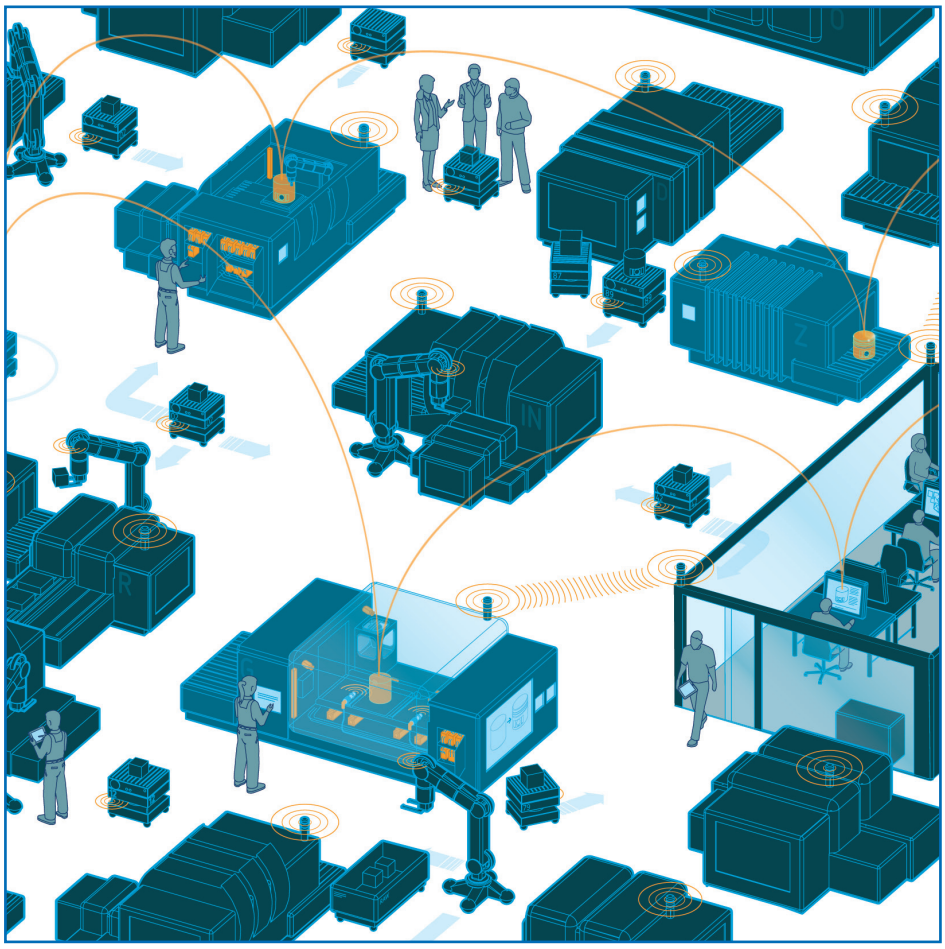
ZVEI:
Die Elektroindustrie

Whitepaper

Integrität von Daten, Systemen und Prozessen als Kernelement der Digitalisierung



November 2017

Zentralverband Elektrotechnik- und Elektroindustrie

ZVEI:
Die Elektroindustrie

Impressum

Integrität von Daten, Systemen und Prozessen als Kernelement der Digitalisierung

Herausgeber:
ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e.V.
Fachverband Automation
Führungskreis Industrie 4.0, SG Sicherheit
Lyoner Straße 9
60528 Frankfurt am Main

Ansprechpartner:
Lukas Linke
Telefon: +49 69 6302-432
Fax: +49 69 6302-322
E-Mail: linke@zvei.org
www.zvei.org

November 2017

Die Autoren

Das Dokument wurde durch die Mitglieder der SG Sicherheit erstellt.
Diese ist Bestandteil des Führungskreises Industrie 4.0 im ZVEI.
Sie übernimmt alle Aspekte zur Industrie- 4.0-Security und unterstützt die Arbeiten der AG 3 „Sicherheit vernetzter Systeme“ der Plattform Industrie 4.0.

Nicole Dönicke	Kjellberg Finsterwalde
Wolfgang Fritsche	IABG
Dr. Thomas Gamer	ABB
Prof. Dr. Tobias Heer	Hirschmann Automation and Control
Dr. Lutz Jänicke	Phoenix Contact .
Michael Jochem	Robert Bosch
Dr. Wolfgang Klasen	Siemens
Thomas Lantermann	Mitsubishi Electric Europe
Lukas Linke	Zentralverband Elektrotechnik- und Elektronikindustrie
Jens Mehrfeld	Bundesamt für Sicherheit in der Informationstechnik
Tobias Pfeiffer	Festo
Andreas Teuscher	Sick

Inhalt

1 Zielsetzung und Adressat 5

2 Worum geht es bei Integrität? 6

2.1 Relevanz: Digitalisierung und Vernetzung 6

2.2 Nutzen der Integrität 6

2.2.1 Bedeutung der Integrität im Wechselspiel mit anderen mit anderen Schutzzielen 8

2.3 Bestimmung: Daten- und Systemintegrität 9

2.4 Betrachtung der Gesamtintegrität eines Systems 10

2.4.1 Parameter und Zusammenhänge 11

2.4.2 Betrachtung der Integrität am Beispiel eines SPS-Szenarios 12

2.5 Technische Maßnahmen zur Prüfung und Gewährleistung von Integrität 14

2.5.1 Einsatz von Protokollen mit Prüfsummen 15

2.5.2 Einsatz von Protokollen mit Signaturen 15

2.5.3 Einsatz von Prüfsummen zur Erkennung von Fehlern/Veränderungen 15

2.5.4 Einsatz von signierter Firmware, Software und Updates 15

2.5.5 Möglichkeiten zur Überwachung der Systemintegrität 15

2.5.6 Möglichkeiten zur Signatur von Steuerungsprogrammen und Konfigurationsparametern 16

2.5.7 Möglichkeiten zur Authentisierung und Autorisierung vor dem Einspielen von Steuerungsprogrammen und Konfigurationsparametern 16

2.5.8 Möglichkeiten zur Validierung von Konfigurationsparametern 16

2.5.9 Rollout von Identitäten auf Komponenten 16

2.5.10 Protokollierung 16

2.5.11 Überwachen der Protokollierung 17

2.5.12 Verwaltung der Identitäten auf den Komponenten 17

2.5.13 Signierung und Prüfung der Herkunft von Firmware-Updates 17

2.5.14 Signierung und Prüfung von Steuerungsprogrammen 17

2.6 Umgang mit Störung der Integrität 17

2.7 Ausblick: Integritätsschutz als Grundlage der Vertrauenswürdigkeit 19

3 Vertrauenswürdigkeit 20

3.1 Was ist Vertrauenswürdigkeit? 20

3.2 Integrität als wesentliche Voraussetzung der Vertrauenswürdigkeit 22

3.3 Vertrauenswürdigkeit als übergreifender Ansatz für Liefer- und Wertschöpfungsnetzwerke 23

4 Anforderungen an die Akteure 24

5 Zusammenfassung 26

1 Zielsetzung und Adressat

Dieses Dokument bündelt die technischen Diskussionen der SG Sicherheit des ZVEI hinsichtlich Anforderungen, Validierung und Umsetzung der Integrität von Daten, Systemen und Prozessen.

Zielsetzung des Dokuments ist, ein gemeinsames Verständnis zum Thema Integrität im Kontext internationaler unternehmensübergreifender Kooperationen sowie der zunehmenden Digitalisierung von Produkten und Systemen (Stichwort Industrie 4.0) zu entwickeln. Das Papier dient als Diskussionsgrundlage, Wissensvertiefung und Orientierungshilfe für andere Arbeitsgruppen im Bereich Industrial Security und Industrie 4.0.

Das Dokument geht auf die Fragestellung ein, inwiefern zum Beispiel Korrektheit, Unveränderbarkeit und Vollständigkeit (= Integrität) von Daten, Systemen und Prozessen bereitgestellt und überprüft werden können und wie diesbezüglichen Störungen zu begegnen ist. Im Fokus stehen technische Daten; personenbezogene Daten, und damit die Aspekte des Datenschutzes, werden nicht betrachtet, um einen angemessenen Umfang zu wahren.

Die Ausführungen richten sich insbesondere an Komponentenhersteller sowie an Integratoren und Betreiber. Die Fragestellungen im Kontext von internationalen Zuliefererbeziehungen und unternehmensübergreifenden Kooperationen sind über die Security-Community hinaus relevant. Das Whitepaper adressiert auch Verantwortliche für das Produktmanagement und den Einkauf.

2 Worum geht es bei Integrität?

2.1 Relevanz: Digitalisierung und Vernetzung

Digitalisierung und Vernetzung erfordern zwingend ein Vertrauen in die Korrektheit von eigenen und zunehmend von externen Daten und die einwandfreie Funktion von Systemen und Prozessen. Dies ist fundamental für alle Geschäftsprozesse innerhalb und außerhalb des Unternehmens. Integrität wird häufig nur als technischer Aspekt betrachtet, hat aber direkte Auswirkungen auf die Wirtschaftlichkeit, die Reputation oder regulatorische Verantwortung.

Digitalisierung

Die Verknüpfung physischer Dinge (Things) schreitet in zahlreichen Bereichen des täglichen Lebens voran. Zwei wesentliche Voraussetzungen zur Umsetzung dieser Verknüpfungen im Internet of Things (IoT), inklusive des Industrial Internet of Things (IIoT) und des Internet of Everything (IoE), sind die Digitalisierung von Informationen sowie die Vernetzung; sie legen somit einen wesentlichen Grundstein für eine Economy of Things and Services. Verknüpft werden beispielsweise Dinge im Bereich der Energienetze, in Städten, im Haushalt und natürlich auch in der Produktion. Man spricht von Smart Grids, Smart Cities, Smart Home und Smart Manufacturing (= Industrie 4.0). Derzeitige Schätzungen gehen davon aus, dass bis 2020 etwa 50 Milliarden Dinge im Internet of Things (IoT) miteinander verknüpft sind. Dabei bleibt es aber nicht bei der reinen Verbindung von Dingen, es erfolgt zukünftig immer stärker eine Verknüpfung zwischen Menschen, Prozessen, Daten und Dingen, die allgemein als das Internet of Everything (IoE) bezeichnet wird.

Während in der Vergangenheit Abläufe primär mechanisch oder elektronisch durch festgelegte Schaltkreise erfolgten, fand in den letzten Jahrzehnten ein Wandel hin zu flexibleren Produkten mit höheren Software-Anteilen statt. Zwar wird Software bereits seit Jahrzehnten in Produktionsumgebungen eingesetzt, jedoch finden sich heute in einer deutlich breiteren Palette an Geräten CPUs mit der Fähigkeit, einen beliebigen Code auszuführen. Insbesondere im Internet of Things (IoT) und im industriellen Pendant, dem Industrial Internet of Things (IIoT), werden Objekte, die bisher nicht über Rechen- und Kommunikationseinheiten verfügen, mit Hardware, Software (inklusive Firmware)[1] und Kommunikationsschnittstellen ausgestattet. Im Gegensatz zu mechanischen und festgelegten elektronischen Lösungen lässt sich die Funktion von Geräten mit Software jedoch entweder durch eine Konfigurationsänderung oder durch ein Einspielen neuer Software verändern. Für den Betreiber ist daher nicht immer klar, ob Funktionen oder Funktionsaspekte nach einer Software- oder Konfigurationsänderung noch identisch sind oder ob gar neue Funktionen oder Verhaltensweisen hinzugekommen sind. Besonders kritisch wird diese Betrachtung, wenn man die Möglichkeit in Betracht zieht, dass ein Angreifer Konfigurationen oder Softwarebestandteile verändern oder ersetzen kann. Durch Schwachstellen wie zum Beispiel Buffer-Overflows oder durch unsichere Software-Uploads können Angreifer gegebenenfalls die Software eines Gerätes manipulieren, sodass die Funktion verändert bzw. eingeschränkt wird oder neue (unerwünschte) Funktionen hinzukommen.

Vernetzung

Die Vernetzung erfolgt durch eine Kommunikation auf allen Ebenen sowie über Unternehmens- und Sektorengrenzen hinweg. Dies umfasst beispielsweise die Kommunikation auf der Ebene der Operational Technology (OT) in der Produktion sowie die Kommunikation zwischen Produktions-OT und Office-IT. Dies schließt auch die Kommunikation zwischen einem Hersteller, seinen Lieferanten, Kunden und sonstigen Partnern ein.

[1] In dem Whitepaper wird Software als Sammelbegriff von Software UND Firmware verwendet.

Generell gelten für IT und OT die gemeinsamen Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität. Sie sind jedoch in den einzelnen Bereichen unterschiedlich priorisiert. Verfügbarkeit und ihre Kontrolle waren früher garantiert durch die Kenntnisse des Betreibers über alle beteiligten Betriebsmittel. Mit der zunehmenden Digitalisierung und Vernetzung befinden sich jedoch Betriebsmittel nur noch zum Teil in dem direkten Einflussbereich eines Betreibers. Damit wächst die Abhängigkeit von externen Kommunikationspartnern und ihrem Verhalten.

Quelle: ZVEI

2.2 Nutzen der Integrität

Gerade im industriellen Umfeld hat die Integrität einen direkten Einfluss zum Beispiel auf die Qualität der erzeugten Produkte und den Betrieb einer Anlage. Der Einfluss auf die Qualität der Produkte wird offensichtlich, wenn die Folgen von fehlender Integrität im Herstellungsprozess näher beleuchtet werden. Werden nicht integre Daten von Sensoren geliefert, kann das Produkt gegebenenfalls nicht richtig oder nicht mit ausreichender Genauigkeit gefertigt werden. Teile werden aufgrund der nicht integren Daten fehlerhaft erzeugt oder Fehler werden nicht im Qualitätssicherungsprozess bemerkt. Dies kann soweit führen, dass nicht spezifikationsgerechte Produkte an Kunden geliefert werden und zum Beispiel Reputationsverluste oder Produkthaftungsfälle auslösen.

Eine nicht integer funktionierende Anlage kann sowohl Einfluss auf die Produktqualität nehmen als auch die Verfügbarkeit der Anlage selbst reduzieren. Auch wenn die Sensorinformationen korrekt an die Anlage übertragen wurden, ist diese bei fehlender Integrität gegebenenfalls nicht in der Lage, die Daten korrekt auszuwerten oder Folgeaktionen richtig

auszuführen. Dies gilt auch für elektronische Steuereinheiten in einer industriellen Anlage. Daraus folgt, dass bei einer nicht integren Anlage keine Aussage über die Qualität eines gefertigten Produkts getroffen werden kann.

Einen ähnlich drastischen Einfluss kann die fehlende Integrität auf kritische Prozesse der Funktionalen Sicherheit haben. Wenn nicht integre, also fehlerhafte oder gefälschte Daten durch sicherheitskritische Anwendungen verarbeitet werden, kann es zu schwerwiegenden Fehlentscheidungen durch die Anwendungen kommen. Dies ist relevant insbesondere vor dem Hintergrund regulatorischer Vorgaben und Verantwortung.

Die Integrität innerhalb einer industriellen Anlage ist also sowohl für die hergestellten Produkte und die Sicherheit des Herstellungsprozesses als auch für die Einhaltung regulatorischer Anforderungen von größter Bedeutung. Werden mehrere industrielle Anlagen zusammengeschaltet, gilt dies auch für die Produktionszelle.

Konsequenz: Digitalisierung und Vernetzung verändern etablierte Ansätze in den Industrieunternehmen:

- Security-Konzepte müssen sich von der unternehmensinternen hin zur unternehmensübergreifenden Absicherung ausdehnen.
- Die Grenze zwischen Produktions-OT und Office-IT verschwindet mit der Zeit.

2.2.1 Bedeutung der Integrität im Wechselspiel mit anderen Schutzzielen

Die Integrität von Daten und Systemen ist eine Voraussetzung für die Erreichung der anderen Schutzziele: Verfügbarkeit und Vertraulichkeit.

Sind Daten oder Systeme nicht integer, können die darauf basierenden Prozesse nicht mehr fehlerfrei ablaufen. Ohne Maßnahmen zur Erkennung einer Integritätsverletzung entstehen Folgefehler, die sich in Form von Produktmängeln oder fehlerhaften Daten bemerkbar machen. Diese Folgefehler sind nicht mehr als Integritätsfehler erkennbar, da eventuell Schutzmaßnahmen wieder neu angewendet werden und keine zusätzliche Überprüfung der Ausgangsdaten stattfindet. Insofern sind überwachende Maßnahmen zum Integritätsschutz mit entsprechender anwendungsabhängiger Bewertung der Auswirkungen, siehe Abschnitt 2.6, zu empfehlen.

Entsprechend wirken sich Integritätsfehler direkt auf die Verfügbarkeit oder durch unvermeidbare Notabschaltungen aus. Werden Daten durch (kryptografische) Prüfsummen geschützt, werden inkorrekte Daten typischerweise direkt verworfen. In Abhängigkeit der Anwendung kann eine Erhöhung der Verfügbarkeit dennoch erreicht werden, wenn die Daten beispielsweise mittels Redundanz oder Neuübertragung trotz einer eventuellen Verzögerung nachgeliefert werden. Wird ein Prozess durch verworfene, fehlerhafte Daten gestört, hat dies zwar sichtbare Auswirkungen auf die Verfügbarkeit, die dann aber mit den Folgewirkungen fehlerhafter Daten in Relation gesetzt werden müssen.

Für die Vertraulichkeit ist insbesondere die Systemintegrität von Bedeutung. Ist ein System kompromittiert, kann ein Angreifer möglicherweise vertrauliche Daten auslesen oder am Endpunkt verschlüsselter Kommunikationsverbindungen mitlesen. Es ist deswegen in verschiedenen Standards und Empfehlungen vorgeschrieben, die Systemintegrität von kryptografischen Systemen beim Start und/oder während des Betriebs zu überprüfen. Die meisten

Protokolle zur Speicherung oder Übertragung von Daten kombinieren Mechanismen der Verschlüsselung mit kryptografischem Integritätsschutz.

Konsequenz:

- Der Schutz der Integrität von Daten, Systemen und Prozessen wird wichtiger und ist eine wesentliche Grundlage für die anderen Schutzziele: Verfügbarkeit und Vertraulichkeit.

2.3 Bestimmung: Daten- und Systemintegrität

Die Integrität einer Komponente oder eines Systems beschreibt die Unverfälschtheit der Funktionalität, das heißt, ein Gerät oder System ist integer, wenn es sich funktional wie gewünscht und beschrieben verhält.

Der Begriff bildet sich dann auf jeder Komponente und Implementierungsebene eines Geräts ab: auf Hardware (HW), Betriebssystem (BS), Treiber, Applikationen, Konfigurationsparameter (HW, BS, Applikationen) und auch auf den Schutz der Integrität dieser Komponenten (z. B. Tamper-Schutz). Die Integrität jeder Teilkomponente eines Geräts geht in die Bewertung der (Gesamt-)Integrität des Geräts ein. Mit Integrität von Daten wird deren Unverfälschtheit bezeichnet.

Mit „Integritätsschutz" bezeichnet man Mechanismen/Funktionen, die eine nicht autorisierte Veränderung (und damit eine Verfälschung) nicht manipulierbar anzeigen oder verhindern. Ein solcher Mechanismus für Daten kann zum Beispiel ein Message-Authentication-Code (MAC) sein. Ein klassischer Cyclic-Redundancy-Check (CRC) schützt nur gegen zufällige Veränderungen von Daten. Jedoch kann ein Angreifer ihn fälschen. Daher ist ein CRC in diesem Sinne kein Mechanismus zum Integritätsschutz.

Bei der Betrachtung der Integrität sind jedoch dynamische Aspekte zu berücksichtigen, die durch eine berechtigte Veränderung von Komponenten, Systemen oder Daten verursacht werden. Werden beispielsweise Daten von Sensoren einer Produktionsstraße zu einem Human Machine Interface (HMI) übertragen und vor ihrer Anzeige entsprechend aufbereitet, so handelt es sich dabei um eine gewollte Veränderung der Daten. Ebenso können berechtigte Änderungen an Systemfunktionen aufgrund eines notwendigen Hardwaretauschs oder durch geplante Software-Upgrades erfolgen. Diese berechtigten, dynamischen Veränderungen dürfen zu keinem Integritätsverlust führen; somit müssen Funktionen für einen „Integritätsschutz" entsprechend ausgelegt sein bzw. flexibel angepasst werden.

Bei der Betrachtung der Integrität sind folgende Fragenstellungen zu berücksichtigen:

Unverfälschtheit von Daten:

Bei der Betrachtung muss unterschieden werden zwischen Daten, die übertragen werden, und Daten, die auf einem System gespeichert sind.

Für die Übertragung ist relevant:

- Integrität: Wie kann zuverlässig erkannt werden, ob es bei einer Übertragung von Daten zwischen verschiedenen Komponenten zu einer Verfälschung gekommen ist? Beziehungsweise: Wie kann sichergestellt werden, dass übertragene Daten korrekt angekommen sind, es also bei der Übertragung weder zu einer zufälligen noch zu einer gezielten Veränderung gekommen ist?

- Authentizität: Wie kann zuverlässig erkannt werden, dass übertragene Daten von einer bestimmten Komponente gesendet wurden? Wie kann die Authentizität der übertragenen Daten geprüft werden? Das heißt, es muss die Möglichkeit bestehen zu prüfen, ob Daten von einer bestimmten Komponente gesendet und nicht durch einen Angreifer erstellt oder während der Übertragung eingespielt oder verändert wurden.

Bei Daten, die auf einer Komponente gespeichert sind:

- Integrität: Wie kann sicherstellt werden, dass Daten seit der letzten Prüfung nicht unbefugt oder zufällig verändert wurden? Dies kann zum Beispiel bei Konfigurationsdaten relevant sein, um gezielte und zufällige Veränderungen zu erkennen.
- Authentizität: Wie kann zuverlässig erkannt werden, wer die Daten abgelegt hat, von wem die Daten stammen oder wer die letzte Veränderung vorgenommen hat?

Für die Aufgabenerfüllung der Komponenten/Systeme ist es essenziell, dass Daten (z. B. Befehle) unverändert ausgetauscht und abgespeichert werden. Ohne integre, also gesicherte und korrekte Daten lässt sich kein korrekter und sicherer Betrieb einer Komponente, Maschine oder Anlage erreichen. Es darf einem Angreifer nicht möglich sein, dass Befehle einer Steuerung (z. B. die korrekte Motordrehzahl oder ein Signal zur Notabschaltung eines Motors) manipuliert werden.

Unverfälschtheit der Systeme:

- Wie kann man sicherstellen, dass an der Kommunikation beteiligte Dinge auch wirklich das – und nur genau das – tun, was ihrer vorgesehenen Funktion im jeweiligen Kontext entspricht?

Ebenso ist es möglich, dass ein anderer Teil der Steuerungssoftware Fehler aufweist, durch deren Ausnutzung ein Angreifer das Verhalten der Steuerung so beeinflussen kann, dass eine Notabschaltung überhaupt nicht mehr ausgeführt wird.

2.4 Betrachtung der Gesamtintegrität eines Systems

In der Regel besteht eine industrielle Anlage nicht nur aus einem einzigen System, sondern aus einer Vielzahl miteinander kommunizierender Teilsysteme. Jedes dieser Einzelsysteme kann, für sich genommen, integer oder nicht integer sein. Die Integrität des Gesamtsystems ergibt sich daher aus der Integrität der Teilsysteme. Zusätzlich ist bei der Integritätsbetrachtung auch die Integrität der Daten, die zwischen diesen Teilsystemen ausgetauscht werden, zu berücksichtigen. Das Gesamtsystem kann als integer betrachtet werden, wenn alle Teilsysteme sowie die Kommunikation zwischen den Teilsystemen integer sind. Im Umkehrschluss beeinflusst jedoch auch eine fehlende Integrität eines Teilsystems oder einer Kommunikation die Integrität des Gesamtsystems.

Der Einfluss von fehlender Integrität einer Komponente lässt sich nicht pauschal beurteilen, sondern hängt von der Rolle der Komponente im Gesamtsystem ab. Fehlende Integrität in einer zentralen Steuerungskomponente wiegt dabei in der Regel schwerer als die fehlende Integrität einer nicht sicherheitskritischen Komponente ohne maßgeblichen Einfluss auf die Produktion und das Produkt. Um die Folgen einer Verletzung der Integrität einer Einzelkomponente beurteilen zu können, ist eine Detailbetrachtung der Auswirkung auf das Gesamtsystem nötig. Die Auswirkungen können dabei von vernachlässigbaren Effekten bis hin zur Gefährdung für Leib, Leben und Umwelt reichen. Für das Gesamtsystem sollte daher eine Abschätzung des Versagens der Teilsysteme erstellt werden.

2.4.1 Parameter und Zusammenhänge

Während eine quantitative Betrachtung der Integrität (z. B. „das System ist zu 78 % integer“) nicht zielführend bzw. nicht machbar ist, ermöglicht eine qualitative Betrachtung der Integrität und ihres Verlusts die Gestaltung von kompensierenden Maßnahmen. Bei dieser Betrachtung sollten die verschiedenen Gründe für ein Fehlen der Integrität berücksichtigt werden. Diese können sein:

- Veränderungen des Systems über die Zeit: Komplexe industrielle Systeme sind oftmals über lange Zeiträume im Einsatz. Dies bedingt, dass die Systeme an unterschiedliche Anforderungen angepasst werden. Diese Anpassungen können schleichend zu negativen Effekten in Bezug auf die Wiederstandsfähigkeit gegen Angriffe führen. Ein System, das graduell unsicherer geworden ist, kann gegebenenfalls von einem Angreifer verändert werden, sodass entweder die System- oder die Datenintegrität nicht mehr gegeben ist. Vorausschauende Maßnahmen können durch zusätzliche Prüfung oder durch Abschottung des Systems eine steigende Verwundbarkeit ausgleichen. Neue kompensierende Maßnahmen sollten bei jeder Veränderung des Systems geprüft werden.

  Beispiel: Eine Firewall wird für eine Anwendung parametriert. Diese Anwendung wird später durch eine andere Anwendung ersetzt, die Firewall-Regeln werden aber nicht nachgepflegt. So können durch Änderungen in der Parametrierung und der Software ungewünschte Wechselwirkungen entstehen, indem zum Beispiel für eine bestimmte Anwendung die Firewall angepasst wird.
- Alterung von Krypto-Algorithmen durch neue wissenschaftliche Erkenntnisse und höhere Rechenkapazität: Der technische Fortschritt und neue wissenschaftliche Erkenntnisse lassen bestehende kryptografische Algorithmen altern, indem zunehmende Rechenleistung und innovative Rechenwege Angriffe auf vormals sicher bewertete Algorithmen ermöglichen. In der Vergangenheit mussten mehrmals kryptografische Mechanismen bereits nach wenigen Jahren ausgetauscht werden, da sie keinen ausreichenden Schutz mehr boten. Zwei der zentralen Elemente der Datenintegrität sind kryptografische Prüfsummen und digitale Signaturen. Auch diese Mechanismen unterliegen der beschriebenen Alterung. Beim Entwurf von Systemen ist daher auf eine Austauschbarkeit der kryptografischen Algorithmen und Schlüssel zu achten. Während des Betriebs ist regelmäßig zu prüfen, ob die eingesetzten Algorithmen noch sicher sind. Ansonsten ist eine unbemerkte Veränderung von Daten und Systemen nicht ausgeschlossen.
- Technischer Fortschritt in der offensiven Sicherheit: Sicherheitsforscher und Angreifer entwickeln stets neue Angriffsmethoden gegen bestehende Systeme. Die Entdeckung eines neuen Angriffs führt oftmals schlagartig zum Verlust der angenommenen Integrität eines Systems. In diesem Falle müssen entweder unsichere Softwarekomponenten aktualisiert oder zusätzliche kompensierende Maßnahmen (z. B. Erkennungs- und Isolationsmaßnahmen) eingesetzt werden, um die Integrität der Systeme weiterhin zu gewährleisten.
- Menschliches Versagen und Fehlbedienung: Bei der Bedienung oder Konfiguration kann es zu Fehleingaben oder einer Änderung an der falschen Komponente kommen. Hier ist eine automatische Überprüfung der Datenbereiche vorzusehen.
- Technisches Versagen und Umwelteinflüsse: Bei Fehlern in der Hardware von Komponenten oder durch störende Umwelteinflüsse (wie z. B. elektromagnetische Strahlung) kann es zu zufälligen Veränderungen an Daten bei der Übertragung oder gespeicherten Daten kommen. Solche Fehler müssen erkannt und es muss entsprechend darauf regiert werden. So können Mechanismen zur redundanten Speicherung, zur Fehlerkorrektur oder einer erneuten Übertragung genutzt werden, um nicht mehr integre Daten wiederherzustellen oder korrekt zu übertragen.

Auch bei der Betrachtung eines Einzelsystems lassen sich Teilbestandteile identifizieren, die einen Einfluss auf das Teilsystem haben. Wichtige Teilkomponenten sind:

a) die Hardware des Systems, einschließlich der IT-typischen Komponenten wie Speicher, CPU und Peripherie, aber auch Sensoren und Steuerungen.
b) die Software des Systems, einschließlich Bibliotheken und Schnittstellen.
c) die Kommunikationsprotokolle, über die ein System Daten austauscht.
d) die Gesamtsystemarchitektur und die sich ergebende Konfiguration der Einzelsysteme.

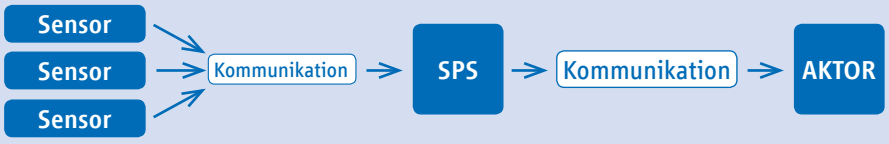
Der Einfluss all dieser Einzelkomponenten ist bei einer qualitativen Untersuchung der Gesamtintegrität eines Systems zu berücksichtigen.

2.4.2 Betrachtung der Integrität am Beispiel eines SPS-Szenarios

Für die weitere Betrachtung und Konzeptualisierung der Integrität wird ein Anschauungsbeispiel gewählt/herangezogen. Angesichts ihrer Verbreitung und Relevanz für die Industrie wird eine speicherprogrammierbare Steuerung (SPS) gewählt. Eine SPS übernimmt zentrale Monitoring-, Steuerungs- und Automationsaufgaben zwischen der Ebene des Manufacturing-Execution-Systems (MES) und der Feldebene. Aus Security-Sicht übernimmt sie damit eine interessante „Schnittstellen- und Gateway-Funktion" innerhalb der Produktion und in anderen Automationsanwendungen (z. B. Smart Home und Smart Building).

Für das weitere Verständnis wird folgende generische Prozess- und Handlungskette angenommen:

Abb. 1: SPS-Szenario



Quelle: ZVEI

Von den Sensoren werden Messdaten (z. B. Temperatur, Druck oder Füllzustand) erfasst und an die SPS übertragen. Die SPS empfängt die Daten, verarbeitet sie und sendet Steuerbefehle an einen Aktor. Der Aktor (z. B. ein Motor oder eine Pumpe) setzt die Befehle um.

Bei der Übertragung der Messdaten von den Sensoren oder an den Aktor sind folgende Gefährdungen der Datenintegrität möglich (Auswahl):

- Zufälliger Übertragungsfehler zum Beispiel durch elektromagnetische Strahlung
- Veränderung der Messdaten
- Einspielen von falschen Messdaten

Die Konsequenz in all diesen Fällen ist, dass die SPS mit falschen oder fehlerhaften Daten arbeitet; aus ihrer Logik heraus können so falsche Entscheidungen getroffen werden und der Aktor kann in der Folge falsch agieren.

Folgende Probleme der Systemintegrität beeinflussen die korrekte Arbeit der SPS (Auswahl):

- Veränderungen des Betriebssystems, des Steuerungsprogramms oder der Konfiguration durch zufällige Fehler

- Gezielte Manipulation des Betriebssystems / der Software, des Steuerungsprgramms oder der Konfiguration durch einen Angreifer
- Versehentliche/falsche Änderung des Steuerprogramms oder der Konfiguration durch einen Bediener

Die Verhaltensweise ist nicht mehr im normalen Bereich. Die Steuerung des Aktors und die Auswertung der Sensordaten erfolgen nicht mehr korrekt.

Die Beispiele zeigen, dass sowohl die einzelnen Komponenten als auch das Gesamtsystem im Zusammenspiel betrachtet werden müssen. So muss die Übertragung der Daten zwischen den Komponenten untersucht und sichergestellt werden, da falsche oder fehlerhafte Daten als Entscheidungsgrundlage vorliegen und so falsche Aktionen ausgelöst werden können. Gleichzeitig müssen aber auch alle Systeme ordnungsgemäß arbeiten. Wenn das nicht der Fall ist, führen auch die korrekt übertragenen Daten nicht zu dem gewünschten Ergebnis.

Wenn die Integrität einer Komponente oder ihre Kommunikation verletzt werden, müssen die Folgen für das gesamte System betrachtet werden. Um den Schutz der Integrität zu erreichen, sind daher präventive und reaktive Maßnahmen zu ergreifen. Diese ermöglichen zum einen das Erkennen von Veränderungen an Daten und Systemen und verhindern zum anderen Veränderungen bzw. ermöglichen eine Rekonstruktion oder beschreiben das Verhalten, wie auf eine solche Verletzung reagiert werden soll.

2.5 Technische Maßnahmen zur Prüfung und Gewährleistung von Integrität

Anhand des zuvor beschriebenen Beispiels werden exemplarische Maßnahmen zur Erkennung des Integritätsverlusts beschrieben. Es wird dabei unterschieden, wer für die Umsetzung der Maßnahmen verantwortlich ist. Die Tabelle gibt einen Überblick über die verschiedenen Maßnahmen. Eine ausführliche Beschreibung erfolgt unterhalb der Tabelle.

Übersicht Maßnahmen für Integritätsschutz

Gefährdung	Hersteller	Integrator	Betreiber
Zufälliger Übertragungsfehler z. B. durch elektromagnetische Strahlung	Einsatz von Protokollen mit Prüfsummen	Nutzung von Protokollen mit Prüfsummen	Überwachung der Protokolle
Veränderung von Messdaten durch einen Angreifer	Einsatz von Protokollen mit Signaturen Protokollierung	Nutzung von Protokollen mit Signaturen Rollout von Identitäten auf Komponenten Protokollierung	Überwachung der Prokollierung Verwaltung der Identitäten auf den Komponenten
Einspielen von falschen Messdaten durch einen Angreifer	Einsatz von Protokollen mit Signaturen Protokollierung	Nutzung von Protokollen mit Signaturen Rollout von Identitäten auf Komponenten Protokollierung	Überwachung der Prokollierung Verwaltung der Identitäten auf den Komponenten
Veränderungen des Betriebssystems, des Steuerungsprogramms oder der Konfiguration durch zufällige Fehler	Einsatz von Prüfsummen zur Erkennung von Fehlern/ Veränderungen	Einsatz von Prüfsummen und Bestätigung	Einsatz von Prüfsummen und Bestätigung
Gezielte Manipulation des Betriebssystems / der Firmware/Schlüsselspeicher durch einen Angreifer	Einsatz von signierten Firmware-Updates Secure-Boot Sicherer Speicherbereich	Prüfung der Herkunft von Firmware-Updates	Prüfung der Herkunft von Firmware-Updates
Gezielte Manipulation des Steuerungsprogramms durch einen Angreifer	Möglichkeiten zur Signatur von Steuerungsprogrammen Möglichkeiten zur Authentisierung vor dem Einspielen von Steuerungsprogrammen Protokollierung	Signierung von Steuerungsprogrammen Rollout von Identitäten zur Prüfung auf die Komponenten Protokollierung	Überwachung der Protokollierung Verwaltung der Identitäten auf den Komponenten
Gezielte Manipulation der Konfiguration durch einen Angreifer	Möglichkeiten zur Signatur von Konfigurationsparamtern Protokollierung	Signierung von Steuerungsprogrammen Rollout von Identitäten zur Prüfung auf den Komponenten Protokollierung	Überwachung der Protokollierung Verwaltung der Identitäten auf den Komponenten
Versehentliche/ falsche Änderung des Steuerungsprogramms oder der Konfiguration durch einen Bediener	Möglichkeiten zur sicheren Identifikation und Authentifizierung[2] von Nutzer und Komponente Möglichkeiten zur Valididierung von Konfigurationsparametern Protokollierung	Authentisierung[3] und Autorisierung vor Änderungen Vorgabe von Werteparametern und Validieren der Werte Protokollierung	Überwachung der Protokollierung Verwaltung der Identitäten auf den Komponenten

[2] Authentifizierung ist die Prüfung der behaupteten Authentisierung.
[3] Authentisierung ist der Nachweis einer Komponente oder Person, dass sie diejenige ist, die sie vorgibt zu sein

2.5.1 Einsatz von Protokollen mit Prüfsummen

Zur Erkennung von zufälligen Fehlern, die zum Beispiel durch elektromagnetische Strahlung entstehen können, ist es bereits heute üblich, Prüfsummen zu nutzen; dies wird bei vielen Übertragungsprotokollen berücksichtigt. Eine bekannte Variante sind CRC-Prüfsummen. Diese ermöglichen die Erkennung von Veränderungen und in begrenzten Maßen sogar die Rekonstruktion von Originaldaten. Entsprechende Protokolle müssen durch den Hersteller in Komponenten implementiert und unterstützt werden.

2.5.2 Einsatz von Protokollen mit Signaturen

Einfache Prüfsummen bieten keinen Schutz vor absichtlichen Veränderungen durch einen Angreifer, denn der Angreifer ist in der Lage, bei der Veränderung auch die Prüfsumme anzupassen. Gegen diese Veränderungen bieten Signaturen oder schlüsselbasierte kryptografische Hashfunktionen ausreichend Schutz. Beispiele hierfür sind Message-Authentication-Code (MAC) oder Signaturen auf Basis von asymmetrischer Krpytografie. Die Funktionen werden durch kryptografische Bibliotheken bereitgestellt, wie sie zum Beispiel in OPC UA[4] oder TLS[5] genutzt werden.Diese Protokolle müssen durch den Hersteller in Komponenten implementiert und unterstützt werden.

Zu beachten ist, dass Sender und Empfänger jeweils in der Lage sein müssen, die Authentizität der Nachrichten zu prüfen (Authentifizierung). Dies kann erfordern, dass beide Seiten mit einer Identität ausgestattet sind, die durch den jeweils anderen geprüft werden kann.

2.5.3 Einsatz von Prüfsummen zur Erkennung von Fehlern/Veränderungen

Ähnlich wie bei der Erkennung von Fehlern bei der Übertragung sollten Mechanismen umgesetzt werden, die zufällig auftretende Fehler auf den Komponenten erkennen. Ursachen können auch hier elektromagnetische Stahlung oder Hardwaredefekte sein.

2.5.4 Einsatz von signierter Firmware, Software und Updates

Die Auslieferung und Installation von Firmware bzw. Software allgemein ist ein kritischer Vorgang. Es muss verhindert werden, dass manipulierte Varianten installiert werden. Ein Angreifer könnte beispielsweise eine Schadfunktion, die ihm später einen Angriff ermöglicht, oder Backdoor-Funktionalitäten integrieren, um an Daten zu gelangen, ohne den Dateninhalt zu verändern.

Daher sollte für solche Installationspakete eine Möglichkeit bestehen, die Integrität und Authentizität zu validieren. Hersteller sollten entsprechende Informationen wie beispielsweise Prüfsummen auf einem unabhängigen Kanal zur Verfügung stellen. Alternativ kann auf einer Komponente, beispielsweise vor einem Update, eine an der Firmware angebrachte Signatur geprüft werden. Die Installation findet nur statt, wenn diese erfolgreich geprüft werden kann.

2.5.5 Möglichkeiten zur Überwachung der Systemintegrität

Hersteller sollten Maßnahmen zur Überprüfung und Überwachung der Integrität von Komponenten vorsehen. Mit diesen soll erkannt werden können, dass eine Veränderung an der Firm- oder Software stattgefunden hat.

Eine Möglichkeit, dies zu realisieren, ist Secure-Boot. Dabei wird das Starten auf bestimmte signierte Firmware beschränkt.

[4] Open-Plattform-Communications – Unified Architecture
[5] Transport-Layer-Security

2.5.6 Möglichkeiten zur Signatur von Steuerungsprogrammen und Konfigurationsparametern

Eine Veränderung von Steuerungsprogrammen oder Konfigurationsdaten auf einer Komponente kann erhebliche Auswirkungen haben. So können durch ein manipuliertes oder falsches Steuerungsprogramm fehlerhafte Aktionen ausgeführt oder falsche Entscheidungen getroffen werden, die sich in Form fehlerhafter Produkte oder eines Schadens an einer Maschine auswirken. Gleiches gilt für Konfigurationen.

Daher sollte die Möglichkeit bestehen, die Daten, die auf eine Steuerung aufgebracht werden, auf Veränderungen zu prüfen und bei Abweichungen nicht einzuspielen.

2.5.7 Möglichkeiten zur Authentisierung und Autorisierung vor dem Einspielen von Steuerungsprogrammen und Konfigurationsparametern

Bevor eine Veränderung an einer Komponente durchgeführt wird, sollte sich ein Nutzer gegenüber einer Komponente authentisieren, das heißt, er sollte einen Nachweis erbringen, dass er die behauptete Identität besitzt (z. B. mittels eines Passworts oder eines digitalen Zertifikats). Dies steht in einem engen Zusammenhang mit Abschnitt 2.5.9 Rollout von Identitäten auf Komponenten. Außerdem muss die Komponente auf dieser Basis entscheiden, ob der Nutzer berechtigt ist, die Veränderungen vorzunehmen. Dieser Vorgang wird Autorisierung genannt.

Um die vorgenommenen Änderungen nachvollziehen zu können, sollten diese protokolliert werden.

2.5.8 Möglichkeiten zur Validierung von Konfigurationsparametern

Um Fehleingaben von Anwendern zu erkennen und vermeiden zu können, sollte es möglich sein, für Eingabeparameter einen Wertebereich vorzugeben. Dies kann ein Zahlenbereich oder eine festgelegte Länge von Zeichen und der Zeichen selbst sein. Dabei wird vor dem Verarbeiten der Werte geprüft, ob vom festgelegten Wertebereich abgewichen wird. Diese Prüfung sollte grundsätzlich bei allen Schnittstellen erfolgen.

Als Alternative können die Abhängigkeiten zwischen Parametern überprüft werden. Beispiel: Parameter A muss FALSE sein, wenn zuvor Parameter B auf „2“ gesetzt wurde. Die Beziehungen kann man zum Beispiel mittels Featurebäume modellieren und später im Code überpüfen.

2.5.9 Rollout von Identitäten auf Komponenten

Damit einige der zuvor genannten Maßnahmen genutzt werden können, muss es einfache und sichere Methoden geben, um Identitäten auf Komponenten einrichten zu können. Diese werden für die Authentisierung benötigt. Obwohl diese Maßnahmen nicht direkt dem Schutz der Integrität dienen, ist ein Fehlen problematisch, da dies eine Hürde für Einrichtung und Betrieb darstellt. In der Folge wird bisher auf die Nutzung von Schutzmaßnahmen verzichtet oder der Aufwand im Einsatz deutlich erhöht. Weitere Informationen zum Thema sichere Identitäten finden sich im „Technischen Überblick: Sichere Idenitäten“ der Plattform Industrie 4.0[6].

2.5.10 Protokollierung

Veränderungen an Daten, Systemen und Prozessen sollten protokolliert werden, um eine Integritätsverletzung feststellen zu können. Registrierte Integritätsverletzungen an Daten,

[6] https://www.plattform-i40.de/I40/Redaktion/DE/Downloads/Publikation/sichere-identitaeten.html

Systemen und Prozessen sind ebenfalls zu dokumentieren. Die Protokolle selbst sind außerdem vor Veränderungen zu schützen.

2.5.11 Überwachen der Protokollierung

Für die Protokollierungsdaten ist festzulegen, wie diese in Bezug auf neue Ereignisse überwacht werden. Es ist in diesem Zusammenhang festzulegen und zu dokumentieren, wie mit festgestellten Integritätsverletzungen umgegangen wird.

2.5.12 Verwaltung der Identitäten auf den Komponenten

Nach dem Rollout von Identitäten gilt es, sie dauerhaft zu verwalten. Dazu gehört neben dem regelmäßigen Austausch der Authentisierungsdaten auch die Pflege der jeweils gültigen Nutzer. Hierfür müssen auf den Komponenten entsprechende Funktionalitäten bereitgestellt und auf der anderen Seite Prozesse etabliert werden, welche die notwendigen Aktivitäten anstoßen.

2.5.13 Signierung und Prüfung der Herkunft von Firmware-Updates

Updates spielen eine wichtige Rolle insbesondere zur Beseitigung von sicherheitsrelevanten Schwachstellen in Komponenten. Um einen Missbrauch zu verhindern, ist es notwendig, dass Updates vor dem Einspielen auf ihre Integrität und Authentizität geprüft werden. Damit wird sichergestellt, dass ein Update nicht verändert wurde (etwa keine durch einen Angreifer hinzugefügte Funktion enthält) und vom Hersteller stammt (d. h. nicht von einem Dritten/Angreifer). Falls die Integrität verletzt ist, darf das Update nicht eingespielt werden.

2.5.14 Signierung und Prüfung von Steuerungsprogrammen

Ähnlich wie bei den Updates sollte auch bei den Steuerungsprogrammen für eine SPS vorgegangen werden. Damit soll verhindert werden, dass ein manipuliertes Steuerungsprogramm eingespielt wird.

2.6 Umgang mit Störung der Integrität

Die Störung der Integrität kann in einer Anlage zu verschiedensten Gefährdungen führen. Wichtig dabei ist, dass je nach Komponente die fehlende Integrität verschiedenste Auswirkungen haben kann und dass daher auch verschiedenste Reaktionen angemessen sind. Das Spektrum der angemessenen Verhaltensweisen bei Feststellung der verletzten Integrität reicht von einem kontrollierten Weiterbetrieb bis hin zu einer sofortigen Abschaltung oder Notfallbehandlung. Die folgenden zwei Beispiele verdeutlichen dies:

Ein Beispiel für einen Fall, in dem trotz des Verlusts der Integrität einer Komponente keine schwerwiegenden Probleme auftreten, wäre beispielsweise eine Maschine, deren Sensoren den Schmiermittelstand zur automatischen Schmierung falsch anzeigen. Die Anlage kann trotz eines gegebenenfalls zu niedrigen Schmiermittelstands weiter betrieben werden, wenn ein zusätzlicher Mechanismus zum Schutz der Maschine vorhanden ist. Eine unmittelbare Notabschaltung der Maschine beim Erkennen der Integritätsverletzung ist folglich nicht nötig, da der Verlust der Integrität keine unmittelbaren schwerwiegenden Auswirkungen hat.

Ein Beispiel, das eine sofortige Abschaltung rechtfertigt, ist die Störung der Integrität einer sicherheitskritischen Einheit, zum Beispiel die Anzeige falscher Temperaturen durch die Sensorik von überwachten Leistungsbauteilen in der Stromversorgung einer Maschine. Dies kann zur Zerstörung der Stromquelle oder sogar zur Gefährdung der Arbeiter führen. In

einem solchen Fall muss umgehend eingegriffen werden. Ein sicherer Weiterbetrieb ist nicht möglich.

Beide Beispiele zeigen, dass eine fehlende Integrität sehr unterschiedliche Auswirkungen haben kann und dass die Reaktionen auf Integritätsverletzungen sehr verschieden ausfallen können. Daher ist eine Einzelbetrachtung nötig. Leitfragen können sein: Welche Komponenten sind kritisch für den Betrieb und welche Daten oder Schwellwerte werden als Basis für weiterführende folgenschwere Entscheidungen verwendet?

Zur weiteren Erläuterung zum Umgang und den Folgen werden zwei Fallbeispiele für Integritätsstörungen dargestellt:

Fallbeispiel 1: „Condition-Monitoring":
Eine Maschine ist mit Sensoren ausgestattet, um rechtzeitig – vor Stillstand – eine Wartung der Maschine veranlassen zu können. Über eine cloudbasierte Plattform werden die erhobenen Sensordaten der Maschine dem Service-Dienstleister zu Verfügung gestellt.

In dieser Informationskette können, ausgehend vom Sensor an der Maschine bis zum Service-Dienstleister, unter anderem folgende Integritätsstörungen auftreten:
- Sensor erhebt die Daten fehlerhaft.
- Auf dem Übertragungsweg zur cloudbasierten Plattform werden die Daten verfälscht.
- Auf der cloudbasierten Plattform werden die Daten verfälscht.
- Auf dem Übertragungsweg von der cloudbasierten Plattform zum Servicedienstleister werden die Daten verfälscht.

Unabhängig davon, wo und auf dem welchem Weg die Integrität der Daten gestört wurde, kann das einen finanziellen Schaden für den Maschinenbetreiber zur Folge haben:
a. Leicht: Finanzieller Schaden durch zu häufige Wartungen aufgrund fehlerhafter Sensordaten (Wartungsfall zu früh erkannt).
b. Schwer: Finanzieller Schaden durch Produktionsausfall aufgrund fehlerhafter Sensordaten (Wartungsfall zu spät erkannt). Die Integritätsstörung geht in diesem Fall einher mit einem Verlust der Verfügbarkeit.

Fallbeispiel 2: „Verbrauchsmaterialbestellung":
Eine Maschine (3D-Drucker) ordert notwendiges Rohmaterial für den Produktionsprozess beim internen (externen) Lieferanten.
Unter anderem können folgende Integritätsstörungen auftreten:
- Rohmaterial wird zu früh bestellt.
- Rohmaterial wird falsch bestellt.
- Rohmaterial wird zu spät bestellt.

Auch hier kann unabhängig davon, wo und auf welchem Weg die Integrität der Daten gestört wurde, ein finanzieller Schaden für den Maschinenbetreiber entstehen:
a. Leicht: Finanzieller Schaden durch zu frühe Lieferung (höhere Lagerhaltungskosten).
b. Schwer: Finanzieller Schaden durch zu späte bzw. falsche Bestellung (neben der Störung der Integrität kommt noch ein Verfügbarkeitsproblem dazu).

2.7 Ausblick: Integritätsschutz als Grundlage der Vertrauenswürdigkeit

Insbesondere die Gestaltung einer unternehmens- und grenzenübergreifenden Kommunikation stellt eine Herausforderung für die Security dar. Um eine sichere (unternehmensübergreifende) Kommunikation überhaupt realisieren zu können, muss zuerst ein Vertrauensverhältnis zwischen den beteiligten Kommunikationspartnern etabliert werden. Die Kommunikationspartner können dabei sowohl schon länger miteinander bekannt sein oder das erste Mal überhaupt miteinander in Kontakt treten. Für den betroffenen Wirtschaftsakteur stellt sich somit verstärkt die Frage, inwiefern er diesen bekannten und neuen Kommunikationspartnern so weit vertrauen kann, dass er sich mit ihnen sicher vernetzen und Informationen austauschen kann.

Die Integrität wirkt sich im Zusammenhang mit Industrieanlagen auch auf die physische Welt und die Sicherheit von Personen und Umwelt aus. Um die Digitalisierung von Industrieanlagen vorantreiben zu können, müssen die Kommunikationspartner möglichst vertrauenswürdig (= trustworthy) sein. Das setzt wiederum voraus, dass sich der Betreiber und der Benutzer auf die korrekte Funktionserfüllung der Systeme verlassen können. Dies bedingt, dass sowohl die Integrität der Kommunikation der Systeme als auch die Integrität des Zustands der Systeme (nach dem aktuellen Stand der Technik) sichergestellt ist.

3 Vertrauenswürdigkeit

3.1 Was ist Vertrauenswürdigkeit?

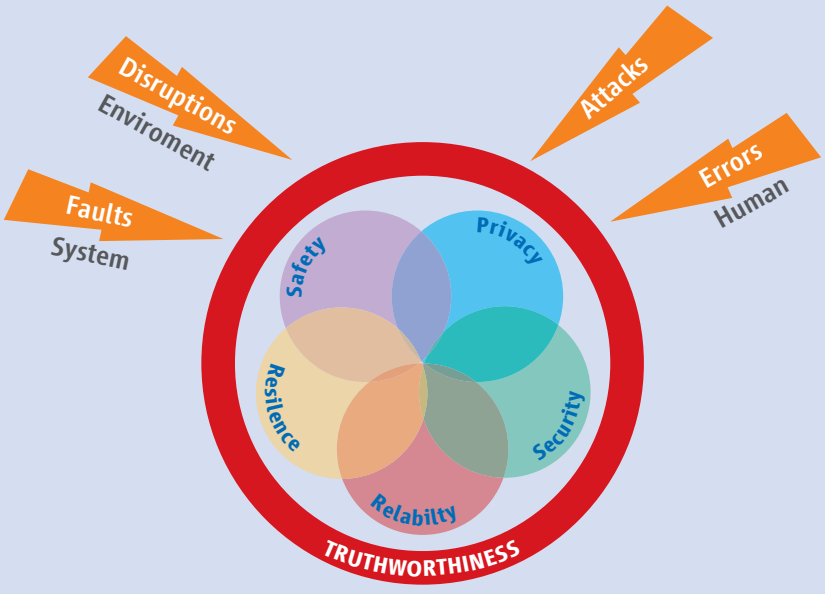
Vertrauenswürdigkeit (= Trustworthiness; siehe Abbildung 2) beschreibt den Grad des Vertrauens[7], den das Produkt[8] in Bezug auf alle wichtigen Systemmerkmale im Hinblick auf Umweltstörungen, menschliche Fehler, Systemfehler und Schutz vor Angriffen erfüllt. Der Begriff dient dazu, die Qualität der bestehenden und der zukünftigen Beziehungen zwischen Firmen, Menschen, Systemen und Komponenten zu beschreiben. Bei einem vertrauenswürdigen System gibt es positive Anhaltspunkte, dass sich eine betrachtete Einheit in einer zu erwartenden Art verhalten wird. Die Integrität einer Einheit stellt einen wichtigen Baustein der Vertrauenswürdigkeit dar, da ohne System- und Datenintegrität keine Aussagen über das angenommene Verhalten einer Einheit gemacht werden können. Die Vertrauenswürdigkeit geht jedoch noch weiter als die Integrität: Beispielsweise kann ein durch den Besitzer bewusst schädlich konfiguriertes System durchaus integer (unverändert und korrekt operierend) und trotzdem für die Interaktionspartner, die mit diesem System kommunizieren, nicht vertrauenswürdig sein. Wie dieses Beispiel zeigt, ist die Integrität zwar eine notwendige Grundkomponente der Vertrauenswürdigkeit, sie ist jedoch nicht allein hinreichend für Vertrauenswürdigkeit, da die Intention eines Besitzers bzw. Betreibers eines Systems, einer Komponente oder gar einer Firma einen weiteren Einfluss auf die Vertrauenswürdigkeit hat. Aus dieser Beobachtung lässt sich schließen, dass die Vertrauenswürdigkeit eine Eigenschaft zwischen verschiedenen Systemen, Firmen und Individuen ist, während die Integrität ein Merkmal innerhalb eines Systems, einer Komponente oder einer Firma darstellt. Das Konzept gilt für die Information-Technology (IT) und für die Operational Technology (OT) gleichermaßen, wenn auch kontextabhängig mit unterschiedlicher Gewichtung der Kategorien.

Die charakteristischen Kategorien für die Vertrauenswürdigkeit sind demnach:

• Security • Safety • Privacy • Zuverlässigkeit (Reliability) • Resilienz (Resilience)

Auch das eventuelle Fehlen einer oder mehrerer Kategorien (z. B. Safety in der IT oder Privacy in der OT) ändert grundsätzlich nichts an dem Konzept.

Abb. 2: Kategorien der Vertrauenswürdigkeit



Quelle: Industrial Internet Consortium

[7] Vertrauen besteht aus den Punkten 1) Parameter, 2) Validierung und 3) menschliche Entscheidung. Das Thema Integrität adressiert nur die Punkte 1 und 2. Vertrauen wird auch als „gefühlte Sicherheit" bezeichnet.

[8] Der Produktbegriff wird hier generisch verwendet und steht für jede Art von Dienstleistung, Hardware oder Software. Ein Produkt ist eine Komposition von Komponenten. Eine Komponente kann Bestandteil sein von einem oder mehreren Produkten (z. B. Softwarekomponenten). Ein Produkt kann wiederum als Komponente von einem anderen Produkt betrachtet werden.

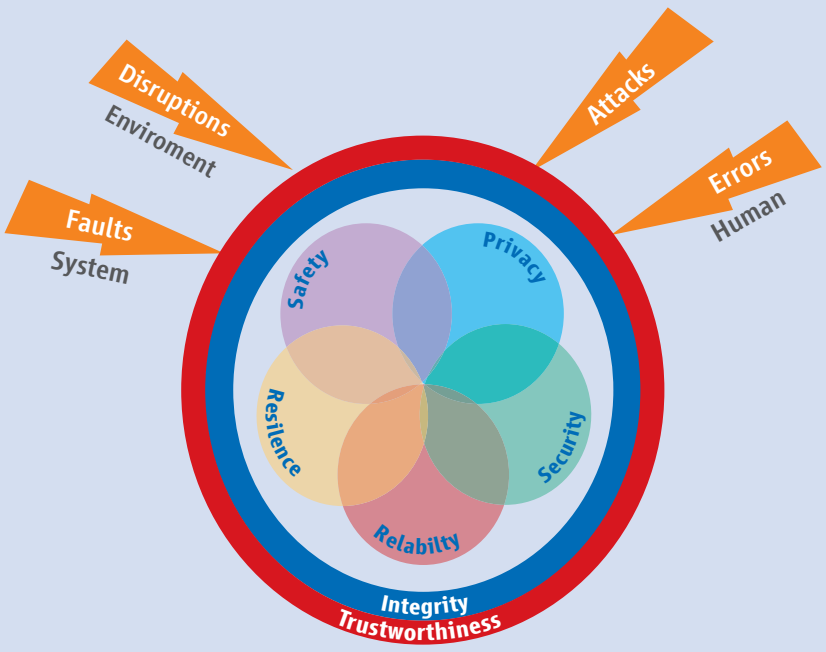
Hersteller, Integratoren und Betreiber stehen vor dem Hintergrund der Digitalisierung und Vernetzung vor der gleichen Herausforderung: Sie sind auf die Korrektheit, Vollständigkeit und Unverfälschtheit der Daten, Systeme, Kommunikation und Prozesse verstärkt angewiesen. Diese Tendenz nimmt zu, je weiter man sich Richtung automatisierter und autonomer Systeme entwickelt. Im Kern führt dies zu einem Umdenken. Traditionell steht in der Industrie das Schutzziel der Verfügbarkeit an oberster Stelle. In automatisierten, autonomen Vorgängen ist die menschliche reaktive Einflussmöglichkeit jedoch gering. Daten, Systeme, Kommunikation und Prozesse müssen von Beginn an korrekt funktionieren. Dahinter steht, dass ein (unbemerkt) mangelhaft produziertes Produkt oder ein fehlerhafter Prozess am Ende aufwendiger oder kostenintensiver sein mag als der punktuelle Stillstand der Maschinen und Anlagen (siehe Produktrückrufe, Gewährleistungspflichten und Schadensersatzansprüche nach dem Verkauf). Sprich: Der Schutz der Integrität gewinnt gegenüber der Verfügbarkeit an Bedeutung. Fehlende Integrität bedeutet, dass ein Fehler in der Übermittlung bzw. ein Fehler in der Umsetzung der Prozesse zu einem fehlerhaften Verhalten und damit potenziell zu einem fehlerhaften Produkt führen können.

Vertrauenswürdigkeit betrachtet sowohl die Fehlerfreiheit der implementierten Funktionen als auch die Abwesenheit von (bekannten) Schwachstellen, die ein Angreifer verwenden kann, um die Funktion einer Komponente zu ändern oder zu beeinträchtigen.[9] Insbesondere gibt es keine unerwünschten oder nicht dokumentierten zusätzlichen veränderten oder entfernten Funktionen.

3.2 Integrität als wesentliche Voraussetzung der Vertrauenswürdigkeit

Unter den oben genannten Gesichtspunkten wird die Integrität zu einem wesentlichen Schutzziel für alle fünf charakteristischen Kategorien der Vertrauenswürdigkeit.

Abb. 3: Integrität als übergreifendes Schutzziel aller fünf Kategorien



Quelle: Industrial Internet Consortium und ZVEI

[9] Zum Beispiel könnte der Algorithmus, der die Entscheidung zur Notabschaltung eines Motors trifft, fehlerhaft entworfen oder implementiert sein, sodass die Notabschaltung nicht in allen kritischen Fällen erfolgt.

Technische Maßnahmen, die Prozesse und die Organisation müssen hinreichend ausgeprägt und miteinander verschränkt werden, um die Integrität als Kernschutzziel der charakteristischen Kategorien Security, Safety, Privacy, Reliability und Resilienz gewährleisten zu können.

Beispiele für die Bedeutung der Integrität in den einzelnen Kategorien:

- Security: In der Informationssicherheit stellt die Integrität ein eigenes, wichtiges Schutzziel dar. Würden beispielsweise Produktionsparameter fehlerhaft übertragen, so kann dies schnell zu fehlerhaften Produkten führen. Die Integrität steht weiter in einem engen Zusammenhang mit der Authentisierung von Nutzern oder Rollen in einem Produktionsumfeld. Ohne eine integre Übertragung von Daten ist deren Authentisierung nicht möglich. Schließlich kann die Integrität auch Auswirkungen auf andere Schutzziele wie die Vertraulichkeit haben, denn die Vertraulichkeit von Daten kann auf kompromittierten Systemen nicht gewährleistet werden.
- Safety: Im Produktionsumfeld werden häufig Lichtschranken für Safetyaufgaben eingesetzt. Betritt beispielsweise eine Person einen gefährlichen Bereich im Umfeld eines Industrieroboters, so wird dies oft durch Lichtschranken detektiert und führt zum Stopp des Roboters. Ein fehlerhaftes Übertragen der Werte (Lichtstrahl unterbrochen / nicht unterbrochen) hätte eine schwerwiegende Auswirkung auf die Mechanismen der Notabschaltung.
- Privacy: Zwischen der Integrität und der Privacy bestehen verschiedene Bezüge. Beispielsweise ist es schwierig, die Vertraulichkeit personenbezogener Daten, und damit die Privacy, zu gewährleisten, wenn diese auf einem kompromittierten System gespeichert sind. Zugleich wird die Integrität auch direkt gefordert, wenn „personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben“[10] müssen.
- Zuverlässigkeit (Reliability): Würden beispielsweise die Daten einer SPS unbemerkt fehlerhaft übertragen, so kann dies leicht eine negative Auswirkung auf das Produktionssystem und seine Zuverlässigkeit haben. Dies kann sogar weitreichende Folgen bis zur Zerstörung der Anlage verursachen, wenn Anlagen in kritischen Bereichen gefahren werden, ohne dass dies der Anlagenbetreiber merkt.
- Resilienz (Resilience): Der Begriff Resilienz wird im allgemeinen Sprachgebrauch oft mit leicht unterschiedlicher Bedeutung verwendet. Unter Resilienz sei hier die Fähigkeit eines technischen Systems zu verstehen, bei Störungen und Teilausfällen nicht vollständig zu versagen, sondern wesentliche Systemfunktionen und -dienste aufrechtzuerhalten und möglichst zeitnah wieder in den ursprünglichen Zustand zurückzukehren. Somit dient die Integrität neben der Verfügbarkeit und Vertraulichkeit eindeutig zur Erhöhung der Resilienz eines Systems, indem zum Beispiel die fehlerhafte Übertragung von erforderlichen Daten zur Produktionssteuerung erkannt wird, damit umgehend Maßnahmen zur Aufrechterhaltung der korrekten Funktionsweise eines Systems eingeleitet werden können. Beispielsweise könnte eine Anforderung zur erneuten Übertragung der benötigten Daten zur Produktionssteuerung gesendet werden.

[10] § 10 Datenschutzgesetz Nordrhein-Westfalen

3.3 Vertrauenswürdigkeit als übergreifender Ansatz für Liefer- und Wertschöpfungsnetzwerke

Im Rahmen der Cybersicherheit im industriellen Umfeld ist Vertrauenswürdigkeit ein wichtiges, qualitatives Entscheidungskriterium für das unternehmerische Handeln entlang der gesamten Wertschöpfungskette (Value-Chain).

Der Hersteller will seinen Kunden klare, umfangreiche und verlässliche Informationen über die Eigenschaften (insbesondere Security und damit auch Integrität) des überlassenen Systems / Produkts / der überlassenen Komponente geben. Dafür benötigt er seinerseits entsprechend vertrauenswürdige Informationen über die von ihm verbauten Komponenten seiner Zulieferer. Die Vertrauenswürdigkeit dieser Informationskette insgesamt ist auch von den beteiligten Entwicklungs-, Produktions- und Logistikprozessen abhängig.

Aus Sicht eines Herstellers ist die Vertrauenswürdigkeit ein Versprechen gegenüber dem Markt, das unter anderem durch eine Herstellerselbsterklärung zum Ausdruck gebracht werden kann. Ein Audit / eine Zertifzierung durch eine unabhängige Stelle kann den Grad des Vertrauens an die Herstellererklärung erhöhen.

Aus Sicht eines Integrators ist Vertrauenswürdigkeit gegenüber seinen Kunden das Versprechen, entsprechend vertrauenswürdige Komponenten mit entsprechend sicheren Prozessen zu integrieren, sodass dem Betreiber eine Anlage mit klar beschriebenen Sicherheitseigenschaften übergeben werden kann. Bei der Auswahl der Produkte ist auf eine entsprechende Vertrauenswürdigkeit der Hersteller zu achten.

Die Vertrauenswürdigkeit einer Anlage kann nur dann über die Lebenszeit hinweg zuverlässig beurteilt werden, wenn die Integrität der Anlage geschützt wird und Veränderungen ihres Zustands im Rahmen des „Security-Managements“ erfasst werden.

Bei der Bewertung der Vertrauenswürdigkeit zwischen Menschen spielen im Alltag Erfahrungen und Intuition (= unbewusste Bewertung, wie z. B. Historie, Hörensagen, allgemeines und persönliches Wissen sowie das „Bauchgefühl“) eine wesentliche Rolle. Im unternehmerischen Umfeld muss dieses Vertrauensverhältnis substanziiert werden, zum Beispiel durch Zertifizierungen oder Audits. Hierbei entstehen Bewertungen, die jedoch nie zu 100 Prozent objektiv sein können. Dabei erlaubt die Betrachtung technischer Systeme eine gewisse Belastbarkeit. Betrachtungen zur Organisation oder zur wirtschaftlichen Lage eines Unternehmens bieten jedoch Spielraum. Die Möglichkeiten vorsätzlicher Täuschung durch Personen oder ganze Organisationen machen eine „objektive“ Betrachtung noch schwieriger. Insofern werden im langfristigen Verhältnis zweier Unternehmen Erfahrung und gemeinsame Historie weiterhin wichtige Aspekte bleiben.

4 Anforderungen an die Akteure

Hersteller, Integratoren, Betreiber und Dienstleister müssen zunächst die grundlegende Bedeutung der Integrität erkennen und umsetzen. Für den Gesamtschutz der Integrität trägt jeder Akteur individuell Verantwortung:

Hersteller:
Hersteller haben schwerpunktmäßig zwei Aufgaben: Lieferung von integren Produkten und Systemen sowie die Transparenz für Prozesse und Produkteingenschaften bezüglich der Integrität. Entsprechend sind Maßnahmen zum Schutz der Integrität in Entwicklungs- und Produktionsprozessen zu berücksichtigen. Konkrete Hinweise geben zum Beispiel die Teile 4-1 und 4-2 der IEC 62443 für vernetzte industrielle Anlagen sowie ISO 27034 für sichere SW-Entwicklungen.

Die Umsetzung der Maßnahmen können über die etablierten Mechanismen der Herstellerselbsterklärung oder einer Deklaration zum Beispiel nach den oben genannten Standards gegenüber den Kunden transparent gemacht werden.

Integrator:
Integratoren sind auf die Dokumentation und Deklaration hinsichtlich Integrität und Vertrauenswürdigkeit seitens der Hersteller angewiesen bzw. fragen diese nach (z. B. über Audits). Ihnen obliegt es, Störungen der Integrität für das System zu erkennen, zu bewerten und entsprechend zu beheben bzw. zu kompensieren. So sind für die jeweilige Anwendung die passenden Wege der Identifikation, Authentifizierung, Signierung und gegebenenfalls Verwendung von Zertifikaten zu finden (siehe Abschnitt 2.5).

Betreiber:
Ähnlich wie der Integrator trägt der Betreiber die Verantwortung für die gesamte Anlage bezüglich der Erkennung, Bewertung, Behebung oder Kompensation von Störungen der Integrität und damit der Vertrauenswürdigkeit, die er als Betreiber gegenüber anderen hat. Durch den Einfluss der Integrität auf Security, Safety und gegebenenfalls Privacy sind Schutzmaßnahmen essenziell für den Betreiber, um seine eigenen Ziele und gesetzliche Vorgaben zu erfüllen.

Dienstleister:
Bei Industrie 4.0 werden zunehmend Dienstleister eine Marktbedeutung erlangen. Ein Beispiel für einen Dienstleister ist der Marktplatz für Prozessdaten. Diese Prozessdaten werden von einem Broker am Markt angeboten und von einem Betreiber gekauft. Der Datenkauf erspart dem Betreiber zum Beispiel Stillstandszeiten und dadurch Produktionsausfall, reduziert Entwicklungsaufwände und verringert somit allgemein Risiken. Die Dienstleister sind auf die Dokumentation und Deklaration hinsichtlich Integrität und Vertrauenswürdigkeit seitens des Anbieters der Prozessdaten angewiesen bzw. fragen diese nach.

Alle vier Akteure haben die gemeinsame Aufgabe, die Integrität für den gesamten Lebenszyklus der Komponenten, Systeme und Anlagen zu gewährleisten. Die Art und Weise sowie die Bereitstellungsdauer der Maßnahmen müssen von allen Akteuren gegenüber ihren Kunden transparent und eindeutig kommuniziert und gegenüber den Zulieferern eingefordert werden. Dies kann zum Beispiel über Erklärung der Beteiligten oder Einkaufsrichtlinien nach den oben genannten Standards erfolgen. Je nach Umfeld sollte es möglich sein, die Maßnahmen zu prüfen.

Politik:

Die Umsetzung von Industrie 4.0 benötigt integre und vertrauenswürdige Infrastrukturen. Die Politik kann ihren Aufbau gemeinsam mit der Industrie unterstützen. Kein Akteur kann die diesbezüglichen Herausforderungen für Mobilfunk, digitale Identitäten, Kommunikation und Datenverarbeitung allein meistern. Es ist eine ähnliche kooperative Kraftanstrengung erforderlich, wie sie zum Beispiel für die Energiewende umgesetzt wird.

Normung:

Internationale Normungsreihen wie IEC 62443 und ISO 2700x stellen eine erste Grundlage für Integrität und Vertrauenswürdigkeit dar. Zusätzlich ist die international einheitliche Dokumentation und Deklaration der Integritäts- und Vertrauenswürdigkeitsangaben eine Herausforderung. Ziel muss die nahtlose Abfrage und Darstellung der Maßnahmen entlang der Lieferkette und über Ländergrenzen hinweg sein.

5 Zusammenfassung

Mit der zunehmenden Komplexität in Produkten und Systemen durch Digitalisierung und Vernetzung wächst die Bedeutung des Integritätsschutzes. Anwender müssen sich immer stärker auf die Korrektheit, Vollständigkeit und Unverfälschtheit ihrer Daten, Systeme und Prozesse verlassen können. Andernfalls werden fehlerhafte Produkte und Lösungen erzeugt bzw. die Ergebnisqualität insgesamt gefährdet – auch mit entsprechender Relevanz für Nachforderungen, Gewährleistungen und Rückrufe. Der Schutz der Integrität hat in der Industrie 4.0 zunehmend mehr Bedeutung für die elementaren Parameter Qualität, Kosten und Zeit der Produktion. Darüber hinaus legt er auch künftig weiterhin die Basis für die Erfüllung der gesetzlichen Vorgaben der Funktionalen Sicherheit (engl. Safety).

Es gibt zahlreiche Möglichkeiten, mit Störungen der Integrität umzugehen (siehe im Abschnitt 2.5. und 2.6). Insgesamt wird es für die Industrie entscheidend sein, die Integrität mit ihrer Dynamik (Technik- und Risikoentwicklung) entlang der Lebenszeit der Produkte und Lösungen über verschiedene Rollen hinweg beherrschen zu können. Letztendlich ist die Integrität von Daten, Systemen und Prozessen eine der Hauptgrundlagen für die Realisierung vertrauenswürdiger Systeme. Dies ist wiederum die Basis für vertrauenswürdige Kooperationen über Unternehmens- und Ländergrenzen hinweg.

ZVEI:
Die Elektroindustrie

ZVEI - Zentralverband Elektrotechnik-
und Elektronikindustrie e.V.
Lyoner Straße 9
60528 Frankfurt am Main

Telefon: +49 69 6302-0
Fax: +49 69 6302-317
E-Mail: zvei@zvei.org
www.zvei.org

Bildnachweis Titelseite: ZVEI