3.3. Verteilung und Management der Credentials (Zugangsdaten)

Jedes der individuellen Benutzerkonten ist mit Zugangsdaten verknüpft, die zur späteren Authentisierung und Autorisierung dem jeweiligen Akteur bekannt sein sollen. Das Management dieser Credentials soll hierbei so gestaltet sein, dass eine sowohl sichere als auch effiziente Verteilung möglich ist. Praktisch bedeutet dies, dass das Verfahren zum Zurücksetzen der Credentials bei Verlust zwar dem jeweiligen Schutzbedarf entspricht, jedoch so flexibel gestaltet werden soll, dass der Betrieb der Maschine immer gewährleistet ist. Dies soll Ausfallzeiten aufgrund zu komplexer Rücksetzungsregelungen verhindern. Bei Einsatz von Passwörtern soll gewährleistet sein, dass beim Zurücksetzen auch Default-Passwörter verändert werden können.

Die Erstellung der Credentials soll aktuellen Standards und Empfehlungen genügen (siehe Abschnitt 14).

Für die Aufbewahrung und Speicherung der Credentials werden vor physischen Angriffen geschützte Sicherheitsmodule (wie z.B. TPMs oder SmartCards) empfohlen. Stehen diese nicht zur Verfügung, so ist zumindest darauf zu achten, dass Credentials niemals im Klartext gespeichert werden dürfen, sondern lediglich deren Salted-Hashes (siehe auch BSI ICS-Kompendium für Hersteller und Integratoren[3]).

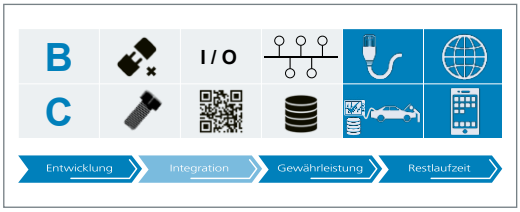


3.4. Authentisierung menschlicher Nutzer sowie von Softwareprozessen und -komponenten

Sämtliche menschlichen Nutzer sowie Softwareprozesse und -komponenten sollen sich vor jedem Zugriff bei der Maschine authentisieren. Dies soll auf Basis der definierten Authentisierungsdaten erfolgen. Hat die Maschine den Akteur erfolgreich authentisiert, so soll der Zugriff nur auf die jeweilige Sitzung beschränkt werden.

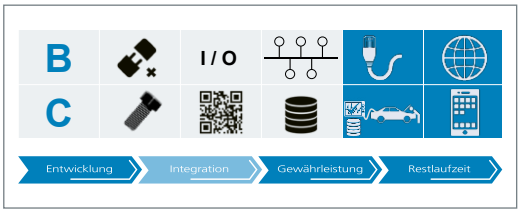
3.5. Public-Key Authentisierung

Bei der Authentisierung sollen wenn möglich Public-Key Verfahren zum Einsatz kommen. Neben einem sicheren und effizienten Schlüsselmanagement sowie einer sicheren und auf die Möglichkeiten von eingebetteten Systemen abgestimmten Wahl des kryptographischen Materials (siehe Abschnitt 14) ist hier insbesondere die Integration der Maschine in bereits bestehende Public-Key Infrastrukturen zu empfehlen[4]. Dabei ist zu berücksichtigen, dass eine PKI üblicherweise keine Funktionen für das Certificate Lifecycle Management mitbringt, welches spätestens durch den Betreiber beigestellt werden soll um Systemausfälle aufgrund abgelaufener Zertifikate zu vermeiden.



3.6. Zonenbildung und Zugriffskonzepte mit entsprechender Authentifizierung

Die Authentifizierung der Akteure soll nicht nur auf den einzelnen Komponenten der Maschine erfolgen, sondern auch beim Übertreten der in Abschnitt 2 definierten Zonengrenzen. Will sich ein Akteur auf einer Komponente authentisieren, die nicht innerhalb seiner Zone liegt, so soll eine Authentisierung an jedem Zonenübergang auf dem Weg zur Zielkomponente stattfinden. Weiter soll bei Zugriff über jegliche Schnittstellen der Maschine eine Authentifizierung erfolgen. Es ist aus Sicht der Usability zielführend und effizient, hierbei etablierte Verfahren zur Automatisierung anzuwenden (Single Sign-On durch Übermittlung von Tokens, etwa SAML, Kerberos oder OAuth 2.0).



[3] https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/Empfehlungen/ICS/empfehlungen_node.html

[4] Sowohl die Microsoft Certificate Services eines Windows Servers als auch die Enterprise Java Bean CA (EJBC) bieten kostengünstige Möglichkeiten zur Ausgabe von Zertifikaten.

3.7. Die Maschine soll nach jeder Authentifizierung eine Autorisierungsprüfung der Akteure/Dienste gewährleisten.

Wurde ein Akteur erfolgreich von der Maschine authentifiziert, sollen direkt anschließend die seinem individuellen Benutzerkonto zugeordneten Rechte überprüft werden. Stimmen die dem Akteur zugeteilten Rechte nicht mit den zum Zugriff erforderlichen Rechten überein, soll der Zugriff verweigert und ein entsprechender Eintrag für das Ereignisprotokoll generiert werden. Während die Rechteverteilung seitens des Akteurs vom Account-Management geleistet wird, so sollen die den Komponenten und Diensten zugeordneten Zugriffsrechte bereits vom Integrator vordefiniert und dokumentiert sein. Die Zugriffsrechte auf Komponenten und Dienste sollen auch nach Inbetriebnahme der Maschine noch verändert werden können. Dies ist aufgrund sich verändernder Umgebungsanforderungen erforderlich. Um die Verwaltung der Berechtigungen für den Betreiber zu vereinfachen und die Komponenten zu entlasten kann es sinnvoll sein, diese (z.B. unter Verwendung von XACML) zentral verwaltbar zu machen.

3.8. Starke Authentisierung auf externen Schnittstellen

Sämtliche Zugriffe auf externe Schnittstellen der Anlage sollen durch starke Authentisierung abgesichert sein. Im Falle kryptographischer Authentisierungsmechanismen sollen die jeweiligen Parameter (z.B. Schlüssellängen) gemäß aktueller Standards gewählt werden. Beispielsweise liefern verschiedene VPN Lösungen, IPSec und TLS bei Fernzugriff bereits eine starke Authentisierung, sichere Konfiguration vorausgesetzt.

Es sei hier erwähnt, dass Maschinenkomponenten im Werkszustand oftmals mit initialen Standardkonten (z.B. Administrator mit Standardpasswort) ausgeliefert werden. Starke Authentisierung bedeutet auch und insbesondere, dass solche Standardkonten bei Inbetriebnahme der Maschine auf die tatsächlichen Konten und die dazu vorgesehenen Identitäten angepasst werden. Hardcodierte und damit unveränderliche Credentials sind nicht nur unsicher, sondern erfordern einen kostspieligem Austausch der Hardware bei Kompromittierung der Zugangsdaten.

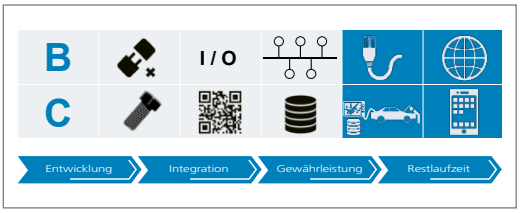
4. Nutzung sicherer Protokolle

Mithören und ändern verboten

Für Angreifer, die nicht direkten Zugang zur Maschine haben, bietet sich oftmals die Kommunikation zu externen Komponenten als initialer Angriffspunkt an. Es sollen daher ausschließlich sichere Protokolle Verwendung finden, die Vertraulichkeit, Integrität und Authentizität der gesendeten Daten gemäß Stand der Technik gewährleisten. Dabei sollen wenn möglich bereits standardisierte Protokolle zum Einsatz kommen.

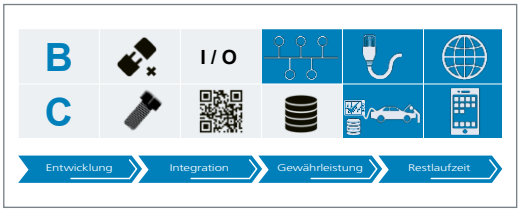
4.1. Vertraulichkeit der Kommunikation bei IP basierten Protokollen

Für IP-basierte Protokolle zur Kommunikation örtlich verteilter Maschinen lässt sich die Vertraulichkeit und Integrität der übermittelten Daten durch etablierte Absicherungsmaßnahmen realisieren. Empfohlen wird hierbei insbesondere die Verwendung von TLS 1.3 und darauf aufbauender Protokolle (wie z.B. HTTPS). Ist eine Verschlüsselung aufgrund erforderlicher Abwärtskompatibilität zu Altsystemen nicht möglich, so sollte die Kommunikation durch ein sicheres Protokoll getunnelt werden. Diese Empfehlung wird unter der Annahme ausgesprochen, dass zeitkritische Anwendungen nicht über IP-basierte Protokolle kommunizieren und die zusätzliche Latenz durch Verschlüsselung der Anwendungsdaten vernachlässigbar ist.



4.2. Integrität der Kommunikation

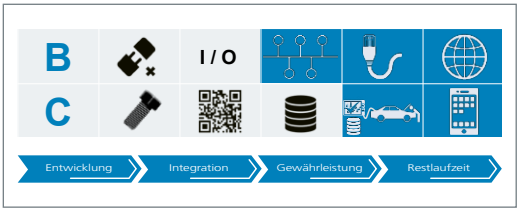
Die Integrität der Kommunikationsdaten soll sowohl innerhalb als auch außerhalb der Maschine gewährleistet sein. Die korrekte Funktionsweise der Maschine ist unmittelbar an die Korrektheit der übertragenen Anwendungsdaten verbunden. Dies hat zur Folge, dass eine unentdeckte Manipulation von Anwendungsdaten während der Übertragung ernstzunehmende Auswirkungen auf die Maschine als Ganzes haben kann. Auch hier empfiehlt sich für eine praktische Realisierung die Verwendung offener Standards und gängiger Implementierungen nach dem Stand der Technik, wie z.B. TLS 1.3.



4.3. Typ, Stärke und Qualität der Verschlüsselungsalgorithmen

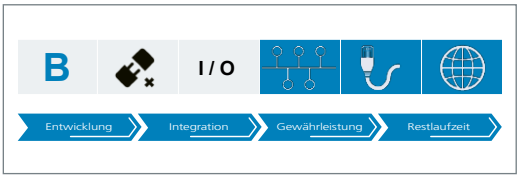
In Anbetracht der Vielzahl an kryptographischen Algorithmen und einer noch größeren Auswahl an möglichen Implementierungen ist unbedingt zu empfehlen, auf standardisierte und von öffentlichen Stellen empfohlene Verschlüsselungsverfahren zurückzugreifen. In den öffentlichen Empfehlungen (siehe Abschnitt 14) finden sich auch Vorgaben zur geeigneten Wahl der Parameter (z.B. Schlüssellängen). Diese Empfehlungen öffentlicher Stellen unterliegen aufgrund der sich ständig verändernden Bedrohungslage regelmäßiger Überarbeitung.

Bei der Entwicklung der Maschine sollte deshalb darauf geachtet werden, dass eine entsprechende Anpassung in bereits bestehenden Maschinen und Anlagen möglich ist. Von Eigenentwicklungen, die nicht einer Kryptoanalyse durch Experten unterzogen wurden, ist dringend abzuraten.



4.4. Sonderbetrachtung des Feldbus

Auf Feldbus-Ebene soll zumindest Authentizität und Integrität der Kommunikation gewährleistet sein. Aufgrund der Echtzeitanforderungen soll je nach Einsatzzweck der Anlage entschieden werden, ob eine Verschlüsselung der Daten auf Feldbusebene notwendig und möglich ist.



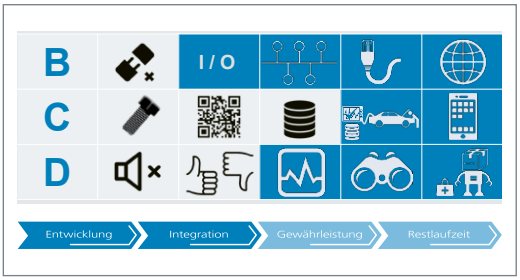
5. Absicherung von Funktechnologien

Von Luftbrücken und Luftlücken …

Sämtliche von der Maschine unterstützten Funktechnologien sollen gemäß Stand der Technik abgesichert werden.

5.1. Sichere Konfiguration

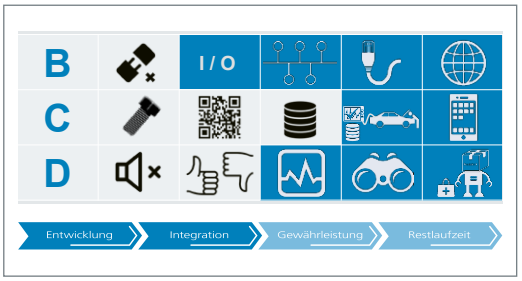
Neben funktionalen Anforderungen müssen auch die Security-Anforderungen der eingesetzten Funktechnologie erfüllt werden. Dies umfasst zunächst die sichere Konfiguration der eingesetzten Funktechnologien. So sollen möglichst geringe Reichweiten (durch Anpassung der Signalstärke oder Abschirmung) und eine möglichst hohe Störfestigkeit realisiert werden. Ist eine sichere Konfiguration der Komponenten aufgrund notwendiger Abwärtskompatibilität nicht durchführbar, so sollen die jeweiligen unsicheren Kommunikationskanäle getunnelt und durch sichere Protokolle abgesichert werden.



5.2. Wireless Access Management

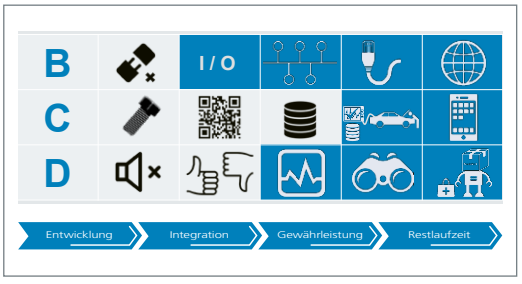
Die Anlage soll bei Zugriff über Funktechnologien eine starke Authentisierung durchführen (vergleiche auch Abschnitte 3 und 6) sowie sämtliche Interaktionen einer Sitzung protokollieren. Die Aktivierung einer Zugangsbeschränkung nach erstmaliger Einrichtung wird empfohlen, sofern diese nicht den effektiven Betrieb der Maschine maßgeblich einschränkt. Die Zugangsbeschränkung kann dabei je nach Bedürfnis konfiguriert werden, technisch kann dies durch eine MAC-Filterung realisiert werden.

Dasselbe gilt für Relay-Stationen, die den physischen Signalbereich erheblich erweitern können. In Umgebungen mit besonderem Schutzbedarf sollte die Nutzung von 802.1x erwogen werden bzw. dessen Nutzung möglich sein.



5.3. Zeitabhängigkeit der Sicherheit von Kryptographischen Funktionen

Aufgrund der Exponiertheit von Funknetzen bei gleichzeitiger langer Einsatzdauer der Maschinen soll eine regelmäßige Überprüfung der Security-Konfiguration erfolgen. Dies umfasst insbesondere die kryptographischen Funktionen des Funknetzes. Sind die eingesetzten Chiffrensammlungen, Parameter oder Implementierungen von aktuellen Angriffen betroffen, so sollten diese umgehend durch sichere Versionen ersetzt werden. Einen Überblick über aktuell sichere Protokolle und kryptographische Funktionen finden sich in entsprechenden Standards und Empfehlungen des BSI und des NIST (vergleiche auch Abschnitt 14). Eignen sich die verwendeten Komponenten aufgrund ihrer limitierten Rechenkapazität nicht für stärkere Algorithmen, besteht als Ausweichmöglichkeit die schnelle Rotation des Schlüsselmaterials.



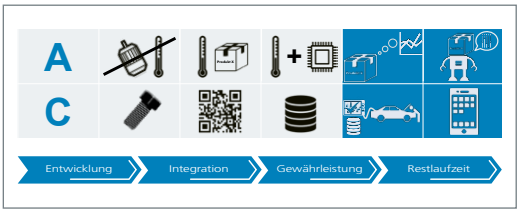
6. Sichere Fernwartung

Der Weg durch unsicheres Terrain

Der Anlagenhersteller soll gewährleisten, dass die Systeme zur sicheren Fernwartung dem identifizierten Schutzbedarf entsprechen.

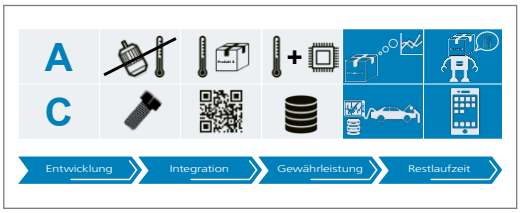
6.1. Regelungen zum Aufbau und Beenden einer Fernzugriffssitzung

Grundlage für die Etablierung eines sicheren Fernwartungsprozesses sind Regelungen zum Aufbau und Beenden einer Fernzugriffssitzung. So soll definiert sein, wann und unter welchen Bedingungen eine Sitzung gestartet werden darf. Vor jeder Fernwartung soll geprüft werden, ob der Akteur die erforderlichen Rechte besitzt und ob die gegenwärtige Auslastung der Maschine ein Wartungsintervall zulässt. Die Sitzung soll nach einer festgelegten Zeitspanne automatisch gesperrt werden, wenn der Nutzer in diesem Zeitraum keine Aktionen ausgeführt hat. Eine gesperrte Sitzung soll nur mittels erneuter Identifikation, Authentifikation und Autorisierung wiederaufgenommen werden können. Das Beenden der Wartungssitzung soll sowohl von der Maschine als auch vom Nutzer der Fernwartung initiiert werden können. Das Beenden seitens der Maschine kann dann notwendig sein, wenn der Nutzer nicht autorisierte Funktionen aufrufen oder Einstellungen vornehmen will. Sämtliche Daten der Sitzung (einschließlich Zeitpunkt, Dauer und ausgeführter Aktionen) sollen protokolliert werden. Zusätzlich zu den genannten Maßnahmen kann ein Fernzugriff über weitere Filtermaßnahmen, z.B. Begrenzung des zugänglichen IP-Adressbereichs eingeschränkt werden.



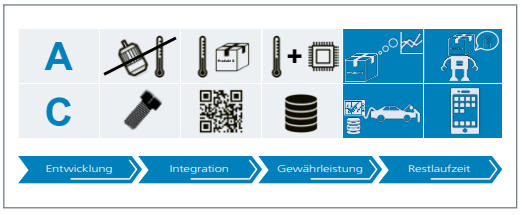
6.2. Absicherung durch technische und organisatorische Maßnahmen

Auf organisatorischer Ebene soll vorgegeben werden, wann und unter welchen Bedingungen eine Fernwartung durchgeführt werden darf. So kann beispielsweise ausgeschlossen werden, dass eine Fernwartung zu Zeitpunkten stattfindet, zu denen die Maschine kritische Funktionen für weitere abhängige Maschinen ausführt. Die Einhaltung dieser Vorgaben soll technisch abgesichert sein, beispielsweise durch automatisierte Überprüfung einer vorgegebenen Policy vor jedem Fernwartungszugriff.



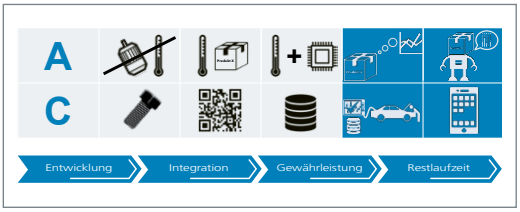
6.3. Verschlüsselung der Verbindungen

Die Fernwartung soll über eine kryptographisch abgesicherte Verbindung erfolgen. Nur so können Authentizität des Akteurs sowie Vertraulichkeit der übermittelten Daten garantiert werden (siehe insbesondere Abschnitt 4).



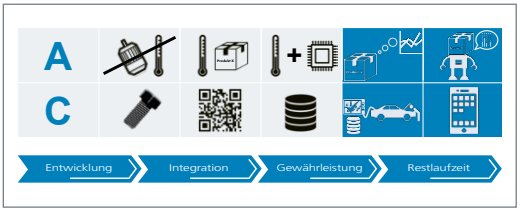
6.4. Etablierung von Zugriffsprozessen

Für jeden Zugriff soll klar definiert sein, welche Aktionen der Akteur ausführen darf. Jegliche Abweichung von diesen Zugriffsprozessen soll zum Beenden der Sitzung führen. Wird die Verbindung innerhalb eines vordefinierten Zeitraums mehrfach hintereinander beendet (z.B. wegen falscher Anmeldedaten), so sollen weitere Zugriffe untersagt und erst dann wieder zugelassen werden, wenn ein Administrator mit entsprechenden Rechten eine erneute Freischaltung vorgenommen hat.



6.5. Übergänge zu anderen Netzen absichern

Will sich ein Akteur mit bereits etablierter Verbindung zu einer Maschinenkomponente von dieser aus in eine weitere Komponente verbinden, so sollen für jede weitere Verbindung dieser Art erneut alle genannten Prozesse zum Aufbau und Beenden der Fernzugriffs-Sitzung sowie zur Etablierung von Zugriffsprozessen ausgeführt werden. Insbesondere soll eine erneute Autorisierung erfolgen, falls sich die Zielkomponente in einem anderen Netzsegment oder einer anderen Zone befindet, siehe hierzu insbesondere auch Abschnitt 3.6. Es bietet sich an, dem Betreiber zusätzlich die Möglichkeit zur Wahl einer Fernwartungsplattform auf Basis von Standarddiensten zu ermöglichen, da der Mehraufwand für den parallelen Betrieb mehrerer Technologien zumeist für den Betreiber sehr hoch ist.



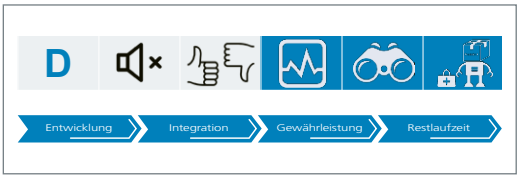
7. Monitoring und Angriffserkennung

Vertrauen ist gut…

Die Annahme einer vollständigen Absicherung der Maschine gegen Angriffe ist auch bei Einsatz von modernster Sicherheitstechnologie unrealistisch. Es sollen daher Funktionen zur Erkennung von Angriffen und anderen sicherheitsrelevanten Ereignissen bereitstehen. Sämtliche aufgezeichneten Daten sollen hierbei möglichst zentral gespeichert werden, um eine spätere Auswertung zu erleichtern.

7.1. Monitoring aller Zugriffe auf Maschinenkomponenten

Zunächst sollen sämtliche Zugriffe auf Maschinenkomponenten erfasst und zur weiteren Verarbeitung gespeichert werden. Insbesondere sollen sämtliche Zugriffe aus nicht-vertrauenswürdigen Netzen protokolliert werden. Auch die Zugriffe von Komponenten auf Dienste innerhalb der Maschine sollen hierbei berücksichtigt werden. Dabei sollen zumindest die Identität der involvierten Akteure/Komponenten, der Zeitpunkt, die Dauer und die Art des Zugriffs für eine spätere Auswertung vorgehalten werden. Das Monitoringsystem sollte vom Produktivsystem getrennt sein. Sollte bereits ein SIEM-System (Security Information and Event Monitoring) beim Betreiber im Einsatz sein, ist die Möglichkeit der Anbindung der Anlage zu prüfen.

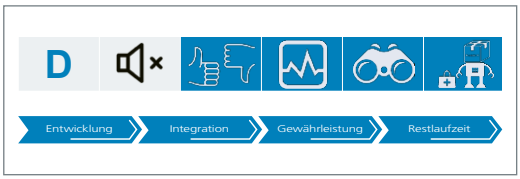


7.2. Funktionen zum Monitoring in Leitstand integrieren

Die Funktionen zum Monitoring von Zugriffen sowie weiterer sicherheitsrelevanter Ereignisse sollen direkt in den Leitstand der Maschine integriert werden, d.h. Leitstände und andere den Maschinen direkt übergeordnete Systeme sollen die Möglichkeit zur Aufzeichnung ebenso unterstützen wie die Maschine selbst. Dies ermöglicht eine direkte Auswertung nach einem erkannten Störfall. Zu sicherheitsrelevanten Ereignissen zählen hier z.B. inkorrekte Passworteingaben, Ressourcenüberlastung, unbefugte Zugriffsversuche oder auch Änderungen in sicherheitsrelevanten Konfigurationsdateien (vgl. auch die IT-Grundschutz-Kataloge des BSI[5]) .

Der Leitstand wird somit zur zentralen Komponente der Erfassung und Verarbeitung sicherheitsrelevanter Daten. Bei Entwurf und Entwicklung der Maschine sollte deshalb die zusätzliche Kommunikationslast zu dieser Komponente berücksichtigt werden, da im Falle komplexer und verteilter Maschinen ein erheblicher Datendurchsatz entstehen kann.

Ferner soll darauf geachtet werden, dass sämtliche erfasste Ereignisse keinerlei sensible Daten (wie z.B. Schlüsselmaterial) enthalten (siehe auch das BSI ICS-Kompendium für Hersteller und Integratoren[6]).



7.3. Virenscanner

Die direkt mit der Maschine verbundenen Rechner sind oftmals Einfallstor für Programme mit Schadwirkung (Malware). Es empfiehlt sich daher der Einsatz von Virenscannern auf diesen Komponenten. Gängige Virenscanner erkennen Angriffe mittels einer vordefinierten Malware-Signatur. Solche regelbasierten Methoden zur Angriffserkennung haben den Vorteil, dass sie bereits bekannte Angriffsmuster relativ zuver-

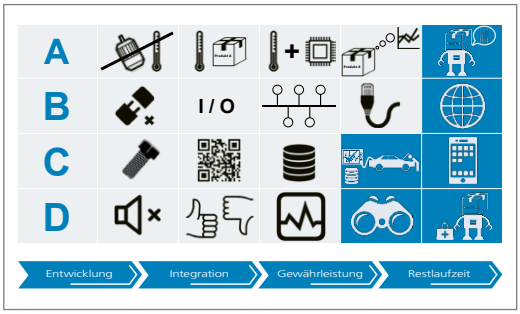
[5] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/kataloge.html
[6] https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/Empfehlungen/ICS/empfehlungen_node.html

lässig identifizieren. Bei der Erkennung neuartiger Schadsoftware, für die noch keine Signaturen generiert wurden, liefern diese Methoden hingegen eine ungenügende Erkennungsrate. Um einen rudimentären Schutz vor gängigen Schadprogrammen zu gewährleisten, sollen die Signaturen regelmäßig aktualisiert werden. Um die Leistungsfähigkeit der Rechner nicht durch zu hohe Scan-Last zu beeinträchtigen, bieten fast alle Hersteller die Möglichkeit, adaptive Scans zu definieren, die bekanntermaßen Schadsoftware-freie Bibliotheken auf Basis ihrer Signatur vom Scan ausschließen.

7.4. Netzwerk IDS und Anomalieerkennung bei komplexen Maschinen

Um auch neuartige, noch nicht bekannte Angriffsmuster zu erkennen, sollen zusätzliche Maßnahmen zur Anomalieerkennung integriert werden. Dieser Ansatz geht von einem Normalverhalten der Maschine aus und erkennt von diesem abweichendes Fehlverhalten als Anomalie. Während solche Methoden in komplexen Netzwerken (z.B. im Office-Netz) oftmals Falschmeldungen generieren, eignen sie sich gut für Maschinennetze, deren Grundverhalten oftmals wesentlich gleichförmiger ist und eine einfachere Charakterisierung zulässt. Normalverhalten der Maschine kann dabei anhand vielfältiger Eigenschaften definiert werden, z.B. durch Muster in der Netzwerkkommunikation, Benutzerverhalten, Aktivität der Maschinenmodule, Sensordaten, oder System-Log-Dateien.

Es sollen Intrusion-Detection Systeme (IDS) und Intrusion-Prevention Systeme (IPS) zur Netzüberwachung von komplexen Maschinen eingesetzt, bzw. deren Einsatz durch den Betreiber ermöglicht werden. Insbesondere sollen besonders exponierte Komponenten mit entsprechender Funktionalität versehen werden, um auf Grundlage von Heuristiken ungewünschtes Verhalten zu erkennen. Es bleibt anzumerken, dass die im Anlagennetz genutzten Protokolle oftmals nicht ausreichend oder gar nicht mit den heute verfügbaren IDS/IPS Lösungen erkannt und verarbeitet werden können. Hier besteht dringender Kooperationsbedarf, um auf Protokollebene schadhafte Pakete automatisiert identifizieren zu können.



8. Wiederherstellungsplan

Plan B

Der Anlagenhersteller sowie der Integrator sollen einen Wiederherstellungsplan definieren, der im Fall einer Störung oder eines Angriffs die Anlage in einen vertrauenswürdigen Zustand zurücksetzt.

8.1. Erstellung von Backup-Systemen

Backup-Systeme sind Speichersysteme, die die Sicherung sämtlicher Daten der Maschine ermöglichen. Backup-Systeme sollen fest in den Entwicklungsprozess der Maschine integriert werden und es wird empfohlen, durch mehrfache Sicherheitskopien ein angemessenes Maß an Datenverfügbarkeit und Ausfallsicherheit zu gewährleisten. Werden zentrale Backup-Server für die Speicherung genutzt, so soll die Maschine über Funktionen zum sicheren Datenaustausch mit diesen Servern verfügen.

8.2. Erstellung regelmäßiger Backups

Sämtliche für den Betrieb der Maschine notwendigen Daten sollen in regelmäßigen Abständen auf Backup-Systemen gesichert werden. Die Zeitintervalle und Verschlüsselungsanforderungen sollen dabei, auf Basis der Bedrohungslage und des Schutzbedarfs, angemessen von Integrator oder Betreiber festgelegt werden.

8.3. Prüfung von Backups auf Wiederherstellbarkeit

Sämtliche Backups sollen auf Wiederherstellbarkeit geprüft werden. Diese Prüfung soll regelmäßig erfolgen. Es soll durch Redundanz der Backup-Systeme garantiert werden, dass im Falle der Nicht-Wiederherstellbarkeit auf ein weiteres Backup ausgewichen werden kann.

8.4. Wiederherstellung eines vertrauenswürdigen Zustandes nach Störung/Angriff

Nach einem Angriff ist es erforderlich, die Maschine wieder in einen vertrauenswürdigen Zustand zu bringen. Die regelmäßig erstellten Backups ermöglichen die Wiederherstellung eines Maschinenzustandes vor dem Zeitpunkt des Störfalls. Es wird weiter empfohlen, auch direkt von der betroffenen Maschine abhängige Komponenten zu überprüfen und gegebenenfalls auch diese in den entsprechend vertrauenswürdigen Zustand zurück zu setzen.

8.5. Wiederherstellung von verschlüsselten Daten

Bei der Wiederherstellung der Maschine in einen vertrauenswürdigen Zustand werden einige Daten nur verschlüsselt vorliegen. Die Backup-Systeme sollen die Wiederherstellung der verschlüsselten Daten ermöglichen.

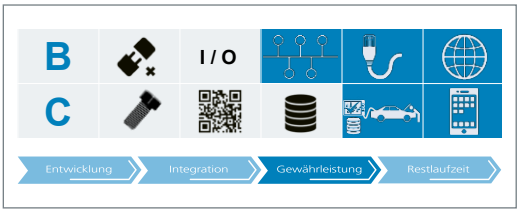
9. Sicherer Produkt-Lebenszyklus

Vom Design bis zum Phase-out

Der Anlagenhersteller soll einen sicheren Maschinen-Lebenszyklus definieren und gewährleisten. Wie eingangs in Abschnitt 1 erwähnt, sollte das Produkt idealerweise einer regelmäßigen Risikoanalyse unterzogen werden. Dies ist für den Mittelstand oft aufgrund fehlender Ressourcen eine gewisse Herausforderung. Um dennoch einen sicheren Produkt-Lebenszyklus der Maschine zu gewährleisten, sind die folgenden praktischen Maßnahmen zu beachten.

9.1. Beobachtung von Schwachstellen

Maschinenhersteller, -integrator und -betreiber sollen neu bekannt gewordene Angriffsvektoren hinsichtlich ihres Gefährdungspotentials einordnen können. Insbesondere soll eine schnelle Abschätzung erfolgen, ob eine neu bekannt gewordene Schwachstelle für eine Maschinenkonfiguration relevant ist. Aufgrund von teils sehr komplexen Maschinenkonfigurationen mit vielfältigen Komponentenklassen sollte hierzu ein Maschineninventar geschaffen werden. Es sei darauf hingewiesen, dass die Inventarisierung seitens des Herstellers regelmäßig nur den Inbetriebnahmezustand festhalten kann. Insofern kann die Verantwortung zum Führen eines solchen Inventars auf den Betreiber der Anlage übergehen, insbesondere bei Änderungen an der Konfiguration durch den Betreiber.



9.2. Beobachtung der Bedrohungslage durch die Hersteller

Über die Beobachtung von aktuellen Schwachstellen hinaus sollte sich der Hersteller der aktuellen Bedrohungslage bewusst sein und dies in die Entwicklung neuer Maschinen einfließen lassen. Häufen sich zum Beispiel konkrete Angriffe auf eine in der Maschine verbaute Komponentenklasse, ohne dass die Maschine direkt davon betroffen ist, so sollte der Hersteller dennoch über Kenntnis entsprechender Schutzmaßnahmen verfügen.

Der Anlagenhersteller soll anhand dokumentierter Bedrohungsmodelle gewährleisten, dass die Security-Funktionen der Anlage den Schutzbedarf angemessen erfüllen (siehe hierzu auch Abschnitt 16).

9.3. Reaktionsfähigkeit auf Schwachstellen

Die Beobachtung von konkreten Schwachstellen und der allgemeinen Bedrohungslage soll den Hersteller/Integrator befähigen, auf bekannt gewordene Schwachstellen zeitnah reagieren und Maschinen und Anlagen gegen neue Gefährdungen schützen zu können. Eine angemessene Reaktionsfähigkeit setzt zumindest eine vordefinierte Vorgehensweise bei Bekanntwerden einer Schwachstelle voraus. So sollen innerbetriebliche Prozesse definiert werden, die gegebenenfalls jederzeit eingeleitet werden können.

9.4. Festlegen der betrieblichen Kommunikationskanäle

Zu den innerbetrieblichen Prozessen zählt insbesondere die Festlegung der Kommunikationskanäle. Es soll klar definiert sein, an welche Stelle des Betriebes extern entdeckte Schwachstellen berichtet werden können. Des Weiteren soll klar festgelegt werden, wie und an wen diese Information innerhalb des Betriebes kommuniziert werden soll. Was die außerbetriebliche Kommunikation betrifft, so ist zu empfehlen

dass der Hersteller/Integrator die Betreiber der betroffenen Maschinenserie frühzeitig von identifizierten Schwachstellen in Kenntnis setzt.

9.5. Patchmanagement

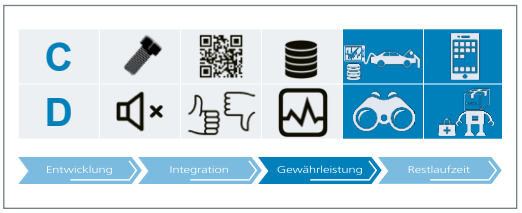
Um die Anpassung der Anlage auf neue Gefährdungslagen und bekannt gewordene Schwachstellen zu gewährleisten, soll der Anlagenhersteller einen sicheren Prozess zur Handhabung und Integration von Patches definieren. Dies beinhaltet auch, dass alle dazu notwendigen Ressourcen im Vorhinein eingeplant werden. Des Weiteren sollen Verteilmechanismen für den Patch definiert werden, die eine zeitnahe Einbringung ermöglichen. Hierzu sollte eine Infrastruktur für die Patchverteilung an die Betreiber vorhanden sein, die ihrerseits wiederum Prozesse und Infrastrukturen für die Annahme, das Testen und die Installation der Patches vorhalten sollen.

9.6. Benennung von internen und externen Verantwortlichen

Für den effizienten Ablauf aller geforderten Prozesse ist die Benennung von internen und externen Verantwortlichen notwendig. Es sollen Personen benannt werden, die für die Einschätzung einer eingehenden Schwachstellenmeldung, für die Entwicklung und für die Auslieferung der Patches verantwortlich sind. Den Verantwortlichen sollen Befugnisse eingeräumt und notwendige Mittel bereitgestellt werden, um das Patchmanagement effizient koordinieren zu können.

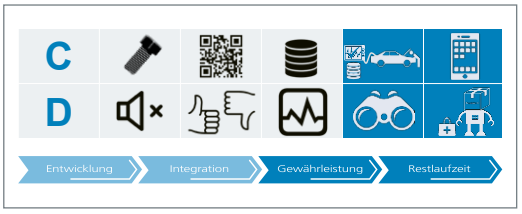
9.7. Umgang mit End Of Support (EOS)

Endet der Support für eine Maschine, sollen hierzu klar definierte Prozesse definiert werden. Sofern möglich soll der Integrator den Betreiber frühzeitig darüber in Kenntnis setzen, dass der Support insbesondere in Form von Patches ausläuft. Da abhängig von der Einsatzumgebung mit sehr langen Betriebszeiten der Maschine über einige Jahre hinweg zu rechnen ist, sollte der Zeitpunkt des EOS idealerweise schon zu Beginn der Anlagenplanung bekannt sein.



9.8. Phase-out Management

Für das Ende des Betriebes der Maschine soll ein sicherer Phase-out-Prozess definiert sein. So soll insbesondere sichergestellt sein, dass keine sensiblen Daten an unbefugte Dritte gelangen. Als wichtigster Punkt ist hier die Zerstörung sämtlicher Massenspeicher der Maschine zu nennen. Ferner kann die Zerstörung von besonders kritischen Komponenten das Risiko von Reverse-Engineering senken.



10. Anpassung und Prüfung der Komponenten

Survival of the fittest

Die Anlage soll regelmäßig hinsichtlich ihrer definierten Security-Funktionalität überprüft werden, um ihre Robustheit auch in einem sehr dynamischen Umfeld zu gewährleisten.

10.1. Anpassen der Standard-Einstellungen

Bei initialer Einrichtung sowie bei jeder Wiederherstellung in einen vertrauenswürdigen Zustand soll darauf geachtet werden, dass die Standard-Einstellungen angepasst werden. So sind häufige Einfallstore z.B. Standardpasswörter für Administrator-Accounts (siehe Abschnitt 3) oder nicht aktivierte Security-Funktionen im Auslieferungszustand. Die Security-Funktionen der Maschine und deren sichere Konfiguration sind dabei vollständig in der Dokumentation gelistet (siehe Abschnitt 16). Die Anpassungen bzw. Einstellungen sollen sämtlich für nachfolgende Prüfungen protokolliert werden.

Die Anpassung der Standardeinstellungen soll sicherstellen, dass die neue Konfiguration der Bedrohungslage angemessen ist.

10.2. Anpassen der Hardwarekonfiguration

Ist die Maschine in verschiedenen Hardwarekonfigurationen verfügbar, so soll noch vor Integration überprüft werden, ob die der Bedrohungslage angemessene Security-Funktionalität von der angestrebten Konfiguration erreicht wird.

10.3. Zugriff auf das Internet innerhalb des ICS-Netzwerks

Es soll überprüft werden, ob ein Zugriff auf das Internet innerhalb des Anlagennetzes möglich ist. Ist dies der Fall soll ferner geprüft werden, ob hierbei der Zugriff der definierten Security-Funktionalität der Anlage widerspricht und ob die zugreifende Komponente ausreichend von kritischen Teilen der Maschine isoliert ist.

10.4. Prüfungen zur Verifikation und Validierung

Es soll sowohl eine Verifikation der Security-Funktionen der Anlage stattfinden (Spezifikationsabgleich), als auch eine Validierung, (d.h. eine Überprüfung der Tauglichkeit der Security-Funktionen). Eine solche Prüfung kann das Auftreten von Schwachstellen zwar meist nicht ausschließen, jedoch stark reduzieren. Eine sorgfältige Testdurchführung erfordert zunächst die Erstellung eines Testplans, der Grundlage für die Testvorbereitung ist, welche die Planung von Testfällen und -szenarien beinhaltet (siehe auch das BSI ICS-Kompendium für Hersteller und Integratoren[7]). Die Testdurchführung kann sehr umfangreich ausfallen und soll von den jeweiligen Verantwortlichen veranlasst werden. Die Ergebnisse der Prüfung sollen dokumentiert werden.

[7] https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/Empfehlungen/ICS/empfehlungen_node.html

10.5. Prüfung der Software- und Informationsintegrität

Die Integrität jeglicher Softwarekomponenten sowie Konfigurationsdaten der Maschine soll gewährleistet sein. Hierzu bieten sich elektronische Signaturen an, die bei jedem Einlesen der Konfigurationsdaten und bei jeder Ausführung von Programmen überprüft werden. Die eingesetzten Signaturverfahren sollen bezüglich Parameter und kryptographischem Material dem Stand der Technik genügen (siehe Abschnitt 14).

10.6. Auswahl sicherer Komponenten

Oftmals werden externe Komponenten von Zulieferern in die Maschine integriert. In solchen Fällen soll vom Integrator geprüft werden ob die externen Komponenten den identifizierten Security-Anforderungen genügen (siehe auch Abschnitt 15). Eine solche Beurteilung kann sowohl anhand von Zertifizierungen der zugelieferten Komponenten, als auch von geschulten Entwicklern (siehe Abschnitt 17) getroffen werden. Werden Zertifizierungen zur Prüfung herangezogen, so sollte darauf geachtet werden, dass die Gültigkeit des Zertifikats mindestens bis zur Inbetriebnahme gegeben ist und der Umfang der Prüfung für den Einsatzzweck in der Anlage genügt.

11. Verzicht auf überflüssige Komponentenfunktionen

So wenig wie möglich, so viel wie nötig

Es kommt oft vor, dass Maschinen als Ganzes oder einzelne Komponenten innerhalb der Anlage über eine Reihe von Funktionen verfügen, die für den Betrieb in bestimmten Einsatzumgebungen nicht in Anspruch genommen werden. Solche im Anwendungsfall überflüssigen Produktfunktionen können die Angriffsoberfläche signifikant vergrößern und sind oft Einfallstor für Angreifer. Deshalb soll auf solche Funktionen, die für den jeweiligen Einsatzbereich der Maschine nicht relevant sind, verzichtet werden.

11.1. Entfernen von unnötiger Software und Diensten

Als erstes sollten sämtliche Dienste und Softwarekomponenten, die nicht unmittelbar für den Betrieb der Maschine notwendig sind, entfernt werden. Ist eine Entfernung nicht möglich, ist die Deaktivierung von nicht benötigten Softwarekomponenten denkbar, die sich je nach Produkt jedoch sehr aufwändig gestalten kann (insbesondere bei Software von Zulieferern). Die Auswahl der tatsächlich aktiven Software soll flexibel und für den Integrator und Betreiber leicht zugänglich umgesetzt werden. Insbesondere sollten Funktionsabhängigkeiten automatisch aufgelöst werden. Im Idealfall wählt der Integrator die zum Betrieb notwendigen Funktionen aus und lediglich diese sowie die davon abhängigen Funktionen/Softwareteile werden in die Maschine eingebracht.

11.2. Entfernung/Deaktivierung aller nicht verwendeten Hardwarekomponenten

Ebenso soll möglichst auf nicht verwendete Hardwarekomponenten verzichtet werden. Je nach Maschine kann eine spezielle Anpassung der Hardwarekonfiguration sehr aufwändig sein. Deshalb sollen sich sämtlichen Hardware-Komponenten der Maschinen zumindest deaktivieren lassen (z.B. nicht benötigte Schnittstellen). Wie bei der Entfernung von unnötiger Software und Diensten deaktiviert die Maschine idealerweise sämtliche aktuell nicht genutzten Hardwarekomponenten automatisch.

12. Komponentenhärtung

Eine Kette ist so stark wie ihr schwächstes Glied

Durch zunehmende Vernetzung und intelligentere Funktionen lässt sich Security nicht mehr ausschließlich mittels Abschottung implementieren. Sichere, gehärtete Komponenten werden dabei eine immer größere Rolle spielen.

12.1. Komponenten dürfen nur gehärteten Code ausführen

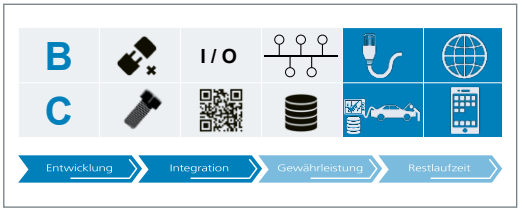
Es sollen nur solche Programme auf der Maschine ausgeführt werden, deren Entwicklungsprozess ein Mindestmaß an Qualitätskriterien berücksichtigt. Hiermit soll sichergestellt werden, dass die Softwarekomponenten einem angemessenen Qualitätsstandard entsprechen. Allgemeiner wird empfohlen, die Programme gemäß dem Stand der Technik des Softwareengineerings zu entwickeln und zu warten. Der VDMA hat dazu einen Leitfaden „Softwarequalitätssicherung“ veröffentlicht[8]. Zudem können als Leitfäden für Qualitätskriterien und die Bewertung von Softwareprodukten sowohl die Norm ISO/IEC 25000 (”Software engineering – Software product Quality Requirements and Evaluation (SQuaRE) – Guide to SQuaRE”) als auch die zugehörige Normenreihe ISO/IEC 250xx herangezogen werden.

12.2. Sicherheitstests als integraler Bestandteil bei der Entwicklung und Systemintegration

Sicherheitsanalysen sollen integraler Bestandteil bei Entwicklung und Anlagenintegration sein. Zunächst sollen mit Fuzzingtools sämtliche als kritisch eingestufte Softwareschnittstellen (APIs) sowie Netzwerkschnittstellen getestet werden. Das randomisierte Testen mit strukturierten aber ungültigen Eingaben deckt oftmals bereits wesentliche Schwachstellen auf, die dann vom Entwickler behoben werden können. Des Weiteren sollen Tools zur statischen Codeanalyse Verwendung finden. Diese unterstützen die Beseitigung häufiger Programmierfehler. Zusätzlich zu diesen automatisierten Herangehensweisen sollen ferner manuelle Codeanalysen vorgenommen werden. Dies kann dadurch geschehen, dass geschulte Entwickler (siehe Abschnitt 17) innerhalb der Entwicklungsabteilung den Quellcode gegenprüfen.

12.3. DoS Schutz

Eine spezielle Gefahr für die Anlage stellt der „Denial of Service“ (DoS) dar, der eine Blockade des von der Anlage angebotenen Dienstes bedeutet. Neben speziellen Angriffsmethoden wird ein DoS mit Abstand am häufigsten durch eine Überlastung der Infrastruktur hervorgerufen, z.B. durch massenweises Versenden von Anfragen an den Dienst. Wird der Beginn eines DoS Angriffes erkannt, so sollen automatisch entsprechende Sperrlisten der Absenderadressen in die Firewall (siehe Abschnitt 2) eingetragen werden. Falls möglich sollen die Dienste durch Serverlastverteilung auf mehrere virtuelle Instanzen verteilt werden, um bei Ausfall eines einzelnen physischen Rechners die Last effektiv auf noch intakte Instanzen verteilen zu können. Über weitere Maßnahmen (wie z.B. die Erkennung von IP-Spoofing gemäß RFC 2267 oder SYN-Cookies) sollen die Entwickler in den jeweiligen Schulungen (siehe Abschnitt 17) unterrichtet werden.



[8] http://www.vdma-verlag.com/home/p123.html

12.4. Application Whitelisting und Blacklisting

Durch Application-Whitelisting wird die Angriffsfläche der Anlage weiter reduziert. Dies kann z.B. dadurch geschehen, dass nur (vom Maschinenhersteller) signierte Programme auf der Maschine ausgeführt werden dürfen. Dabei wird vor jedem Programmstart geprüft, ob die Programmsignatur korrekt verifiziert werden kann und ob der Aussteller auf der Whitelist eingetragen ist. Mit Application-Whitelisting lassen sich sehr flexible wie auch restriktive Policies zur Programmausführung umsetzen.

Analog zum Whitelisting kann auch das Blacklisting hinzugezogen werden, das heißt der Ausschluss von bekannt schadhaften oder prinzipiell nicht erlaubten Programmen (etwa Internet Explorer, Java, Flash). Blacklisting erfordert regelmäßige Aktualisierungen der Liste und daher einen entsprechenden Updateprozess in der Anlage.

12.5. Reduzierung der Systemkomplexität

Bei der Entwicklung der Maschine soll darauf geachtet werden, dass die Komplexität der Komponenten und des Gesamtsystems möglichst gering gehalten wird. Zunächst ist hier die Funktionsreduzierung zu nennen, die in Abschnitt 11 gesondert behandelt wird. Außerdem sollen ähnliche Funktionengruppen in Modulen und Komponenten zusammengefasst werden. Eine solche Zusammenfassung ermöglicht es oft, die Abstraktionsebenen der Maschinenfunktionen auf Komponenten abzubilden. Dies erleichtert die Wartbarkeit, Weiterentwicklung und Modifikation der Maschinen und verringert letztendlich die Angriffsfläche.

12.6. Absicherung von Feldgeräten außerhalb der Anlage gegen physische Angriffe

Ist die Maschine als verteiltes System implementiert, so soll die Absicherung von entfernten Feldgeräten außerhalb der Anlage gewährleistet sein. Hierzu zählt insbesondere die Absicherung gegen physische Angriffe. Bei entfernten Komponenten mit besonders hohem Schutzbedarf ist hier gegebenenfalls der Einsatz von Hardware-Sicherheitsmodulen (HSM) zur sicheren Aufbewahrung von sensiblem Schlüsselmaterial notwendig.

12.7. Absichern der elektronischen externen Schnittstellen

Sämtliche digitalen, externen Schnittstellen der Maschine sollen gegen vom Hersteller nicht beabsichtigte Zugriffe abgesichert sein.

Eine solche Absicherung erfolgt zunächst auf Basis einer vollständigen Identifikation und Dokumentation aller implementierten Schnittstellen. Um auch solche Schnittstellen zu erfassen, die durch andere Systeme aufgerufen werden, sollen insbesondere auch alle Kommunikationswege zu externen Softwaremodulen definiert werden. Diese sind in Form eines Kontextdiagramms nachvollziehbar zu dokumentieren.

Eine besondere Klasse stellen hier Debugschnittstellen dar, die oftmals von Angreifern mit direktem Zugang zur Maschine ausgenutzt werden. In einem ersten Schritt sollen deshalb zunächst alle Debugschnittstellen (wie z.B. IEEE 1149.1 JTAG, Background Debug Mode (BDM) oder auch USB Schnittstellen) identifiziert und dokumentiert werden. Die Behandlung solcher Debugschnittstellen hängt vom zu erwartenden Angreifermodell ab.

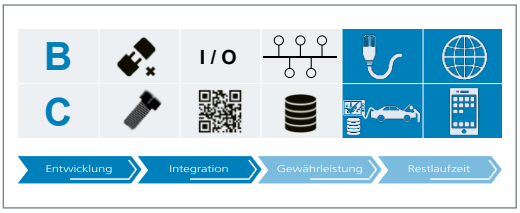
13. Isolationstechniken innerhalb der Maschine / Virtualisierung

Fein säuberlich getrennt

Um die Auswirkungen eines Störfalls innerhalb der Maschine weitestgehend zu reduzieren, sollen die einzelnen Softwarekomponenten mittels geeigneter Isolationstechniken voneinander getrennt werden. Hierbei können sowohl Virtualisierungslösungen als auch Trusted Execution Environments (TEE) zum Einsatz kommen. Die Umsetzung dieser Techniken kann sich in bestimmten Maschinenkonfigurationen als anspruchsvoll erweisen.

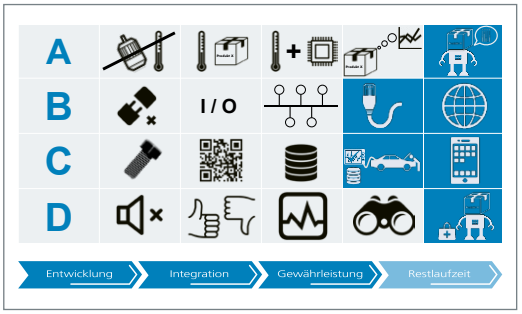
13.1. Schutz vor Schadcode durch Sandboxing und Virtualisierung

Oft können die Störungen durch Schadcode dadurch begrenzt werden, dass Maschinenprogramme in einer Sandbox oder einer virtuellen Umgebung ausgeführt werden. Erstens lassen sich dadurch die Rechte und Funktionen, die dem jeweiligen Programm zur Verfügung stehen, gezielt einschränken. Dies hat oft eine stark reduzierte Angriffsfläche zur Folge. Zweitens beschränken sich die Auswirkungen eines erfolgreichen Angriffs meist auf die lokale virtuelle Umgebung. Zwar sind genügend Angriffe bekannt, die gezielt gegen die Virtualisierungslösungen gerichtet sind (z.B. Angriffe auf Hypervisoren). Das Ausbrechen aus der isolierten Umgebung stellt jedoch für viele der gängigen Schadprogramme eine effektive Hürde dar.



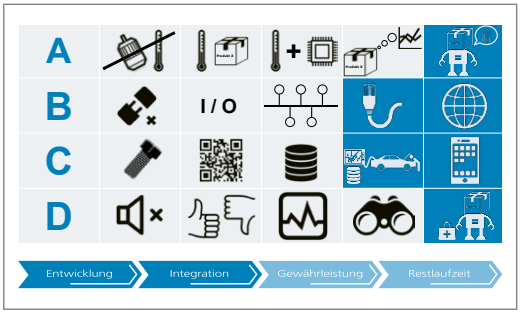
13.2. Die Maschine soll Restriktionen für „mobilen Code“ implementieren

Unter „mobilem Code“ sind hier oft ausgetauschte Programme und Skripte (z.B. in Java(Script), ActiveX oder VBScript) gemeint, die erheblichen Schaden innerhalb der Maschine anrichten können. Ähnlich wie im Abschnitt 12.4 beschrieben sollen deshalb nur Programme mit vertrauenswürdigem Ursprung ausgeführt werden. Eine schwächere Variante dieser Empfehlung ist die Ausführung von Programmen unbekannter Herkunft mit stark reduzierten Rechten. Durch Sandboxing und Virtualisierung lassen sich Programme in Umgebungen mit vordefinierter und eingeschränkter Funktionalität ausführen.



13.3. Abgrenzung der Betriebs- und Konfigurationsdaten von Anwendungsprogrammen

Durch Virtualisierungstechniken ist es insbesondere möglich, Betriebs- und Konfigurationsdaten von Anwendungsprogrammen zu isolieren. Da auf solche Daten oft von mehreren Maschinenkomponenten zugegriffen wird, kann so das Risiko der Kompromittierung großer Teile der Maschine durch schadhafte Manipulation der Konfigurationsdaten weitestgehend minimiert werden.



14. Kryptographie

Das Buch mit standardisierten Siegeln

Basis für die Nutzung sicherer Protokolle, für Authentisierungsmaßnahmen und für die Absicherung von Funktechnologien ist die Verwendung von sicheren kryptographischen Verfahren. Es soll gewährleistet sein, dass sämtliche kryptographischen Algorithmen und Parameter dem Stand der Technik entsprechen. In diesem Abschnitt wird auf die Auswahl geeigneter Algorithmen und Parameter eingegangen.

14.1. Implementierung von standardisierten Algorithmen

Die Entwicklung sicherer kryptographischer Algorithmen ist ein aufwändiger Prozess, der insbesondere die Kryptoanalyse durch Spezialisten beinhaltet. Es wird deshalb dringend von Eigenentwicklungen abgeraten. Zusammenstellungen und Empfehlungen ausgereifter und aktuell sicherer Verfahren und Parameter werden von öffentlichen Stellen bereitgestellt. So

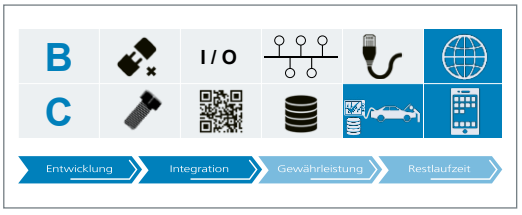
Es wird dringend von kryptographischen Eigenentwicklungen abgeraten.

werden z.B. in den entsprechenden Dokumenten des BSI [9, 10], des NIST[11] und der Bundesnetzagentur[12] Empfehlungen zu kryptographischen Verfahren und Schlüssellängen ausgesprochen. Bei der Auswahl soll der Produktlebenszyklus der Anlage herangezogen werden, um bei langer Einsatzdauer über viele Jahre hinweg auch die Entwicklung der Rechenleistung berücksichtigen zu können. Die Schlüssellänge soll entsprechend der geplanten Einsatzdauer gewählt werden. Verfahren zum Austausch bzw. zur Aktualisierung der Cipher Suites sind nach Möglichkeit bereit zu stellen.

14.2. Einbindung in bestehende PKI

Der Anlagenhersteller soll gewährleisten, dass die Anlagen in bestehende PKI integriert werden können. Insbesondere sollen bestehende Zertifikate bereits existierender PKI Verwendung finden können. Hierfür soll ein sicheres Verfahren zur Erzeugung, Einbringung und Handhabung des entsprechenden kryptographischen Materials definiert werden. Die Bereitstellung eines bzw. die Möglichkeit zur Nutzung eines Certificate Lifecycle Management (CLM) beim Betreiber ist vorzusehen, sodass Zertifikate im laufenden Betrieb aktualisiert werden können. Auf Microsoft Windows basierende Komponenten können hierbei Simple Certificate Enrollment Protocol (SCEP) und Network Device Enrollment Service (NDES) als Protokolle nutzen, falls eine Microsoft CA zum Einsatz kommt.

Bei der Validierung von Zertifikaten ist darauf zu achten, Inhaber, Aussteller und Gültigkeitsstatus zu überprüfen. Ferner sollen die Zertifikatsketten vollständig geprüft und möglichst wenige Root-Zertifikate in die Liste der vertrauenswürdigen Zertifikate aufgenommen werden. Da sich die Funktionsweise einer Certificate Revocation List (CRL) im Umfeld der Maschine zu Maschine (M2M) Kommunikation durch teilweise hohe Änderungshäufigkeit und damit schnell wachsende Listenlängen als nicht zielführend erweist, ist die Nutzung von OCSP (Online Certificate Status Protocol) zu erwägen.



[9] BSI TR-03111 „Elliptic Curve Cryptography“
[10] SI TR-02102-1 ”Kryptographische Verfahren: Empfehlungen und Schlüssellängen”
[11] http://csrc.nist.gov/groups/ST/toolkit/
[12] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen)

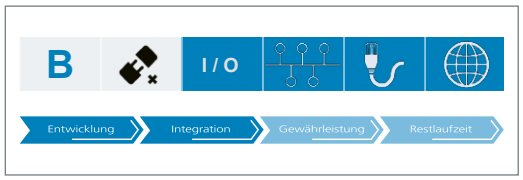
15. Bestimmung der Security-Anforderungen für Lieferanten und Zulieferer

Erkläre und fordere was du haben willst

Werden zugelieferte Komponenten in Anlagen integriert und entsprechen diese Komponenten nicht den identifizierten Security-Anforderungen, so kann das Security-Konzept der Maschine dadurch unterlaufen werden. Als schwächstes Glied in der Kette bieten sich solche Komponenten oftmals als erster Einstiegspunkt für Angreifer da. Es sollen daher geeignete Regelungen für sichere Drittkomponenten und einen sicheren Integrationsprozess von zugelieferten Komponenten definiert werden.

15.1. Überprüfung der Security-Anforderungen an zugelieferte Komponenten

Die vom Hersteller/Integrator der Anlage identifizierten Security-Anforderungen sollen von jeder zugelieferten Komponente im Rahmen ihres Funktionsbereichs erfüllt werden. Die Überprüfung der Security-Anforderungen kann dabei vom Integrator, vom Zulieferer oder in gemeinsamer Zusammenarbeit erfolgen. Bei streng vertraulichen Projekten wird der Integrator die Überprüfung anhand der vom Zulieferer bereitgestellten Dokumentation vornehmen. Ist dies nicht erforderlich, so ist auch eine erste Konformitätsabschätzung in Form eines Angebots seitens des Zulieferers denkbar. Es soll sichergestellt sein, dass die zugelieferte Komponente dem identifizierten Schutzbedarf genügt. Dafür können auch Konformitätsprüfungen oder Auditergebnisse von Dritten herangezogen werden.

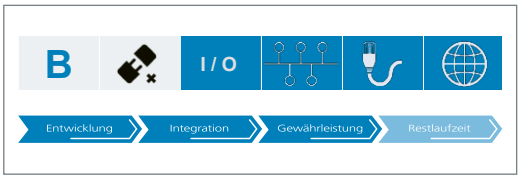


15.2. Identifikation der eigenen Rolle als Zulieferer

Wird eine Maschine wiederum als Unterkomponente in ein weiteres Produkt integriert, so soll der Hersteller eine Dokumentation aller Schutzmaßnahmen an den Kunden übergeben. Die Dokumentation soll eine Überprüfung ermöglichen, ob die auszuliefernde Komponente dem Schutzbedarf des Zielsystems entspricht. Der Hersteller sollte sich seiner eigenen Rolle als Zulieferer bewusst sein und dementsprechende Organisationsprozesse definieren. Dies kann die Überprüfung von Security-Anforderungen an die auszuliefernde Maschine mit entsprechendem Lieferangebot sein, aber auch die Dokumentation und Offenlegung des Schutzkonzeptes.

15.3. Ausgelagerte Softwareentwicklung

Werden Software oder Teile davon von Dritten zur Verfügung gestellt – dies betrifft insbesondere auch Bibliotheken und Code aus offenen Repositories – sind diese in den sicheren Entwicklungsprozess mit einzubeziehen. Dabei sind Kontrollmechanismen zu etablieren, die einerseits die Umsetzung der eigenen Security-Maßnahmen auch im Drittprodukt sicherstellen, andererseits auch das Potential für Schwachstellen oder bewussten Schadcode minimieren. Auch fremde Systemteile sind hier in die Risikobewertung mit einzubeziehen, daher sind die hierfür notwendigen Informationen zu diesen Teilen einzuholen.



16. Dokumentation

Wer schreibt der bleibt

Die reibungslose Umsetzung aller genannten Sicherheitsmaßnahmen kann nur dann geschehen, wenn diese vollständig dokumentiert werden.

16.1. Schnittstellen

Sämtliche sicherheitsrelevanten Schnittstellen sollen identifiziert und dokumentiert werden. Hierzu zählen insbesondere auch Debug-Schnittstellen in Hardware und Software.

16.2. Etablierte Prozesse

Sämtliche im Verlauf dieses Dokumentes benannten organisatorischen und technischen Prozesse sollen identifiziert und dokumentiert werden. Aus der Dokumentation sollen der organisatorische Ablauf und die zuständigen Rollen hervorgehen. Es soll auch eine mit dem Prozess nicht vertraute Person erkennen können, wie in einer der genannten Situationen zu verfahren ist. Die etablierten Prozesse sollen intern dokumentiert werden.

16.3. Dokumentation der Risikoanalyse

Die Ergebnisse der Risikoanalysen (siehe Abschnitt 1) sollen dokumentiert und für den späteren Gebrauch archiviert werden. Dazu zählen auch insbesondere dokumentierte Bedrohungsmodelle. Aus der Dokumentation sollte hervorgehen, welche Methode der Risikoanalyse zu Grunde lag und auf Basis welcher Information die Abschätzung von Auswirkung und Wahrscheinlichkeit der Angriffe stattgefunden hat. Eine offengelegte Risikoanalyse kann von Angreifern dazu genutzt werden, die Bedrohungen mit größtem Schadenspotential zu identifizieren. Deshalb soll die Risikoanalyse nur intern dokumentiert werden. Lediglich die resultierenden Anforderungen an Schutzmaßnahmen und Schutzbedarf sollen in die externe Dokumentation einfließen.

16.4. Rechteverteilung

Die Verteilung der Rechte auf die in Abschnitt 3 definierten Akteure soll dokumentiert werden. Insbesondere sollen Änderungen in der Rechteverteilung protokolliert und für spätere Sicherheitsanalysen herangezogen werden können.

16.5. Maschineninventar

Der Hersteller soll ein Maschineninventar erstellen, das sämtliche relevanten Geräte-, Kommunikations- und Managementaspekte (Hard- und Software inklusive) berücksichtigt. Idealerweise ist die Maschine in der Lage, einen Report über die momentan installierten Komponenten mitsamt deren Eigenschaften zu generieren. Eine schematische Auflistung der Komponenten soll den funktionalen Zusammenhang zwischen den Komponenten veranschaulichen.

16.6. Dokumentmanagement

Es sollen organisatorische Prozesse zur Erstellung, Verteilung und Veröffentlichung von Dokumenten definiert werden. Relevante Dokumente sollen in regelmäßigen Abständen auf Aktualität überprüft werden.

16.7. Sicherheitsvorfälle

Sämtlichen Sicherheitsvorfälle sollen dokumentiert und archiviert werden. Hierzu zählen Vorfälle innerhalb der Organisation, wenn möglich aber auch Sicherheitsvorfälle, die bei bereits im Betrieb befindlichen Maschinen beobachtet wurden. Die Dokumentation der Sicherheitsvorfälle soll zunächst intern erfolgen. Sind von dem Sicherheitsvorfall auch Dritte betroffen oder bewirkt die Ursache des Vorfalls eine Gefahr für die Umwelt, so soll ein entsprechender Bericht erstellt und kommuniziert werden (siehe Abschnitt 9.4).

16.8. Strategie und Schutzmaßnahmen

Das Security-Konzept sowie sämtliche Schutzmaßnahmen der Maschine sollen dokumentiert werden. Dies umfasst neben der reinen Funktion der Schutzmaßnahmen auch deren Implementierung, Konfiguration sowie Informationen zur Wartung. Dies ist Grundlage für die in Abschnitt 15.2 aufgeführten Überprüfungen von Security-Anforderungen. Idealerweise stellt der Hersteller ein Handbuch zur Security-Funktionalität der Maschine zur Verfügung.

16.9. Organisatorische Prozesse und Rollen

Sämtliche sicherheitsrelevanten organisatorischen Prozesse sowie die jeweiligen Verantwortlichen, Zuständige und Ansprechpartner sollen dokumentiert werden. Die Ansprechpartner nach außen hin sollen für externe Akteure dokumentiert und jederzeit erkenntlich sein (siehe auch Abschnitt 9.6).

17. Entwicklerschulungen bezüglich Security

Nichts außer Wissen ersetzt Wissen

Der Ausbau der Kompetenzen der Mitarbeiter hinsichtlich Informationstechnologie im Allgemeinen, der IT-Sicherheit und Netzwerksicherheit sowie der IT-technischen Besonderheiten von Produktionsanlagen im Speziellen gehört zu den dringenden Maßnahmen, die für eine nachhaltige Entwicklung und Verbesserung der Sicherheitslage absolut notwendig sind. Hierbei besteht die Anforderung, etablierte Berufsbilder um neu erforderlich gewordene Anforderungen zu ergänzen (die etwa durch Fortbildung gedeckt werden).

Da Anlagen aufgrund der „Safety"-Abnahmen nicht beliebig im Betrieb verändert werden können (etwa durch Einspielen von Softwareupdates nach der Abnahme) kommt der Verbesserung der IT-Sicherheit durch u.a. eine Erhöhung der Codequalität bei allen in Anlagen verbauten Komponenten eine extrem hohe Bedeutung zu. Folglich soll bei der Fortbildung insbesondere auf einem Ausbau der Kompetenzen hinsichtlich sicherer Softwareentwicklung Wert gelegt werden; erweiterte Kenntnisse zu Netzwerktechnik, Systemarchitektur und Protokollen sowie IT-Standards sind ebenfalls unerlässlich, um das Gesamtniveau der Security für die Anlagen an sich und deren späteren Betrieb zu heben. Die folgenden Abschnitte zeigen wichtige zu vermittelnde Inhalte auf und weisen auf bereits etablierte Angebote für Seminare hin.

17.1. Awareness der Mitarbeiter

Jede Maßnahme der Security ist nur so stark wie ihr schwächstes Glied, und kritische Lücken können sowohl durch Unachtsamkeit, Unwissenheit als auch Nachlässigkeit entstehen. Jedem Mitarbeiter muss verdeutlicht werden, dass er Teil der ganzheitlichen Sicherheit (Safety & Security) ist, und sein Beitrag entscheidenden Einfluss auf die Qualität der Anlagensicherheit hat. Folglich sind alle leitenden Angestellten, Management, Mitarbeiter und Aushilfen auf die Kritikalität ihres Handelns hinzuweisen und entsprechende konforme Handlungsweisen zu kommunizieren. Eine generelle Unterweisung in grundlegenden Themen der IT-Sicherheit schützt dabei nicht nur die Anlagen als Produkte an sich, sondern das gesamte Unternehmen. Nur wer die möglichen Risiken kennt, kann umsichtig agieren!

17.2. (Software-)Entwickler und Konstrukteure

Sowohl Konstrukteure, Entwicklungsingenieure als auch ausgebildete Softwareentwickler (etwa Fachinformatiker Anwendungsentwicklung) sollten regelmäßig über die Relevanz der Codesicherheit geschult werden. Insbesondere generelle Konzepte wie „Secure Development Lifecycle" (SDL) und die Auffrischung von Grundlagen zu Authentisierung, Autorisierung und Session Management sind unerlässlich, um gängige Fehler zu vermeiden und die Qualität im Entwicklungsprozess zu erhöhen. Kernanforderungen für Entwickler sind demnach:

- Einweisung in SDL
- Durchführung von Code Reviews, manuell
- Nutzung statischer Werkzeuge für Code Review
- Durchführung von Security-Tests
- Methoden der sicheren Softwareentwicklung
- Datenklassifikation (Berechtigung, Zugriff)
- Unterschiede zwischen Büroinformatik und ICS
- Angriffsflächen von industriellen IT-Systemen und Komponenten (ICS/SCADA)
- Besonderheiten in Bus-Topologien
- Schutzmaßnahmen für ICS/SCADA Geräte
- Netzsegmentierung und Firewallkonzepte
- Einbindung in das Sicherheitsmanagement

17.3. Anlagenplaner und Projektierer

Neben den reinen Entwicklungsingenieuren kommt den Planern und Produktmanagern eine wichtige Rolle zu. Ohne die Anforderungen von Kunden (Betreibern) hinsichtlich der immer aufwändigeren Integration einer neuen Anlage in bestehende Produktionslandschaften zu verstehen, können die Produktmanager nur schwer den Entwicklern konkrete Vorgaben für wichtige Funktionen und Eigenschaften der Anlagen machen. Hierzu gehören unter anderem Anforderungen hinsichtlich der genutzten Betriebssysteme, Netzwerktechnologien, Protokolle und Schnittstellen. Folglich sollten die oben genannten Schulungsinhalte verbindlich für alle mit Planung und Produktmanagement betrauten Personen sein, und um folgende Inhalte ergänzt werden:

- (IT-)Komponenten in Produktionsnetzen
- Grundlagen Verzeichnisdienste/Datenbanken
- Grundlagen TCP/IP und Bus-Netze
- Sicherheitsrelevante Angaben für die Anlagendokumentation (Kontextdiagramme)
- Wichtige Sicherheitsprotokolle und deren Arbeitsweise (kryptographische Grundlagen)
- Risikoanalyse und Risikomanagement
- Moderne Betriebssysteme und ihr (Sicherheits-)Management
- Grundlagen des Asset-, Patch- und Vulnerability Managements
- Härtung von IT-Systemen gegen Angriffe
- Grundlagen der Virtualisierung
- Computer Emergency Response und Incident Management in Anlagennetzen
- Gesetzliche Rahmenbedingungen
- Angriffsvektoren und typische Schwachstellen

Die oben dargestellten Inhalte fokussieren sich zumeist auf technische Sachverhalte, den organisatorischen und soziologischen Aspekten kommt jedoch mindestens gleichwertige Bedeutung zu. Ohne eine starke Unterstützung durch die Entscheider und das Management eines Unternehmens, die IT-Sicherheit der eigenen Produkte und Lösungen zu stärken, kann auf operativer Ebene auch mit guter Ausbildung kein Fortschritt erreicht werden. Die alleinige Schulung auf Secure Development Lifecycle Ansätze ist nicht zielführend, wenn das Unternehmen nicht die notwendigen technischen Rahmenbedingungen und organisatorischen Voraussetzung schafft, die Entwicklungsprozesse und Konstruktion auch an SDL anzupassen. Hierzu gehört zunächst, Security als Designziel zu fixieren und den Mitarbeiten die Zeit und die Mittel zu geben, eben diese Security auch von Anfang an zu implementieren. Die Entscheidungsträger sollen sich bewusst werden, dass eine nachhaltige Verbesserung der Security nur durch ebenso nachhaltige Neuausrichtung der Firma erreicht werden kann.

17.4. Verantwortlicher für Produktschutz

Auch wenn in der überwiegenden Zahl der Unternehmen noch kein „Product Security Officer“ benannt ist, steht der Bedarf für eine solche Funktion bereits fest. Um seine Aufgabe erfüllen zu können, sollte der PSO neben den grundlegenden Kenntnissen der ICS/SCADA Technologie auch über ein solides Basiswissen der IT-Infrastruktur verfügen. Darüber hinaus ist es notwendig, dass er sich mit dem Themenkomplex Sicherheitsmanagement befasst, um zusammen mit dem Chief (Information) Security Officer und den Produktmanagern die Sicherheitsstrategie für die eigenen Produkte festlegen und kommunizieren zu können. Hierfür benötigt der PSO tiefere Einblicke in:

- Sicherheits- und Risikomanagement
- Risikoanalysen und Bewertung
- Regelwerke und Policies
- Schwachstellen- und Incident Management
- Produktlebenszyklus IT/Anlage
- Meldewesen und Meldewege für Vorfälle

17.5 Trainingsmethoden

Da teilweise sehr komplexe, spezifische Inhalte vermittelt werden sollen und die jeweiligen Teilnehmer stark unterschiedliche Kenntnisstände aufweisen, ist es nur begrenzt möglich, den Trainingsbedarf durch standardisierte Schulungen abzudecken. Als Basis und Grundlage können deutschsprachige Kurse zur Einführung in die IT-Sicherheit in der Produktion sowie Industrial Security diverser bekannter Anbieter genutzt werden. Darüber hinaus haben sich die eher international ausgerichteten Kurse von SANS (insbesondere Teile von ICS410 und SEC401) als hilfreicher Einstieg in den Themenkomplex erwiesen. Spezialwissen vermittelt kostenfrei auch das US-CERT, sowohl webbasiert als auch im ICS-Lab[13]. Die Erfahrung der Autoren zeigt, dass eine leicht angepasste Einstiegsschulung für ein kleines internes Team zielführend ist. Hierauf basierend lässt sich dann ein maßgeschneiderter Ausbildungsplan erstellen, der die Bedürfnisse des Unternehmens besser abdeckt.

[13] https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT

Übersicht der Handlungsempfehlungen			Entwicklung	Integration	Betrieb mit Gewährleistung
Risikoanalyse	1.1.	Identifikation der schutzbedürftigen Werte	●		●
	1.2.	Ermittlung der Schutzziele	●		●
	1.3.	Identifikation der Bedrohungen	●		●
	1.4.	Risikobewertung	●		●
Netzsegmentierung	2.1.	Definition des Risiko-basierten Schutzbedarfs, der den Anlagen und Komponenten zugeordnet wird	●	●	
	2.2.	Zonierung der Dienste	●		
	2.3.	Einsatz von Isolationsmaßnahmen	●	●	
	2.4.	Periodische Überprüfung der Isolationsmaßnahmen auf Effektivität und Patchbarkeit von Filterkomponenten			●
	2.5.	DNS und andere Services pro Zone	●	●	
Benutzerkonten, Credentials, Authentisierung und Autorisierung	3.1.	Individuelle Benutzerkonten	●	●	●
	3.2.	Account Management	●	●	●
	3.3.	Verteilung und Management der Credentials	●	●	●
	3.4.	Authentisierung menschlicher Nutzer sowie von Softwareprozessen und -komponenten	●		●
	3.5.	Public-Key Authentisierung	●		●
	3.6.	Zonenbildung und Zugriffskonzepte mit entsprechender Authentifizierung	●		●
	3.7.	Die Maschine soll nach jeder Authentifizierung eine Autorisierungsprüfung der Akteure/Dienste gewährleisten.	●		●
	3.8.	Starke Authentisierung auf Externen Schnittstellen	●	●	●
Nutzung sicherer Protokolle	4.1.	Vertraulichkeit der Kommunikation bei IP basierten Protokollen	●	●	●
	4.2.	Integrität der Kommunikation	●	●	●
	4.3.	Typ, Stärke und Qualität der Verschlüsselungsalgorithmen	●	●	●
	4.4.	Sonderbetrachtung des Feldbus	●	●	●
Absicherung von Funktechnologien	5.1.	Sichere Konfiguration	●	●	
	5.2.	Wireless Access Management	●	●	
	5.3.	Zeitabhängigkeit der Sicherheit von Kryptographischen Funktionen	●	●	●
Sichere Fernwartung	6.1.	Regelungen zum Aufbau und Beenden einer Fernzugriffssitzung	●	●	●
	6.2.	Absicherung durch technische und organisatorische Maßnahmen	●	●	●
	6.3.	Verschlüsselung der Verbindungen	●	●	●
	6.4.	Etablierung von Zugriffsprozessen	●	●	●
	6.5.	Übergänge zu anderen Netzen absichern	●	●	●
Monitoring und Angriffserkennung	7.1.	Monitoring aller Zugriffe auf Maschinenkomponenten	●	●	●
	7.2.	Funktionen zum Monitoring in Leitstand integrieren	●	●	●
	7.3.	Virenscanner	●	●	●
	7.4.	Netzwerk IDS und Anomalieerkennung bei komplexen Maschinen	●	●	●
Wiederherstellungsplan	8.1.	Erstellung von Backup-Systemen	●	●	●
	8.2.	Erstellung regelmäßiger Backups			●
	8.3.	Prüfung von Backups auf Wiederherstellbarkeit			●
	8.4.	Wiederherstellung eines vertrauenswürdigen Zustandes nach einer Störung/Angriff			●
	8.5.	Wiederherstellung von verschlüsselten Daten	●	●	
Sicherer Produkt-Lebenszyklus	9.1.	Beobachtung von Schwachstellen			●
	9.2.	Beobachtung der Bedrohungslage durch die Hersteller	●		
	9.3.	Reaktionsfähigkeit auf Schwachstellen	●		●
	9.4.	Festlegen der betrieblichen Kommunikationskanäle	●		●

Betrieb ohne Gewährleistung	Integration von Sensoren/ Aktoren	Kommunikation	Funktionalitäten zu Datenspeicherung und Informationsaustausch	Monitoring	Hersteller	Integrator	Betreiber
●	1	1	1	1	●	●	●
●	1	1	1	1	●	●	●
●	1	1	1	1	●	●	●
●	1	1	1	1	●	●	●
		3	4		●	●	
		3	4		●	●	
		3	4		●	●	
●		3	4			●	●
		3	4		●	●	
●		4	2		●	●	●
●		4	2		●	●	●
●		4	2		●	●	●
●	1	1	1	1	●	●	●
●		4	4		●	●	●
●		4	4		●	●	●
●	1	1	1	1	●	●	●
●	1	1	1	1	●	●	●
●		4	4		●	●	●
●		3	4		●	●	●
●		3	4		●	●	●
●		3			●	●	●
		2	4	3		●	●
		2	4	3	●	●	●
●		2	4	3	●	●	●
●	4		4		●	●	●
●	4		4		●	●	●
●	4		4		●	●	●
●	4		4		●	●	●
●	4		4			●	●
●				3	●	●	●
●				2		●	
●	1	1	1	1	●	●	●
●	5	5	4	4	●	●	●
●	1	1	1	1	●	●	●
●	1	1	1	1			●
●	1	1	1	1			●
●	1	1	1	1	●	●	●
	1	1	1	1	●	●	●
		3	4		●	●	●
	1	1	1	1	●		
	1	1	1	1	●	●	●
	1	1	1	1	●	●	●

Übersicht der Handlungsempfehlungen			Entwicklung	Integration	Betrieb mit Gewährleistung
Sicherer Produkt-Lebenszyklus	9.5.	Patchmanagement			●
	9.6.	Benennung von internen und externen Verantwortlichen	●	●	●
	9.7.	Umgang mit End Of Support (EOS)			●
	9.8.	Phase-out Management			●
Anpassung und Prüfung der Komponenten	10.1.	Anpassen der Standard-Einstellungen		●	
	10.2.	Anpassen der Hardwarekonfiguration		●	
	10.3.	Zugriff auf das Internet innerhalb des ICS-Netzwerks		●	
	10.4.	Prüfungen zur Verifikation und Validierung	●	●	●
	10.5.	Prüfung der Software- und Informationsintegrität	●	●	●
	10.6.	Auswahl sicherer Komponenten	●	●	
Verzicht auf überflüssige Komponentenfunktionen	11.1.	Entfernen von unnötiger Software und Diensten	●	●	
	11.2.	Entfernung/Deaktivierung aller nicht verwendeten Hardwarekomponenten	●	●	
Komponentenhärtung	12.1.	Komponenten dürfen nur gehärteten Code ausführen	●	●	
	12.2.	Sicherheitstests als integraler Bestandteil bei der Entwicklung und Systemintegration	●	●	
	12.3.	DoS Schutz	●	●	
	12.4.	Application Whitelisting und Blacklisting	●	●	●
	12.5.	Reduzierung der Systemkomplexität	●	●	
	12.6.	Absicherung von Feldgeräten außerhalb der Anlage gegen physische Angriffe	●	●	
	12.7.	Absichern der elektronischen externen Schnittstellen	●	●	
Isolationstechniken innerhalb der Maschine / Virtualisierung	13.1.	Schutz vor Schadcode durch Sandboxing und Virtualisierung	●	●	
	13.2.	Die Maschine soll Restriktionen für „mobilen Code“ implementieren	●	●	●
	13.3.	Abgrenzung der Betriebs- und Konfigurationsdaten von Anwendungsprogrammen	●	●	
Kryptographie	14.1.	Implementierung von standardisierten Algorithmen	●	●	
	14.2.	Einbindung in bestehende PKI	●	●	
Bestimmung der Security-Anforderungen für Lieferanten und Zulieferer	15.1.	Überprüfung der Security-Anforderungen an zugelieferte Komponenten	●	●	
	15.2.	Identifikation der eigenen Rolle als Zulieferer	●	●	
	15.3.	Ausgelagerte Softwareentwicklung	●	●	●
Dokumentation	16.1.	Schnittstellen	●	●	
	16.2.	Etablierte Prozesse	●	●	●
	16.3.	Dokumentation der Risikoanalyse	●		●
	16.4.	Rechteverteilung	●	●	●
	16.5.	Maschineninventar	●	●	●
	16.6.	Dokumentmanagement	●	●	●
	16.7.	Sicherheitsvorfälle			●
	16.8.	Strategie und Schutzmaßnahmen	●	●	●
	16.9.	Organisatorische Prozesse und Rollen	●	●	●
Entwicklerschulungen bezüglich Security	17.1.	Awareness der Mitarbeiter	●	●	●
	17.2.	(Software-)Entwickler und Konstrukteure	●		
	17.3.	Anlagenplaner und Projektierer	●	●	●
	17.4.	Verantwortlicher für Produktschutz	●	●	●
	17.5.	Trainingsmethoden	●	●	●

Betrieb ohne Gewährleistung	Integration von Sensoren/ Aktoren	Kommunikation	Funktionalitäten zu Datenspeicherung und Informationsaustausch	Monitoring	Hersteller	Integrator	Betreiber
	1	1	1	1	●	●	●
	1	1	1	1	●	●	●
			3	3		●	●
●			3	3		●	●
	1	1	1	1		●	●
	1	1	1	1	●	●	
	1	1	1	1		●	●
	1	1	1	1	●	●	
	1	1	1	1	●	●	
	1	1	1	1	●	●	●
	1	1	1	1	●	●	
	1	1	1	1	●	●	
	1	1	1	1	●	●	
	1	1	1	1	●	●	
		4	4		●	●	
	1	1	1	1	●	●	●
	1	1	1	1	●	●	
	1	1	1	1	●	●	●
	1	1	1	1	●	●	
		4	4		●	●	
	5	4	4	5	●	●	
	5	4	4	5	●	●	
	1	1	1	1	●	●	
		5	4		●	●	●
		2			●	●	●
	1	1	1	1	●	●	
		2			●	●	
	1	1	1	1	●	●	
	1	1	1	1	●	●	●
	1	1	1	1	●	●	●
	1	1	1	1	●	●	●
	1	1	1	1	●	●	
	1	1	1	1	●	●	●
	1	1	1	1	●	●	●
	1	1	1	1	●	●	●
	1	1	1	1	●	●	●
●	1	1	1	1	●	●	●
	1	1	1	1	●	●	
●	1	1	1	1		●	
●	1	1	1	1		●	●
	1	1	1	1	●	●	●

Weiterführende Informationen

Die aufgeführten Handlungsempfehlungen sollen einen grundlegenden Schutz von mittelständischen Unternehmen auf dem Weg zur Industrie 4.0 darstellen. Ist dieser Weg beschritten und will man die Maschine auch bei voller Industrie 4.0 Funktionalität zukunftssicher gestalten, so bietet sich ein Blick in die weiterführende Literatur an.

Im Folgenden sind wichtige Informationsquellen aufgelistet, die eine weitere Hilfestellung für die Etablierung einer sicheren Produktion bieten können.

- BSI ICS Security Kompendium[14]
- VDMA Fragenkatalog „Industrial Security“[15]
- VDMA Studie zum Status Quo der „Industrial Security“[16]
- VDMA Leitfaden Industrie 4.0[17]
- Light and Right Security ICS (LARS ICS)[18]
- VdS Quick Check Security[19]
- Industrie 4.0-Readiness – Online-Selbst-Check für Unternehmen[20]
- ICS-CERT-Newsletter, Reports und Handlungsempfehlungen
- VDI 2182 – Informationssicherheit in der industriellen Automatisierung
- ISO/IEC 27000-Reihe zu Informationssicherheit
- IEC 62443 zu ICS Security
- ISO/IEC 15408-1 Evaluation criteria for IT security
- NAMUR Arbeitsblatt NE 153
- NAMUR Arbeitsblatt NA 115

[14] https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/Empfehlungen/ICS/empfehlungen_node.html
[15] http://pks.vdma.org/article/-/articleview/6262936
[16] https://www.vdma.org/article/-/articleview/2717338
[17] http://industrie40.vdma.org/article/-/articleview/8567185
[18] https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/Tools/LarsICS/LarsICS_node.html
[19] http://vds.de/de/vds-cyber-security/cyber-security-fuer-kmu/
[20] https://www.industrie40-readiness.de/

Glossar

Authentisierung
Anmeldung mit Zugriffsdaten (aus Sicht des Überprüften).

Authentifizierung
Nachweis eines Benutzers/Gerätes zum berechtigten Zugriff (aus Sicht des prüfenden Geräts).

Autorisierung
Freigabe/Berechtigung zum Zugriff.

Betreiber
Betreiber einer Anlage im Sinne der VDI/VDE 2182.

Credentials
Zugangsdaten, wie Passwörter, Schlüssel oder biometrische Daten.

DNS (Domain Name System)
Verzeichnisdienst zur Auflösung von Adressen in IP-Adressen.

DoS (Denial of Service).
Ausfall eines Netzwerkdienstes aufgrund von (evtl. mutwilliger) Überlastung.

ERP (Enterprise Resource Planning)
Einsatzplanung von Ressourcen in einem Unternehmen.

FMEA (Failure Mode and Effects Analysis)
Methode zur Ermittlung und Bewertung von Fehlern.

Hersteller
Hersteller einer Komponente oder Maschine im Sinne der VDI/VDE 2182.

HSM (Hardware Security Module)
Dedizierter Sicherheitschip zur Ausführung von kryptographischen Operationen mit sicherem Speicher.

ICS (Industrial Control System)
IT-basiertes Steuersystem der Anlage.

IDS (Intrusion Detection System)
System zur automatischen Erkennung von Angriffen.

Integrator
Anlagenbauer oder Integrator mehrerer Komponenten oder Maschinen im Sinne der VDI/VDE 2182.

IPS (Intrusion Prevention System)
IDS Systeme, die zusätzlich Methoden zur Abwehr von Angreifern beinhalten.

MAC-Filterung
Filterung von Datenpaketen anhand ihrer MAC-Adresse.

MES (Manufacturing Execution Systems)
Produktionsleitsystem.

PKI (Public Key Infrastructure)
Verteiltes System zur Verwaltung und Überprüfung von Zertifikaten basierend auf asymmetrischer Kryptographie.

Sandboxing
Ausführung von Code in einer kontrollierten und isolierten Ausführungsumgebung.

SCADA
(Supervisory Control and Data Acquisition)
System zur Überwachung und Steuerung technischer Prozesse.

TEE (Trusted Execution Environment)
Sichere und vertrauenswürdige Laufzeitumgebung für Programme, z.B. auf einem eigenen Prozessorkern.

Verifizierung
Überprüfung einer Software auf Erfüllung ihrer Spezifikation.

Validierung
Überprüfung einer Software in Bezug auf ihre Tauglichkeit im Einsatzszenario.

VPN (Virtual Private Network)
Virtuelles, in sich geschlossenes, Kommunikationsnetz, das ein bestehendes Kommunikationsnetz als Transportmedium verwendet und mittels Verschlüsselung abgesichert ist.

Security im VDMA

Auf den richtigen Schutz kommt es an

Ohne den Schutz von Daten und Know-how in den unternehmensübergreifenden Produktions- und Kommunikationsprozessen ist Industrie 4.0 undenkbar. Der VDMA unterstützt seine Mitglieder in allen für die Security relevanten Gebieten.

Industrial Security dient dem Schutz von Maschinen und Anlagen vor Ausfall, Manipulation, Know-how-Abfluss und Sabotage. Die Schutzziele können auch mit dem VIVA-Begriff definiert werden, der für Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität steht.

Mit den Security-Themen befassen sich im VDMA die zwei Arbeitskreise

- Informationssicherheit,
- Industrial Security

sowie die Arbeitsgemeinschaft

- Produkt- und Know-how-Schutz.

Informationssicherheit

Der Arbeitskreis „Informationssicherheit“ erarbeitet Leitlinien und Praxishilfen zur „klassischen“ IT- und Informationssicherheit. Grundlagen sind unter anderem die Normenreihe ISO 27000 sowie der Grundschutz des Bundesamts für Sicherheit in der IT (BSI). Teilnehmer sind IT-Sicherheitsbeauftragte der Maschinen- und Anlagenbauer.

Industrial Security

Der Arbeitskreis „Industrial Security“ erarbeitet Leitlinien und Arbeitshilfen für die Security in der Produktion sowie für Maschinen- und Anlagenbauprodukte. Teilnehmer sind Maschinen- und Anlagenbauer, Betreiber, Automatisierer, Dienstleister, Security-Spezialisten und das BSI.

Integrated security first: Maschinen und Anlagen, Produkte und Know-how brauchen effektiven Schutz.

Produkt- und Know-how-Schutz

Die Arbeitsgemeinschaft Produkt- und Know-how-Schutz (AG Protect-ing) bündelt die Aktivitäten der Anbieter von Technologien und Dienstleistungen zu Produktpiraterie, Security und Know-how-Schutz. Vom Austausch zwischen Herstellern, Behörden und Anwendern profitieren nicht nur Maschinenbauer.

Kontakt

Steffen Zimmermann
Produkt- und Know-how-Schutz
Telefon +49 69 6603-1978
E-Mail steffen.zimmermann@vdma.org

Internet http://pks.vdma.org/security
www.protect-ing.de
www.i40-security.de

Industrie 4.0 im VDMA

Bausteine bereiten den Weg

Wie Unternehmen von Industrie 4.0 profitieren können, welche Aspekte bei der Umsetzung zu beachten sind und wie der Weg zur vernetzten Produktion aussehen kann – Antworten auf diese Fragen gibt das VDMA-Forum Industrie 4.0.

Mit Industrie 4.0 geht ein grundlegender Wandel in der Produktion einher: IT- und Internettechnologien dringen noch stärker in die Produkte und in die Fabriken ein. Menschen, Maschinen und Produktionsmittel kommunizieren über die ganze Wertschöpfungskette miteinander. Diese Veränderungen finden jedoch nicht von heute auf morgen statt. Statt einer Revolution gleicht die Entwicklung hin zu Industrie 4.0 eher einer Evolution: Damit die Umsetzung Stück für Stück gelingt, begleitet und unterstützt der VDMA seine Mitglieder auf vielfältige Weise:

Im VDMA-Forum Industrie 4.0 hat der VDMA sein verbandsinternes Know-how gebündelt. Das Forum besteht aus einem interdisziplinären Team von VDMA-Experten. Als Partner und Dienstleister bieten sie den Mitgliedsunternehmen sowie den Fachverbänden und Abteilungen des VDMA in den für Industrie 4.0 maßgeblichen Handlungsfeldern ganz konkrete Unterstützung an:

Politik & Netzwerke: Mit Politik und Gesellschaft müssen wichtige politische Rahmenbedingungen vereinbart werden.

Produktion & Geschäftsmodelle: Intelligente Produktionssysteme erhöhen die Effizienz von Organisation und Prozessen. Automatisierung und Losgröße 1 schließen einander zukünftig nicht mehr aus. Innovative Geschäftsfelder entstehen.

Forschung & Innovation: Mehr denn je sind Forschungsergebnisse entscheidend für die Wettbewerbsfähigkeit des Industriestandorts Deutschland. Förderinstrumente müssen verlässlich sein und ein schneller Transfer von Forschungsergebnissen in die industrielle Praxis stattfinden.

Normung & Standards: Die Vernetzung entlang der Wertschöpfungskette gelingt nur über einheitliche Normen und Standards. Es ist entscheidend, diese mitzugestalten und die relevanten Akteure in einen Dialog einzubinden.

IT-Sicherheit & Recht: Der automatisierte Datenaustausch vernetzter Produktionssysteme muss sicher und zuverlässig sein. Neben dem Schutz von Produkten, Maschinen und Anlagen geht es auch um die Weiterentwicklung und Neuauslegung bestehenden Rechts.

IT-Technologien & Software: Moderne Software-Architekturen sind der Schlüssel zu modularen und flexiblen Systemen. Damit diese heutigen Ansprüchen an Qualität, Verfügbarkeit und Usability genügen, braucht es die richtigen methodischen Ansätze und das Fachwissen unterschiedlicher Experten.

Mensch & Arbeit: In der Fabrik der Zukunft werden die Tätigkeiten sowohl in technologischer als auch in organisatorischer Sicht anspruchsvoller; interdisziplinäre Kompetenzen werden immer wichtiger. Das Bildungssystem und die Unternehmen müssen sich darauf einstellen.

Unterstützung auf dem Weg

Auf diese Weise entsteht am Ende aus vielen kleinen Bausteinen das große Ganze: Mit dem Forum Industrie 4.0 engagiert sich der VDMA, um die Vision Industrie 4.0 in umsetzbare Handlungsempfehlungen für den Maschinen- und Anlagenbau weiterzuentwickeln und insbesondere die Anwenderperspektive zu berücksichtigen. Ziel ist es, langfristig und nachhaltig ein Netzwerk zum Erfahrungsaustausch unter den Mitgliedsunternehmen aufzubauen.

Kontakt
Dr. Beate Stahl
Forum Industrie 4.0
Telefon +49 69 6603-1295
E-Mail beate.stahl@vdma.org
Internet http://industrie40.vdma.org

Projektpartner / Impressum

VDMA
Produkt- und Know-how-Schutz
Steffen Zimmermann
Lyoner Str. 18
60528 Frankfurt am Main
E-Mail protect-ing@vdma.org
Internet pks.vdma.org

Fraunhofer Institut für Angewandte und Integrierte Sicherheit (AISEC)
Bartol Filipovic
Abteilungsleiter Produktschutz und Industrial Security
Parkring 4
85748 Garching bei München
E-Mail bartol.filipovic@aisec.fraunhofer.de
Internet: www.aisec.fraunhofer.de

accessec GmbH
Sebastian Rohr
CTO + CSO
Marktstr. 47–49
64401 Groß-Bieberau

Projektleitung
VDMA Produkt- und Know-how-Schutz
Steffen Zimmermann

Inhaltliche Beiträge
Fraunhofer AISEC
Konstantin Böttinger
Bartol Filipovic
Dr. Martin Hutle

accessec GmbH
Sebastian Rohr

Design und Layout
VDMA-Forum Industrie 4.0
Dr. Beate Metten
VDMA Verlag GmbH
Martina Becker

Verlag
VDMA Verlag GmbH
Lyoner Str. 18
60528 Frankfurt am Main

Druck
Druck- und Verlagshaus Zarbock

Erscheinungsjahr
2016

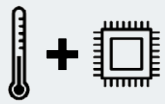
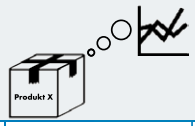
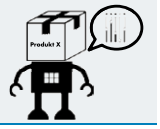
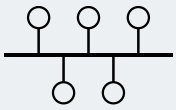
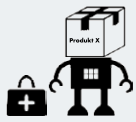
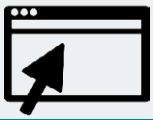
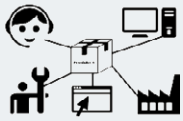
Bildnachweise
Titelbild: Olivier Le Moal – Fotolia.com
Seite 3: Kolbus

Grafiken
Fraunhofer AISEC
VDMA
Piktogramme: https://thenounproject.com

Werkzeugkasten Industrie 4.0

Industrie 4.0

Produkte

A	Integration von Sensoren / Aktoren					
		***Keine Nutzung** von Sensoren/Aktoren*	***Sensoren/Aktoren** sind **eingebunden***	***Sensordaten** werden vom Produkt **verarbeitet***	*Daten werden vom Produkt **für Analysen ausgewertet***	*Das Produkt **reagiert** auf Basis der gewonnenen Daten **eigenständig***
B	Kommunikation / Connectivity					
		***Keine Schnittstellen** am Produkt*	*Das Produkt sendet bzw. empfängt **I/O-Signale***	*Das Produkt verfügt über **Feldbus-Schnittstellen***	*Das Produkt verfügt über **Industrial Ethernet-Schnittstellen***	*Das Produkt verfügt über **Zugang zum Internet***
C	Funktionalitäten zu Datenspeicherung und Informationsaustausch					
		Keine Funktionalitäten	*Möglichkeit zur **eindeutigen Identifikation***	*Produkt verfügt über passiven **Datenspeicher***	*Produkt mit **Datenspeicher** zum autonomen **Informationsaustausch***	*Daten- und Informationsaustausch als **integraler Bestandteil***
D	Monitoring					
		***Kein Monitoring** durch das Produkt*	***Detektion von Ausfällen***	*Erfassung des **Betriebszustands zur Diagnose***	***Prognose** der eigenen **Funktionsfähigkeit***	***Selbstständige Maßnahmen** zur Steuerung*
E	Produktbezogene IT-Services					
		Keine Services	*Services über **Online-Portale***	***Service-Ausführung direkt über Produkt***	***Selbstständige Ausführung** von Services*	*Vollständige Eingliederung in **IT-Service-Infrastruktur***
F	Geschäftsmodelle um das Produkt					
		*Gewinne durch **Verkauf der Standardprodukte***	***Verkauf und Beratung** zum Produkt*	***Verkauf, Beratung und Anpassung** des Produktes an Kundenwünsche*	*Zusätzlicher Verkauf **produktbezogener Dienstleistungen***	*Verkauf von Produktfunktionen*

Werkzeugkasten Industrie 4.0 – Produkte (Quelle: VDMA / Leitfaden Industrie 4.0)

Die vier Abschnitte des Produktlebenszyklus

Entwicklung | Integration | Gewährleistung | Restlaufzeit

VDMA
Produkt- und Know-how-Schutz
Lyoner Str. 18
60528 Frankfurt am Main
Telefon +49 69 6603-1978
Fax +49 69 6603-2978
E-Mail protect-ing@vdma.org
Internet pks.vdma.org

Fraunhofer Institut für Angewandte und Integrierte Sicherheit (AISEC)
Parkring 4
85748 Garching bei München
Internet: www.aisec.fraunhofer.de

accessec GmbH
Marktstr. 47–49
64401 Groß-Bieberau

pks.vdma.org
www.i40-security.de

VDMA Verlag
ISBN 978-3-8163-0689-4