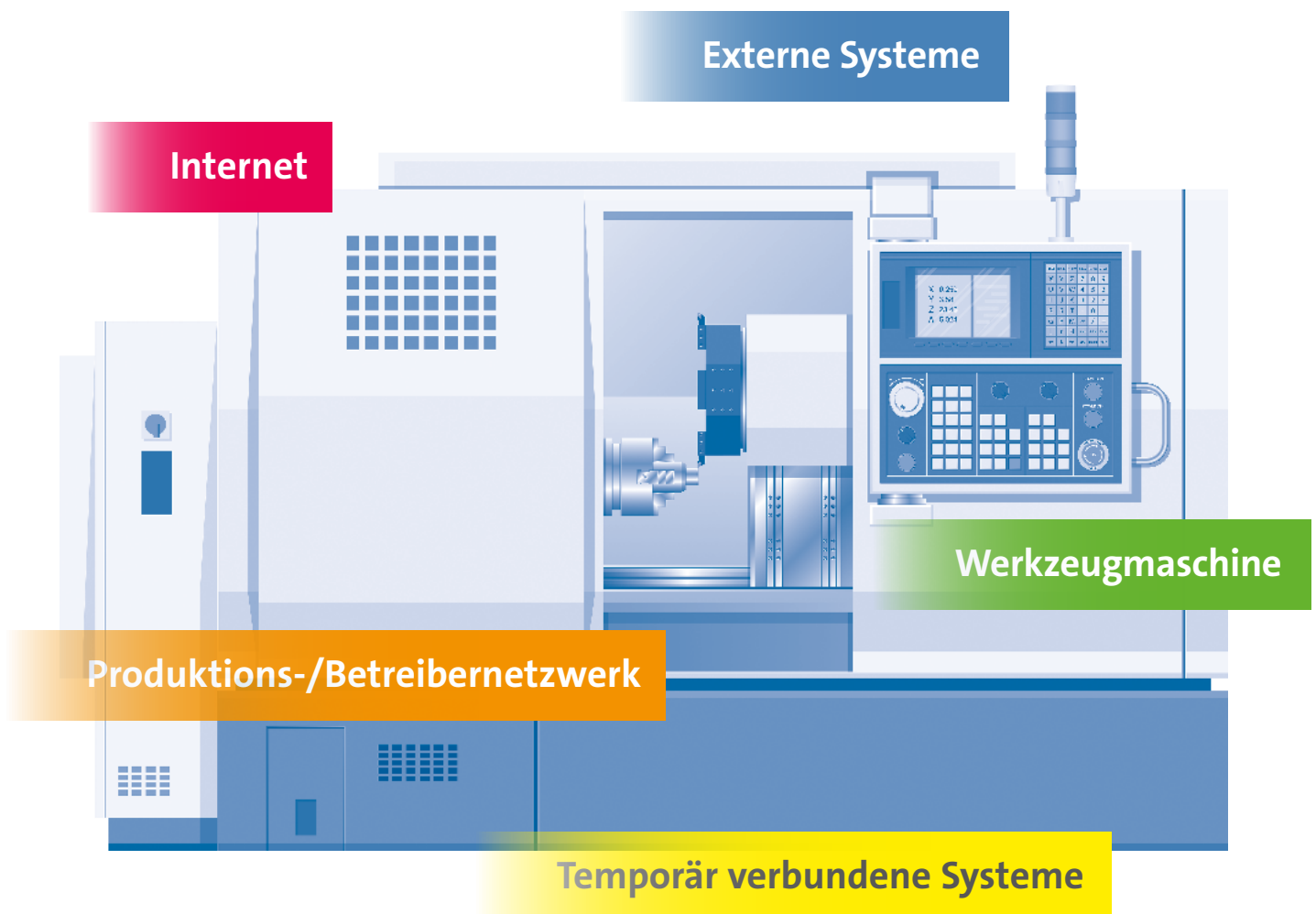


Security an Werkzeugmaschinen

Ein Leitfaden zur methodischen Umsetzung,
Betrachtungen über die gesamte Nutzungsdauer und
Anregungen zur Behandlung von Bestandsmaschinen.

Leitfaden
für
Hersteller



1. Einleitung	3
1.1 Motivation	3
1.2 Zielgruppe	3
1.3 „IT“ vs. „OT“	3
1.4 Anwendungsbereich	4
2. Technischer Hintergrund zu Security	5
2.1 Allgemeine Begriffserläuterung und Definitionen	5
2.1.1 Asset	5
2.1.2 Bedrohung und Gefährdung	5
2.1.3 Brutto-Risiko	6
2.1.4 Conduit (Sicherheitszonenübergang)	6
2.1.5 Device Management (Geräteverwaltung)	6
2.1.6 Eingebettete Komponente	6
2.1.7 HMI (Human Machine Interface)	6
2.1.8 IACS (Industrial Automation and Control System)	6
2.1.9 Integrität (Integrity)	6
2.1.10 Maßnahme (Gegenmaßnahme)	6
2.1.11 Netto-Risiko/Restrisiko	6
2.1.12 Risiko	6
2.1.13 Schnittstelle	7
2.1.14 Schutzbedarf	7
2.1.15 Schutzklassen	7
2.1.16 Schutzniveau	7
2.1.17 Schutzziel	7
2.1.18 Secure Development Lifecycle (SDL) (gesicherter Entwicklungslebenszyklus)	7
2.1.19 Security-Kontext	7
2.1.20 Sicherheitslücke (Schwachstelle)	8
2.1.21 Sicherheitszone (Zone)	8
2.1.22 Sicherheitszonenübergang (Conduit)	8
2.1.23 SL (Security Level)	8
2.1.24 SL-A (Security Level Achieved)	8
2.1.25 SL-C (Security Level Capability)	8
2.1.26 SL-T (Security Level Target)	8
2.1.27 SuC (System under Consideration)	8
2.1.28 Verfügbarkeit (Availability)	8
2.1.29 Vertraulichkeit (Confidentiality)	8
2.2 Die Normenreihe IEC 62443 und die Rolle von Werkzeugmaschinenherstellern	9
2.2.1 Einteilung der Normenreihe	9
2.2.2 Rolle des Werkzeugmaschinenherstellers	10
2.3 Schutzstrategie	11

3. Methodik zur erstmaligen Absicherung einer Maschine	13
3.1 Security-Kontext	13
3.2 Bestimmung eines Security Level Target (SL-T)	17
3.3 Architekturentwurf und Einteilung in Sicherheitszonen	18
3.4 Assets und Schutzbedarf	20
3.4.1 Definition und Beispiele von Assets	20
3.4.2 Ermittlung der Schutzbedarfe	21
3.5 Bedrohungsanalyse und Produktrisiko	22
3.5.1 Allgemeine Beschreibung der Bedrohungsanalyse	22
3.5.2 Die S.T.R.I.D.E.-Methodik	22
3.5.3 Bewertung von Bedrohungen	24
3.5.4 Das CVSS-Bewertungssystem	25
3.5.5 Risikomatrix nach IEC 62443-3-2	26
3.5.6 Exemplarische Bedrohungsanalyse	27
3.6 Security-Anforderungen und -Maßnahmen	28
3.7 Restrisiko	29
3.8 Dokumentation	30
4. Betrachtungen über die gesamte Nutzungsdauer	31
4.1 Grundsätzliches	31
4.2 Maßnahmen und Herangehensweise	31
4.2.1 Management von Sicherheitslücken	32
4.2.2 Umgang mit Sicherheitsupdates	32
4.3 Unterstützung durch Systemlieferanten	33
4.3.1 Rolle der Systemlieferanten	33
4.3.2 Unterstützungsangebote	33
5. Behandlung des „brown field“	34
5.1 Ausgangslage	34
5.2 Abgrenzung und Kapselung von Systemen	34
6. Literatur	37

1. Einleitung

1.1 Motivation

Die digitale Transformation der Fertigung, speziell auch von Werkzeugmaschinen und Anlagen, schreitet weiter voran. Vormalig als Insellösung betriebene Steuerungskomponenten werden unternehmensweit vernetzt oder direkt mit Hilfe des Internets miteinander verbunden und interagieren mit Software-Services in der Cloud. Dabei entstehen sogenannte cyber-physische Systeme.

Diese Systeme werden von Hackern immer mehr in den Fokus genommen, da sie oft sehr einfache Ziele für Cyberangriffe darstellen. Schadsoftware (wie beispielsweise „Mirai“, „Hajime“, „WannaCry“ oder „Petya“) ermöglicht den Angreifern, auf schnelle Weise die Verfügbarkeit von Anlagen und Maschinen erheblich zu beeinträchtigen; Produktionsprozesse kommen zum Stillstand, wirtschaftliche Verluste in Millionenhöhe sind die Folge. Neben den erpressten Geldzahlungen haben die Firmen oft auch große Image-Schäden zu erleiden.

Einen ersten und wichtigen Beitrag zum sicheren Maschinenbetrieb kann der Betreiber selbst leisten. Hinweise und Vorschläge hierzu wurden bereits an anderer Stelle vorgestellt (→ [1])* . Um den Bedrohungen adäquat begegnen zu können, müssen aber auch die Anlagen- und Maschinenbauer künftig sehr viel mehr Wert auf Security legen – sowohl beim Bau der Maschinen als auch im Betrieb. „Security by Design“ ist dabei eine wichtige Methode, die in der Software-Entwicklung seit vielen Jahren erfolgreich angewandt wird. Übertragen auf den Maschinen- und Anlagenbau findet sie Anwendung in der internationalen Norm IEC 62443.

Bisherige Veröffentlichungen bieten eine gute Grundlage für die Auseinandersetzung mit dem Themenkomplex und der Norm, beziehen sich aber vielfach auf Lösungen aus dem Anlagenbau und nehmen noch nicht auf die besonderen Belange von Werkzeugmaschinen Bezug. Dieses Dokument erweitert den Betrachtungsraum auf den gesamten Entwicklungsprozess in Anlehnung an die Normenreihe IEC 62443 und ist spezifisch für Werkzeugmaschinen ausgeführt.

1.2 Zielgruppe

Das vorliegende Dokument richtet sich vorrangig an die **Hersteller von Werkzeugmaschinen und Fertigungsanlagen für die Produktion**.

Als Hersteller im o. g. Sinne werden hier vorrangig Unternehmen des Maschinenbaus angesehen, welche entsprechende Produktionsanlagen entwickeln, vertreiben bzw. in Verkehr bringen und im Laufe ihres Lebenszyklus servizieren.

1.3 „IT“ vs. „OT“

In vielen Betrachtungen zur IT-Security der hier im Fokus stehenden Produktionsanlagen ist der Ausdruck „OT“ („Operational Technology“) in Abgrenzung zur „IT“ („Information Technology“) gebräuchlich. Der Begriff hat sich etabliert, um die technologischen und funktionalen Unterschiede zwischen traditionellen IT-Systemen (wie etwa im Büroumfeld) und der Umgebung von Industrial Control Systems, der sogenannten „IT in non-carpeted areas“, aufzuzeigen.

OT bezeichnet demnach vorrangig Hard- und Software zur Steuerung, Regelung, Kontrolle und/oder Überwachung von industriellen Anlagen, Maschinen, Assets, Prozessen oder Ereignissen. Einen Vergleich IT/OT in Anlehnung an → [2] zeigt → Abb. 1.

*) Literatur-Verweise in eckigen Klammern, siehe Seite 37

Abb. 1:
Unterschiede
in den An-
forderungen
an IT (Büro-
umgebung)
und OT
(Produktions-
umfeld)
Quelle: → [2]

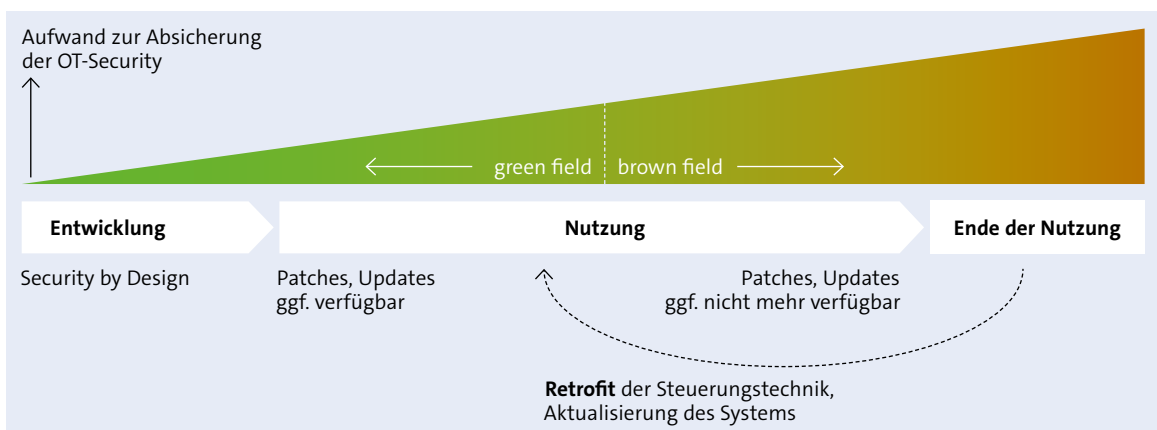
	IT-Systeme	OT-Systeme
Lebensdauer	3 bis 5 Jahre	5 bis >20 Jahre
Entwicklungszyklus	Kurz	An Lebensdauer angepasst
Patchmanagement	Oft, täglich	Selten, benötigt Freigabe vom Systemintegrator/ Komponentenhersteller
Verfügbarkeit	Kurze Ausfälle toleriert	24/7 Die IEC 62443 definiert Sicherheitsziele in Teil 1-1, wobei die Verfügbarkeit als höchstes Schutzziel definiert wurde.
Zeitabhängigkeit	Verzögerungen akzeptiert	Kritisch Die IEC 62443 definiert Sicherheitsziele in Teil 1-1, wobei die Echtzeitfähigkeit als Millisekundenbereich angegeben wird.
Kosten	ca. 1.000 €	Viele T€ bis zu Mio. €

Es wird deutlich, dass erhebliche Unterschiede bestehen, welche wiederum eine darauf zugeschnittene Herangehensweise erfordern.

1.4 Anwendungsbereich

Im Anschluss an eine Einführung in das Thema mit einer Klärung/Definition der wichtigsten Begriffe im Rahmen von → Kapitel 2 folgt in → Kapitel 3 der Schwerpunkt der vorliegenden Veröffentlichung: Dieser liegt auf der Vermittlung einer Methodik zur Absicherung des Entwicklungs- bzw. Entwurfsprozesses. Auf die Nennung von Best Practices wird größtenteils zugunsten eines überschaubaren Umfangs und einer breiten technischen Abdeckung verzichtet. Im Vordergrund steht die Absicht, den Maschinenhersteller selbst zu befähigen, einen solchen sicheren Entwicklungsprozess durchzuführen: Zum Entwurfszeitpunkt bei Neumaschinen im „green field“ bestehen die besten Ausgangsbedingungen, effizient einen hohen Schutzgrad zu erreichen (→ Abb. 2). Der Aufwand steigt in den späteren Phasen der Nutzung entlang der Zeitachse stetig an, weshalb eine initiale Anstrengung die bestmögliche Grundlage für ein sicheres System darstellt.

Abb. 2:
Anwendungs-
bereich des
vorliegenden
Dokuments



Aufgrund der zu erwartenden langjährigen Nutzungsdauer von Werkzeugmaschinen – verbunden mit der Gewissheit, dass ein Großteil der Maschinen beim Kunden aus Bestandsmaschinen besteht – reicht eine Auseinandersetzung mit dem Entwicklungsprozess allein jedoch noch nicht aus, weshalb auch die weitere Nutzungsdauer (→ Kapitel 4) und auch das „brown field“ (→ Kapitel 5), also der Bestand, in den Blick genommen wird. Zu diesen Betriebsphasen werden Hinweise gegeben, die als Weiterführung eines Gesamtkonzeptes zum sicheren Betrieb verstanden werden können, aber auch als Einzelmaßnahmen etwa im Bestand umsetzbar sind.

2. Technischer Hintergrund zu Security

2.1 Allgemeine Begriffserläuterung und Definitionen

2.1.1 Asset

Physisches oder logisches und im Allgemeinen schutzwürdiges Objekt, das sich im Besitz oder unter der Obhut einer Organisation befindet und das entweder einen wahrgenommenen oder tatsächlichen Wert für die Organisation hat.

Anmerkung: Ein Asset kann materiell oder immateriell sein.

Beispiele: Komponente, Steuerung, Know-how, Daten, NC-Programme.

2.1.2 Bedrohung und Gefährdung

Potenzial zur Verletzung der Sicherheit oder zur Herbeiführung eines Schadens, verursacht durch eine Handlung, eine Fähigkeit, ein Ereignis oder einen Umstand. Den Sachverhalt illustriert → Abb. 3.

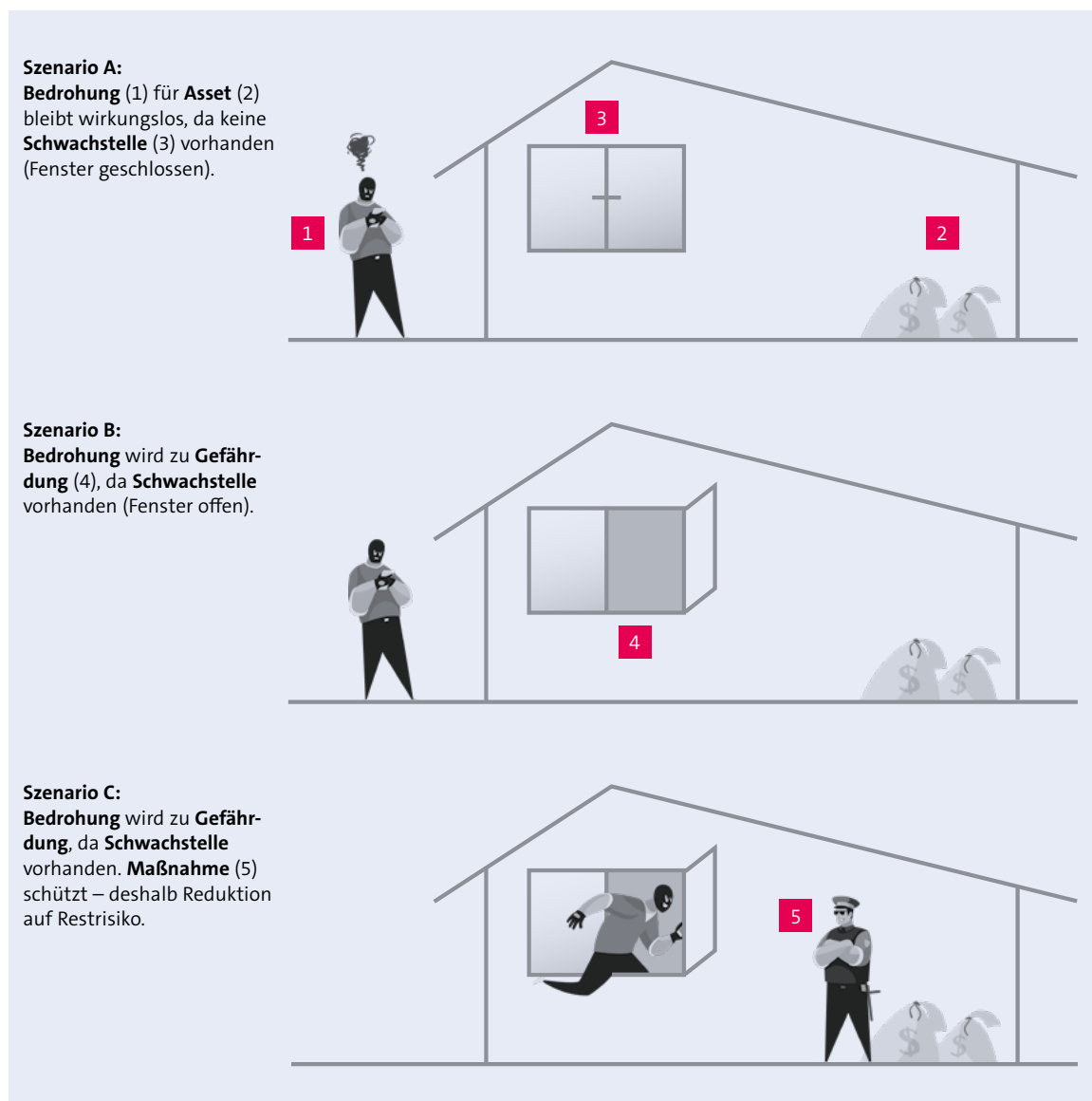


Abb. 3:
Zusammenhang zwischen Bedrohung und Gefährdung

Eine Bedrohung stellt zunächst eine abstrakte, theoretisch mögliche Gefährdung dar. Ein Beispiel wäre die Existenz zahlreicher Schadsoftware-Programme im Internet, welche etwa Portscans ausführen, um „Opfer“ zu finden. Die Bedrohung wirkt sich i. d. R. aufgrund entsprechender Schutzmaßnahmen zunächst nicht aus, etwa aufgrund einer Firewall. Sie wird aber in dem Moment zu einer realen Gefährdung, in dem eine Sicherheitslücke ausgenutzt wird (z. B. eine Lücke in der Firewall) und damit die Bedrohung konkret zur Gefährdung für ein Asset wird. Auch dies bedeutet noch nicht den zwangsläufigen Eintritt eines Schadensereignisses, erhöht aber die Wahrscheinlichkeit bzw. das Risiko dafür deutlich.

2.1.3 Brutto-Risiko

Risiko vor Anwendung von Maßnahmen zur Risikobehandlung.

2.1.4 Conduit (Sicherheitszonenübergang)

Logische Gruppierung von Kommunikationskanälen, die zwei oder mehr Zonen verbindet, für die gemeinsame IT-Security-Anforderungen gelten.

Anmerkung: Ein Conduit darf eine Zone durchqueren, solange die IT-Security der im Conduit verlaufenden Kanäle durch die Zone nicht beeinträchtigt wird.

2.1.5 Device Management (Geräteverwaltung)

Verstanden wird darunter die (meist von einer zentralen Stelle aus, z. B. einem Dienstleister erfolgende) Verwaltung eines IT-Gerätes. Darunter fallen sowohl die Überwachung der Hardware (Auslastung, Lüfterdrehzahlen, freier Speicher etc.) als auch die Wartung der Software (Aktualisierung des Softwarestands aufgrund von Sicherheitspatches oder Funktionserweiterungen, Installieren/Löschen von Software etc.) sowie zentrale Management-Aufgaben, z. B. eindeutige Identifikation und Katalogisierung von Geräten, automatisches Neueinrichten bei Gerätetausch.

2.1.6 Eingebettete Komponente

Eine eingebettete Komponente ist eine Komponente, die im Produkt verwendet wird. Bei Software sind dies z. B. verwendete Bibliotheken. Eingebettete Komponenten können weitere eingebettete Komponenten enthalten (transitive Einbindung).

2.1.7 HMI (Human Machine Interface)

Als HMI wird die Benutzerschnittstelle einer Maschine bezeichnet (umfasst Hardware und Software).

Anmerkung: Im Kontext dieses Dokuments i. d. R. das Software-System zur Bedienung der Maschine.

2.1.8 IACS (Industrial Automation and Control System)

Industrielle(s) Automatisierungssystem(e).

2.1.9 Integrität (Integrity)

Qualität eines Systems,

- die logische Korrektheit und Zuverlässigkeit des Betriebssystems,
 - die logische Vollständigkeit der Hard- und Software zur Umsetzung der Schutzmechanismen und
 - die Konsistenz der Datenstrukturen und die Korrektheit der gespeicherten Daten
- zu gewährleisten.

Daten dürfen ohne Berechtigung nicht verändert, manipuliert oder gelöscht werden können, durchgeführte Änderungen müssen nachvollziehbar sein.

2.1.10 Maßnahme (Gegenmaßnahme)

Tätigkeit, Gerät, Prozedur oder Verfahren, durch die eine Bedrohung, eine Sicherheitslücke oder die Folgen eines Angriffs verringert werden, und zwar durch die Verringerung des möglichen Schadens oder durch Entdeckung und Bericht, so dass Korrekturmaßnahmen eingeleitet werden können.

2.1.11 Netto-Risiko/Restrisiko

Risiko nach Anwendung von Maßnahmen zur Risikobehandlung.

2.1.12 Risiko

Schaden, ausgedrückt als die Wahrscheinlichkeit, dass eine bestimmte Bedrohung eine bestimmte Sicherheitslücke mit einer bestimmten Konsequenz ausnutzt.

2.1.13 Schnittstelle

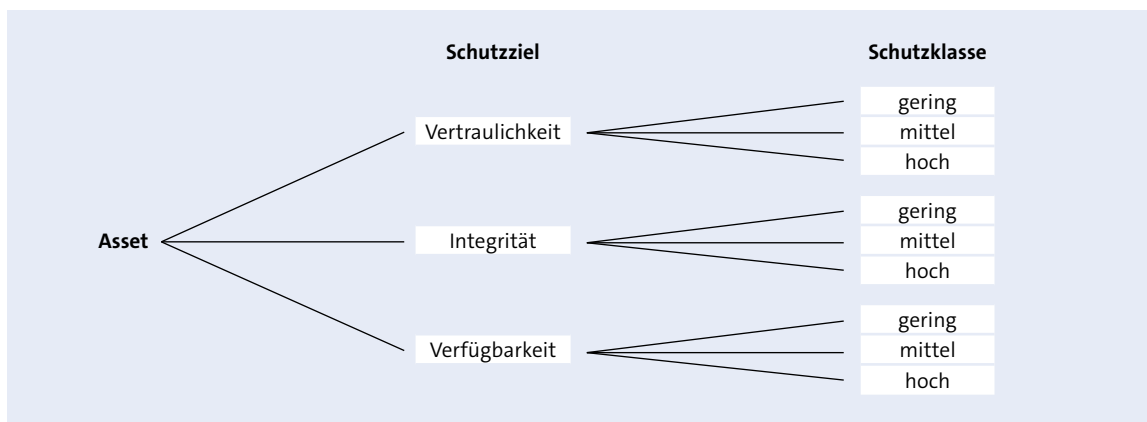
Jede Art von physikalischer oder Software-Schnittstelle.

2.1.14 Schutzbedarf

Der Schutzbedarf eines Objekts klassifiziert und orientiert sich an dem Ausmaß der Schäden, die entstehen können, wenn seine Funktionsweise durch Beeinträchtigung der Schutzziele beeinflusst ist.

Für jedes Asset ist der Schutzbedarf zu ermitteln. Dazu ist für jedes der Schutzziele zu bewerten, wie hoch die Schutzklasse gewählt werden muss, also ob der Schutzbedarf für ein Asset bezüglich Vertraulichkeit, Integrität und Verfügbarkeit als gering, mittel oder hoch einzustufen ist (→ Abb. 4).

Abb. 4:
Schutzbedarf
eines Assets



2.1.15 Schutzklassen

Unter Schutzklassen versteht man die Gruppierung des Schutzbedarfs anhand von (potenziellen) Schäden (z. B. finanziell oder bezüglich der Reputation) oder Gefährdungen, um eine einheitliche Behandlung zu ermöglichen.

Anmerkung 1: Durch die Gruppierung in Schutzklassen lässt sich eine einfache und objektive Bewertung von Schadenshöhe und Schadensfolgen erreichen.

Anmerkung 2: In diesem Dokument kommt die Einteilung in die Schutzklassen „gering“, „mittel“ und „hoch“ zur Anwendung.

Anmerkung 3: Andere Einteilungen sind möglich.

2.1.16 Schutzniveau

Höhe des Security Level.

2.1.17 Schutzziel

Schutzziele sind Aussagen oder Definitionen zu einem Sicherheitsniveau, welches im Minimum erreicht werden soll.

Anmerkung: In diesem Dokument kommt die Einteilung in die Schutzziele „Vertraulichkeit“, „Integrität“ und „Verfügbarkeit“ zur Anwendung.

2.1.18 Secure Development Lifecycle (SDL) (gesicherter Entwicklungslebenszyklus)

Alle Phasen eines Entwicklungsprozesses, von der Analyse und Definition von Security-Anforderungen über das Produkt-Design, die Implementierung, die Verifikation und Validierung bis zur Behandlung von Security-Problemen während des gesamten Produktlebenszyklus bis zum Ende der Nutzungsphase.

2.1.19 Security-Kontext

Beschreibung des OT-Sicherheitsumfelds, in dem die Werkzeugmaschine eingesetzt wird und das für den bestimmungsgemäßen Betrieb vorausgesetzt wird.

2.1.20 Sicherheitslücke (Schwachstelle)

Fehler oder Schwäche in Entwurf, Implementierung, Betrieb oder Verwaltung eines Systems, die genutzt werden können, um die Integrität oder die Sicherheitsrichtlinien des Systems zu verletzen.

2.1.21 Sicherheitszone (Zone)

Gruppierung von Assets, für die gemeinsame Security-Anforderungen gelten.

Anmerkung 1: Eine Zone hat eine klare Grenze zu anderen Zonen.

Anmerkung 2: Die Sicherheit einer Zone kann durch Mechanismen innerhalb der Zone oder an der Zonen-grenze oder durch eine Kombination von beidem erreicht werden.

2.1.22 Sicherheitszonenübergang (Conduit)

→ *Abschnitt 2.1.4*

2.1.23 SL (Security Level)

Maß des Vertrauens, dass die Werkzeugmaschine frei von Sicherheitslücken ist und in der beabsichtigten Weise funktioniert.

Anmerkung 1: Sicherheitslücken können bei der Entwicklung des IACS entstehen, während seines Lebens-zyklus zu irgendeinem Zeitpunkt in dieses hingebacht werden oder sich aus verändernden Bedrohungen ergeben.

Anmerkung 2: Bei der Entwicklung entstandene Sicherheitslücken können möglicherweise erst lange nach der Inbetriebnahme erkannt werden, beispielsweise wurde eine Verschlüsselungstechnik ungenügend umgesetzt oder die Leitlinien zur Verwaltung von Nutzerkonten waren unzureichend, wozu z. B. das Nicht-Entfernen alter Benutzerkonten zählt.

Anmerkung 3: Eingebachte Sicherheitslücken können das Ergebnis eines Patches oder geänderter Leitlinien sein, durch die eine neue Sicherheitslücke geöffnet wird.

2.1.24 SL-A (Security Level Achieved)

Erreichter Security Level.

2.1.25 SL-C (Security Level Capability)

Erreichbarer Security Level.

2.1.26 SL-T (Security Level Target)

Angestrebter Security Level.

Anmerkung: Der zu erzielende Security Level ist i. d. R. ein Ergebnis der Bedrohungs-/Risikoanalyse.

2.1.27 SuC (System under Consideration)

Betrachtetes System.

Anmerkung: In diesem Dokument ist die Werkzeugmaschine das betrachtete System.

2.1.28 Verfügbarkeit (Availability)

Der Zugriff auf Daten innerhalb eines vereinbarten Zeitrahmens muss gewährleistet sein.

2.1.29 Vertraulichkeit (Confidentiality)

Sicherstellung, dass Informationen nicht an unbefugte Personen, Prozesse oder Geräte weitergegeben werden.

2.2 Die Normenreihe IEC 62443 und die Rolle von Werkzeugmaschinenherstellern

2.2.1 Einteilung der Normenreihe

IEC 62443 bezeichnet eine Normenreihe, welche sich mit IT-Security für „Industrial Automation and Control Systems“ (IACS) befasst. Sie entstand ursprünglich als Norm für die Automatisierungstechnik in der Prozessindustrie, deckt jedoch heute alle Industriebereiche von diskreter Fertigung bis hin zu verteilten Versorgungssystemen für Strom, Öl, Wasser und Gas ab. Diese Normenreihe hat sich als Maßstab zur Betrachtung von Industrial Security über den gesamten Lebenszyklus von Automatisierungslösungen etabliert. Sie wird als die zentrale Norm für Security angesehen, in ihrer Bedeutung ähnlich, wie es die ISO 13849 für die funktionale Sicherheit ist.

1	IEC TS 62443-1-1	IEC 62443-1-3*		
Allgemeine Grundlagen	Terminology, concepts and models	System security conformance metrics		
2	IEC 62443-2-1	IEC 62443-2-2*	IEC TR 62443-2-3	IEC 62443-2-4
Für Betreiber	Security program requirements for IACS asset owners	Security protection rating	Patch management in the IACS environment	Requirements for IACS service providers
3	IEC TR 62443-3-1	IEC 62443-3-2	IEC 62443-3-3	
Für Systemintegratoren	Security technologies for IAC	Security risk assessment and system design	System security requirements and security levels	
4	IEC 62443-4-1	IEC 62443-4-2		
Für Komponentenhersteller	Secure product development life-cycle requirements	Technical security requirements for IACS components		

Abb. 5: Übersicht der Normenreihe IEC 62443 (Darstellung in Anlehnung an IEC 62443-3-1)

*) Entwurf

Es handelt sich um eine umfangreiche Normenreihe, deren einzelne Bestandteile sich in ihrer Ausrichtung an drei unterschiedliche Zielgruppen wenden. Entsprechend der in → Abb. 5 gezeigten Übersicht können die einzelnen Teile wie folgt zugeordnet werden:

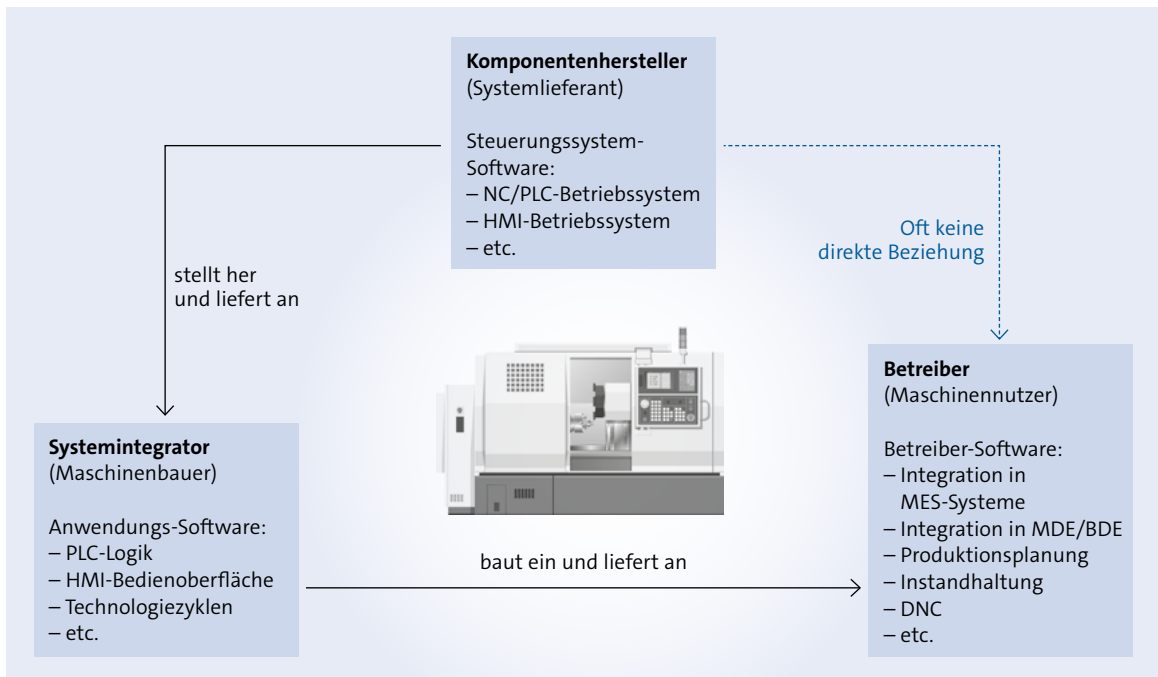
- 1 IEC 62443-1 beschreibt **allgemeine Grundlagen** und Konzepte und stellt damit für alle weiteren Teile der Normenreihe eine Bezugsbasis dar.
- 2 IEC 62443-2 wendet sich vorrangig an die **Betreiber** von industriellen Anlagen – aus Sicht eines Werkzeugmaschinenherstellers also an die Käufer und Anwender der Maschinen.
- 3 IEC 62443-3 adressiert in der Sprechweise der Norm die **Systemintegratoren und Anlagenhersteller** – dieser Teil ist von **zentraler Bedeutung für die Hersteller von Werkzeugmaschinen**, da diese vorrangig als Systemintegrator im Sinne der Norm agieren.
- 4 IEC 62443-4 ist fokussiert auf die **Hersteller von Maschinenkomponenten** (also in erster Linie auf die Zulieferer, etwa von Steuerungen) – wobei sich hier eine starke inhaltliche Überlappung insbesondere mit Teil 3 ergibt, da Werkzeugmaschinenhersteller vielfach auch Komponenten für die eigenen Anlagen herstellen und ggf. Komponenten auch einzeln veräußern.

2.2.2 Rolle des Werkzeugmaschinenherstellers

Aufgrund der Historie der IEC 62443 im Umfeld des Anlagenbaus ergibt sich für einen Werkzeugmaschinenhersteller zunächst keine ganz eindeutige Trennung zwischen der Rolle eines Systemintegrators und eines Komponentenherstellers. Es gibt aber eine klare Schwerpunktsetzung: Ein Unternehmen des Maschinenbaus als Hersteller und Entwickler von Werkzeugmaschinen nimmt in dieser Aufstellung vorrangig die Rolle des **Systemintegrators** ein, da eine Vielzahl von Komponenten von verschiedenen Zulieferern zu einem Gesamtsystem kombiniert werden, welches aus Sicht des Betreibers (vor allem aus einer IT-Perspek-

tive) dann als eine Maschine angesehen wird. Entsprechend dieser Zuordnung zeigt → *Abb. 6* die Beziehungen zwischen den drei Rollen Komponentenhersteller, Systemintegrator und Betreiber.

Abb. 6:
Zusammen-
spiel der
Rollen
Hersteller,
Integrator,
Betreiber



Bisweilen findet sich ein Werkzeugmaschinenbauer auch in der Rolle des Komponentenherstellers wieder, wenn dieser für seine eigenen (oder andere) Maschinen selbst entsprechend tätig wird. Im Sinne der IEC 62443 **betrifft diese Rolle aber vorrangig die IT-Perspektive**; die Eigenfertigung von rein mechanischen Baugruppen wie Gestellkomponenten, Führungen etc. wird hier also nicht in den Mittelpunkt gestellt. Anders gelagert ist der Fall insbesondere bei den verbreiteten **Eigenentwicklungen im Bereich Software** (z. B. HMI-Systeme, Technologiezyklen, Interface-Software). Hier ist im Sinne der IEC 62443 der Werkzeugmaschinenbauer klar in der Rolle des Herstellers verortet und damit im Sinne von Teil 4 der Norm auch verantwortlich für eine entsprechende sichere Umsetzung seiner Eigenentwicklung. Dies gilt auch für „kombinierte“ Systeme aus Hard- und Software, etwa intelligente Spindeln oder komponentenintegrierte Sensorik, sofern diese im IT-Sinne eigenständige Komponenten bilden.

Prinzipiell gilt das beschriebene Rollenmodell auch für die Komponentenlieferanten: Beispielsweise wird ein Steuerungshersteller seinerseits auch (Software-)Komponenten von Dritten einsetzen, aus deren Sicht ist er dann der Systemintegrator. Entwickelt ein Betreiber eigene Software-Komponenten, welche auf der Maschine eingesetzt werden, so wird er ebenfalls im Sinne der Norm zuständig als Hersteller oder Systemintegrator.

2.3 Schutzstrategie

Werkzeugmaschinen sind komplexe technische Systeme, die aus **mehreren Subsystemen** (aus Steuerungssicht z. B. HMI, NC-Steuerung, Connectivity-Gateways) bestehen und mit einer Reihe von Aggregaten verbunden sind (etwa Lademagazine, KSS-Anlagen, Hydraulikaggregate etc.). Zusätzlich werden die Maschinen regelmäßig **vom und mit dem Kunden angepasst und häufig mit Erweiterungen von Dritt-anbietern** (z. B. einer Werkzeugbruchüberwachung) ergänzt – und darüber hinaus im Laufe ihres Einsatzes über die Jahre oft weiter modifiziert.

Dieser komplexe Anwendungsfall führt dazu, dass **eine isoliert betrachtete und einmalige Absicherung der Maschine (im Sinne der OT-Security) noch keine ausreichende Schutzwirkung entfaltet**.



Abb. 7:
Schutz-
strategie für
Werkzeug-
maschinen

Erforderlich ist vielmehr eine kombinierte Schutzstrategie im Sinne von → Abb. 7:

1. Ein bereits auf einen **hohen Sicherheitsstandard hin ausgerichteter Entwicklungsprozess**, welcher anhand einer entsprechenden Methodik gestaltet wird.

- Eine solche Methodik zur Gewährleistung eines sicheren Entwicklungsprozesses wird in diesem Dokument in Anlehnung an die IEC 62443-4-1 vorgeschlagen und soll im Folgenden vermittelt werden (→ Kapitel 3).
- Diesen **inneren Schutzmantel** bilden hier die im Entwicklungsprozess abgesicherten Eigenschaften – angefangen bei der Spezifikation der Security-Anforderungen und -Richtlinien über die Methodik zur „Security by Design“ bis zur gesicherten Implementierung mit anschließender Verifikation.
- Ziel ist die möglichst vollständige **erstmalige Absicherung** der Maschine.

2. **Begleitende Maßnahmen während des gesamten Lebenszyklus** der Maschine, auch nach der Lieferung an den Kunden, um einen hohen Sicherheitsstandard über die gesamte Nutzungsdauer halten zu können.

- Den **äußeren Schutzmantel** bildet der sichere Betrieb, also Maßnahmen zur Laufzeit bzw. während der gesamten (!) Lebenszeit der Maschine.
- Diesem Aspekt wurde bereits eine Veröffentlichung (→ [1]) gewidmet, in → Kapitel 4 und → Kapitel 5 folgen weitere Ausführungen zur Absicherung auch nach der Lieferung.

Die IEC 62443 definiert allgemeine Anforderungen an einen gesicherten Entwicklungsprozess für Produkte, die in industriellen Automatisierungssystemen eingesetzt werden. Die Norm beschreibt dazu einen gesicherten Entwicklungslebenszyklus („Secure Development Lifecycle“, SDL). Der SDL umfasst alle Phasen eines Entwicklungsprozesses, von der Analyse und Definition von Security-Anforderungen über das Produkt-Design, die Implementierung, die Verifikation und Validierung bis zur Behandlung von Security-Problemen während des gesamten Produktlebenszyklus bis zum Ende der Nutzung („End of Life“, EoL).

Weiterhin werden Anforderungen an ein Security-Management definiert, das zum einen sicherstellen soll, dass alle Aktivitäten angemessen geplant, ausgeführt und dokumentiert werden. Zum anderen muss gewährleistet werden, dass diese Aktivitäten durch angemessene organisatorische Prozesse gestützt sind und entsprechende fachkundige Verantwortlichkeiten definiert werden.

Sämtliche Prozesse und Grundsätze sollen dazu beitragen, dass Security bereits im Entwurf („Security by Design“) und mit Hilfe eines gestaffelten Sicherheitskonzeptes („Defense-in-Depth-Konzept“) umgesetzt wird.



Es reicht nicht aus, sich auf eine einmalige Absicherung der Maschine zu beschränken, der **gesamte Entwicklungsprozess und der weitere Lebenszyklus** müssen an einer hohen OT-Security orientiert sein.



Einfache Maßnahmen auf der Betreiberseite wurden bereits im Dokument **IT-Sicherheit an Werkzeugmaschinen** (→ [1]) vorgestellt.

3. Methodik zur erstmaligen Absicherung einer Maschine

Bereits von Anfang an soll ein möglichst hoher Sicherheitsstandard erreicht werden, um die Maschine möglichst robust gegenüber den zu erwartenden ständigen Veränderungen des Maschinenumfelds in ihrer Lebenszeit auszuführen. Dazu dient die im Folgenden vorgestellte Methodik, deren Schrittfolge in → Abb. 8 dargestellt ist.

1	Security-Kontext	→ Kapitel 3.1
2	Bestimmung eines Security Level Target (SL-T)	→ Kapitel 3.2
3	Architekturentwurf und Einteilung in Sicherheitszonen	→ Kapitel 3.3
4	Assets und Schutzbedarf	→ Kapitel 3.4
5	Bedrohungsanalyse und Produktisiko	→ Kapitel 3.5
6	Security-Anforderungen und -Maßnahmen	→ Kapitel 3.6
7	Restrisiko	→ Kapitel 3.7
8	Dokumentation	→ Kapitel 3.8

Abb. 8:
Überblick
eines auf IT-
Security aus-
gerichteten
Entwicklungs-
prozesses

Im vorliegenden Dokument wird diese Methodik **exemplarisch anhand einer generischen Werkzeugmaschine** durchgeführt und mit einigen ausgewählten Beispielen erläutert; die Gegebenheiten im konkreten Einzelfall können daher entsprechend abweichen.

Den Einstieg (→ Kapitel 3.1) bildet die **Betrachtung des sicherheitstechnischen Kontextes**; in diesem Zusammenhang stehen insbesondere die Schnittstellen der Maschine nach außen im Vordergrund, da diese maßgebliche Eintrittspforten für Bedrohungssituationen bilden. Im Anschluss muss ein **Ziel-Schutzniveau** in Form eines definierten „Security Level Target“ festgelegt werden (→ Kapitel 3.2). Der dritte Schritt besteht in einer eingehenderen **Betrachtung der Systemarchitektur** (→ Kapitel 3.3), wobei hier Bereiche zu Sicherheitszonen zusammengefasst und gemeinsam betrachtet werden können. Dann werden die einzelnen **Assets und ihre Schutzbedarfe analysiert** (→ Kapitel 3.4). Den Kern der Methodik bildet die sich anschließende **Bedrohungsanalyse** (→ Kapitel 3.5), verbunden mit einer Einschätzung der realen Risiken aus dem Blickwinkel der Maschinenbetreiber. Aus der Analyse werden dann **Maßnahmen** abgeleitet (→ Kapitel 3.6) und es wird das **Restrisiko** nach Umsetzung dieser Maßnahmen bewertet (→ Kapitel 3.7). Der **gesamte Prozess ist zu dokumentieren** (→ Kapitel 3.8) und ggf. zu iterieren, falls das verbleibende Risiko als zu hoch angesehen wird.

3.1 Security-Kontext

Im ersten Schritt der Methode ist der Security-Kontext festzulegen.

Den Einstieg der Betrachtung bildet eine systematische **Dokumentation des Einsatzortes und Sicherheitsumfeldes** der Maschine. Einige besonders beachtenswerte Punkte zeigt → Abb. 9.

1

Abb. 9:
Physische
und logische
Umgebung
der Maschine



Die Umgebung wird für die Analyse aus unterschiedlichen Blickwinkeln betrachtet: Einmal die physikalische Welt mit ihrer Infrastruktur, den zugangs-/zutrittsberechtigten Personen und Zugriffsmöglichkeiten auf die verschiedenen Maschinenfunktionen. Auf der anderen Seite steht eine logische Einordnung der Maschine in der „digitalen Infrastruktur“.

In diesem ersten Schritt geht es noch nicht um eine Detailanalyse sämtlicher Teilsysteme einer Maschine, sondern um eine **Einordnung der im „bestimmungsgemäßen Betrieb“ zu erwartenden Rahmenbedingungen**. Diese sind zu dokumentieren.

Eine solche Dokumentation könnte etwa die folgenden Fragestellungen beantworten:

Physische Umgebung

- *Welcher Personenkreis hat üblicherweise Zugang zur Werkzeugmaschine?*
 - *Wie sind diese qualifiziert?*
 - *Werden in diesem Personenkreis unterschiedliche Berechtigungen unterschieden?*
 - *Sind unterschiedliche Berechtigungen technisch abgesichert (z. B. mittels Kennwörtern)?*
- *Besteht eine Kontrollmöglichkeit des physischen Zugangs (z. B. über Zugangsbeschränkungen, Zeiterfassung)?*
- *Ist die Werkzeugmaschine technisch in einen Anlagenverbund eingebunden oder steht sie für sich?*
- *Beeinflusst ein Ausfall der Anlage unmittelbar Folgesysteme (z. B. verkettete Handlingsysteme) oder gibt es hier Entkopplungsstellen?*

Logische Umgebung

- *Befindet sich die Maschine in einem abgeschotteten Netzwerksegment, z. B. einem Produktionsnetz?*
- *Besteht eine gesonderte Abschottung der Werkzeugmaschine durch eine Firewall?*
- *Mit welchen Zielpunkten/-systemen kommuniziert die Maschine (etwa Produktionssysteme wie MES, Office-IT-Systeme wie ERP, Cloud-Dienste)?*
- *Mit welchen Protokollen kommuniziert die Maschine mit ihrer Außenwelt (z. B. SMB für Dateifreigaben, OPC UA für Betriebsdaten)?*

Für die weitere Betrachtung entscheidend ist an dieser Stelle, eine saubere **Abgrenzung der Werkzeugmaschine gegenüber den identifizierten externen Systemen** (physisch und logisch) vorzunehmen, um eine sinnvolle Bilanzhülle für die Analyse festzulegen. Als Anhaltspunkt kann hier gelten, dass Schnittstellen bzw. Protokollendpunkte solche Übergabestellen definieren, an denen der Betrachtungsraum der Maschine/Anlage endet.



Beispiel: Physische Umgebung

- Eine Werkzeugmaschine ist innerhalb einer Fabrikhalle frei zugänglich, zu der Halle hat aber nur ein beschränkter Personenkreis Zugang. Es kann in der weiteren Betrachtung also davon ausgegangen werden, dass der Zugang zur Anlage entsprechend reglementiert ist. Die Zugangskontrolle zur Halle selbst liegt hier klar außerhalb der Systemgrenze „Maschine“.
- Der Zugang zu bestimmten Maschinenfunktionen ist über ein Kennwort abgesichert. Die ordnungsgemäße Funktion und Reichweite dieses Kennwortschutzes in der Maschinensteuerung ist Gegenstand der Betrachtung, die organisatorische Verwaltung des Kennwortes beim Kunden liegt außerhalb und kann ggf. nur mit Empfehlungen versehen werden.

Beispiel: Logische Umgebung



- Eine Maschine kommuniziert mittels OPC UA Server mit anderen Systemen in der Fertigung, z. B. einem MES. Der in der Maschine enthaltene OPC UA Server ist Gegenstand der Betrachtung, das System welches darauf zugreift, liegt außerhalb.
- Die Maschine kommuniziert über eine Cloud-Anbindung mit einem Fernwartungssystem. Der Endpunkt in der Maschine ist Gegenstand der Betrachtung, der Cloud-Service an sich nicht.

Als Ergebnis dieses ersten methodischen Schrittes liegt ein Dokument vor, in dem im o. g. Sinne die **Rahmenbedingungen und Abgrenzungen** der Maschine aufgeführt werden.



Beispiel: Generische Werkzeugmaschine



Die in → Abb. 10 dargestellte generische Werkzeugmaschine erläutert diese verschiedenen Zugangswege detaillierter. Sie wird im Weiteren noch eingehender betrachtet.

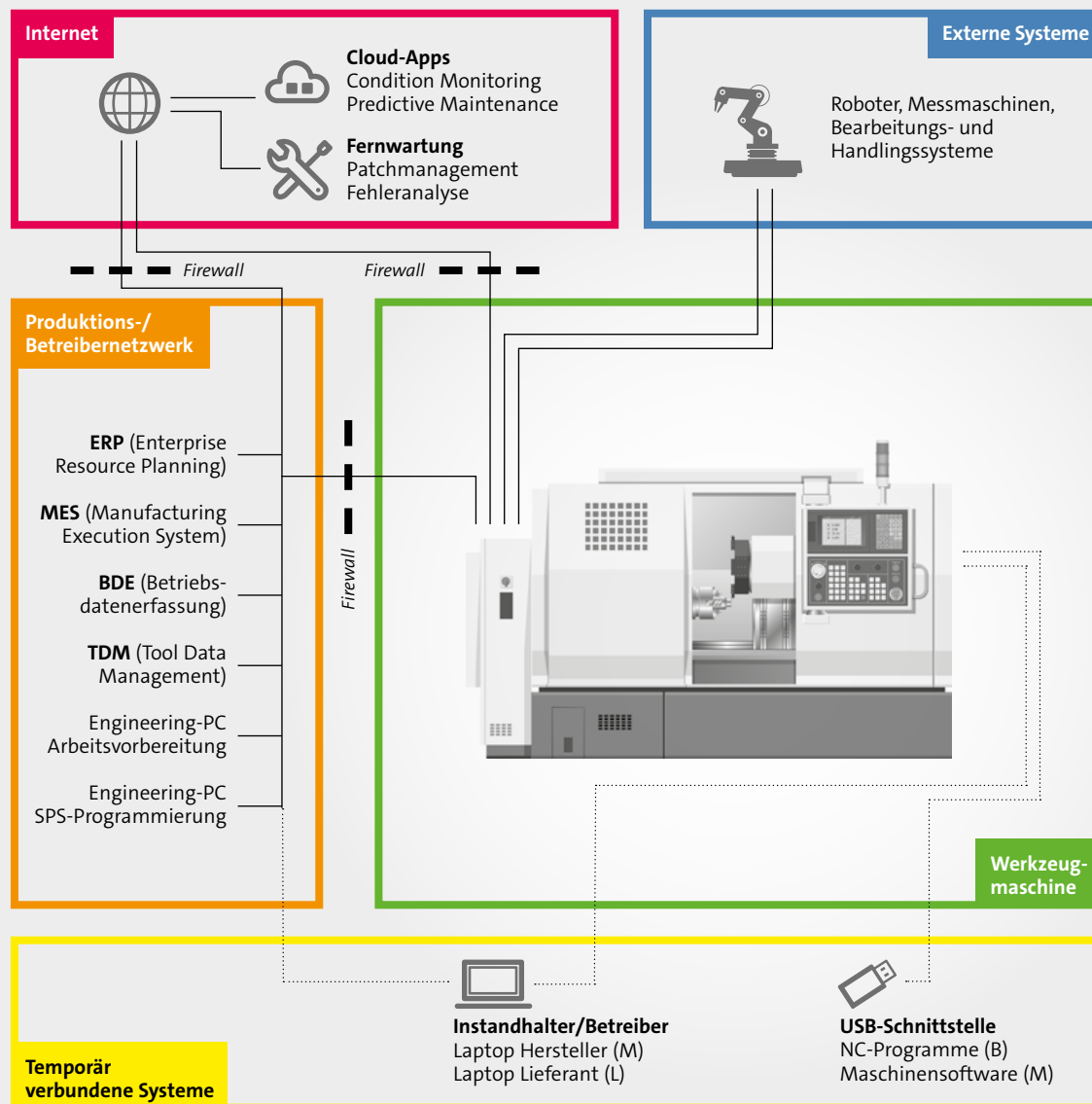


Abb. 10:
Generische
Werkzeug-
maschine

Die Beispielmachine ist per LAN an ein Firmennetz angebunden, in dem verschiedene produktionsrelevante Serverdienste zur Verfügung stehen (z. B. MES) und über welches auch die Konfiguration der NC-Steuerung/SPS erfolgen kann (Engineering-PCs). Die Werkzeugmaschine kommuniziert auch mit weiteren Maschinen (etwa im Rahmen einer Fertigungszelle oder z. B. mit Messmaschinen, Industrierobotern), entweder direkt über eine Feldbusanbindung oder ebenfalls über das Firmennetzwerk. Über einen Internetzugang erfolgt die Anbindung an Cloud-Dienste sowie Services zur Fernwartung. Weiterhin ist die lokale Bedienstelle mit verschiedenen Funktionalitäten, z. B. der Datensicherung und der Zugriffsmöglichkeit durch Service-Techniker, angedeutet. Physikalisch sind hier meist USB-Schnittstellen oder auch weitere Ethernet-Ports vorhanden.

Auch das angenommene OT-Sicherheitsumfeld wird beschrieben, welches für den bestimmungsgemäßen Betrieb vorausgesetzt wird. Dieser „Security-Kontext“ beschreibt sowohl den physikalischen als auch den logischen Einsatzort, z. B. innerhalb einer Netzwerkstruktur.

Dafür sind relevant:

- die **Netzwerkinfrastruktur** des Betreibers bzw. der Ort im Netzwerk, an dem die Anlage betrieben werden soll, z. B. ob die Maschine in einem separaten, abgesicherten Netzwerkabschnitt steht oder ob eine Verbindung zum Internet besteht
- die **physische Sicherheit**, die durch die Umgebung gegeben ist, auch Zutrittsregelungen
- mögliche **Auswirkungen auf die Umgebung**, z. B. Produktionsausfall, Umwelteinflüsse

Eine wesentliche Aufgabe der Definition des betrachteten Systems („System under Consideration“, SuC) ist die Festlegung der Komponenten, die zum Anwendungs- bzw. Verantwortungsbereich gehören. **Diese Komponenten müssen im Security-orientierten Entwicklungsprozess durch eine Bedrohungsanalyse detailliert betrachtet werden.** Der grün umrandete Bereich in → Abb. 10 zeigt den abgegrenzten Verantwortungsbereich des Herstellers (die Werkzeugmaschine). Die spätere Bedrohungsanalyse berücksichtigt Datenflüsse zu diesen Komponenten, nicht jedoch die abgegrenzten Komponenten selbst. Hier im Beispiel sind dies Serverdienste und Engineering-PCs, ebenso andere Maschinen, mit denen per M2M kommuniziert wird, und die Cloud-Anbindungen. Weiterhin ist die technische Anbindung an die verschiedenen Server, z. B. über Plug-ins wie im Falle des ERP-Systems oder über eine angebotene Application Programming Interface (API) wie bei der Betriebsdatenerfassung, vom Verantwortungsbereich abgegrenzt.

Die getroffenen **Annahmen bezüglich des Security-Kontexts**, die für den bestimmungsgemäßen Betrieb der Werkzeugmaschine vorausgesetzt werden, müssen dokumentiert werden und sind Grundlage für ein gemeinsames Verständnis der Verantwortlichkeiten von Hersteller, Integrator und Betreiber.

3.2 Bestimmung eines Security Level Target (SL-T)

2

Im zweiten Schritt der Methode ist der Security Level festzulegen.

Zur Bewertung des gewünschten/erforderlichen Security Level einer Sicherheitszone (definierter Bereich) werden in der IEC 62443-1-1 bzw. -3-3 verschiedene Ausprägungen entsprechend der folgenden Definition in → *Tabelle 1* beschrieben:

Security Level	Beschreibung	Beispiele
SL-1	• Schutz gegen ungewollten, zufälligen Missbrauch	• Ein Bediener ändert versehentlich Maschinenparameter • Ein Programmierer löscht versehentlich NC-Programme
SL-2	• Schutz gegen gewollten Missbrauch • Einfache Mittel • Niedriger Aufwand • Allgemeine Kompetenzen • Niedrige Motivation	• Der Rechner eines Instandhalters ist von einer Schadsoftware befallen, diese wird auf die Maschine übertragen • Ein Angreifer nutzt einfach zugängliche Schadsoftware, welche bekannte Sicherheitslücken in Betriebssystemen ausnutzt
SL-3	• Schutz gegen gewollten Missbrauch • Technisch ausgefeilte Mittel • Moderater Aufwand • Automatisierungsspezifische Kompetenzen • Moderate Motivation	• Gestaffelte Zugriffe: Über eine Sicherheitslücke in einem System (z. B. SPS) wird in weitere Systeme vorgedrungen, bis man im Zielsystem angekommen ist (z. B. im Unternehmens-ERP) • Erpressung von Unternehmen mittels Schadsoftware über eine gezielte Manipulation oder Beeinträchtigung der Produktion
SL-4	• Schutz gegen gewollten Missbrauch • Technisch ausgefeilte Mittel • Erheblicher Aufwand • Automatisierungsspezifische Kompetenzen • Hohe Motivation	• Geheimdienstliche Aktivitäten (wie z. B. bei „Stuxnet“ eingesetzt) • Aktivitäten der organisierten Kriminalität mit dem Ziel, bestimmte Unternehmen zu erpressen • Instrumentalisierung großer Ressourcennetzwerke (Cloud, Bot-Netze) • Maßgeschneiderte Entwicklungen für spezielle Systeme einzelner Kunden, etwa im Rüstungsbereich

Tabelle 1:
Security
Level nach
IEC 62443-
1-1/3-3

Die Security Levels werden im Zuge der Sicherheitsbewertung einzelnen Funktionen zugewiesen, wobei die IEC 62443 hier zwischen Basisanforderungen (Foundational Requirements, FR), Security-Anforderungen (Security Requirements, SR) und erweiterten Anforderungen (Requirement Enhancements, RE) differenziert.

Security Levels können einzelnen Funktionalitäten in unterschiedlicher Ausprägung zugewiesen werden. In vielen Fällen ist es zweckmäßig (oder eine Kundenvorgabe), eine **Einigung auf einen Security Level für die gesamte Anlage zu finden**, z. B. SL-2.

An dieser Stelle sei auf den vom VDMA herausgegebenen **Leitfaden IEC 62443 für den Maschinen- und Anlagenbau** (→ [3]) verwiesen, der SL-2 für die gesamte Anlage vorgibt und auf dieser Annahme die Vorgehensweise nach IEC 62443-3-3 detailliert beschreibt.



Neben ihrem Niveau (→ *Tabelle 1*) werden Security Levels in der IEC 62443 auch nach ihrer vorgesehenen Anwendung weiter spezifiziert. Es werden unterschieden:

- SL-T (Security Level Target): Ziel-Security-Levels können während des PDCA-(Plan-Do-Check-Act-)Zyklus über eine Risikobewertung ermittelt werden. Sie stellen den **zu erreichenden Security Level** dar.
- SL-C (Security Level Capability): Erreichbare Security Levels stellen den **maximalen Level** dar, der unter der Verwendung von Sicherheitsmaßnahmen erreicht werden kann.
- SL-A (Security Level Achieved): **Erreichte Security Levels** werden verwendet, um zu bewerten, ob Sicherheitsmaßnahmen ihren Zweck und damit die Vorgaben des Ziel-Security-Levels erfüllen.



Als Ergebnis des zweiten Schrittes ist nun festgelegt, welchen **Schutzbedarf** die Werkzeugmaschine erfüllen soll.



In der vorgestellten Beispielmachine aus → Abb. 10 wird im Weiteren davon ausgegangen, dass alle Anlagenteile einen gemeinsamen Security Level aufweisen sollen. Dieser Security Level wird als Zielniveau definiert (Security Level Target, SL-T).

3

3.3 Architekturentwurf und Einteilung in Sicherheitszonen

Im dritten Schritt der Methode ist die Architektur zu analysieren und in Sicherheitszonen zu unterteilen.

Wurde bislang die Werkzeugmaschine als Gesamtsystem betrachtet, so soll dieses nun für die weitere Betrachtung gemäß Normkapitel IEC 62443-3-2 in einzelne Sicherheitszonen unterteilt werden, welche ihrerseits durch Sicherheitszonenübergänge miteinander in Kontakt stehen.

Bei der Gruppierung in Sicherheitszonen und Sicherheitszonenübergänge sind folgende Aspekte zu berücksichtigen:

- Anlagensysteme (also der Werkzeugmaschine zugehörige Systeme) und Enterprise- bzw. Businesssysteme (also übergeordnete Systeme des Produktionsbetriebes) müssen auf verschiedene Sicherheitszonen aufgeteilt werden.
- Komponenten bzw. Assets, die kritisch bezüglich ihrer funktionalen Sicherheit sind (safety-critical), gehören in eigene Sicherheitszonen.
- Für Komponenten, die nur zeitweilig mit dem betrachteten System verbunden sind, sollte eine eigene Sicherheitszone eingerichtet werden.
- Für drahtlose Geräte und drahtlose Kommunikation wird eine eigene Sicherheitszone eingerichtet.
- Geräte, die über nicht vertrauenswürdige Netze zugreifen (z. B. Remote Access), gehören ebenfalls in eine eigene Sicherheitszone.



Als Ergebnis des dritten Schrittes sind ein **High-Level-Architekturbild** sowie eine **Einteilung in unterschiedliche Sicherheitszonen** anhand dieser Architektur verfügbar.

Ein High-Level-Architekturbild der in diesem Dokument gezeigten exemplarischen/generischen Werkzeugmaschine (WZM) aus → Abb. 10 bildet den Ausgangspunkt der weiteren Analyse und ist in → Abb. 11 gezeigt.

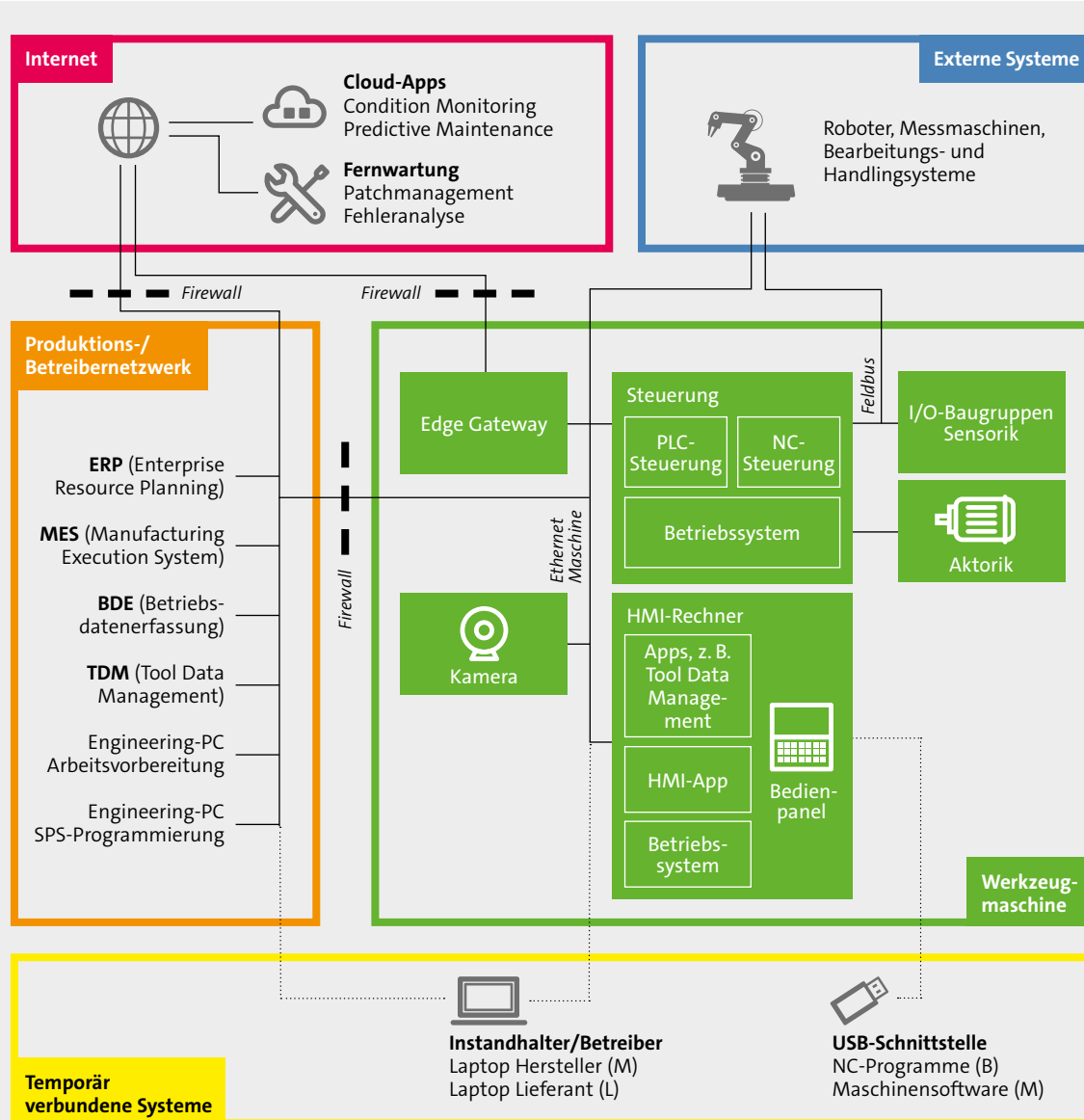


Abb. 11:
Detailbild
mit Kom-
ponenten
und Ver-
bindungen

Folgende Sicherheitszonen bzw. Sicherheitszonenübergänge werden bei der betrachteten Werkzeugmaschine unterschieden:

- die **Kern-Werkzeugmaschine mit ihren Komponenten** (grün umrandet) wie NC-Steuerung, HMI-PC und weiteren Baugruppen, welche alle auch einen Bezug zur funktionalen Sicherheit aufweisen
- das **Produktions- bzw. Betreibernetzwerk** (orange umrandet) mit allen darin verfügbaren und ggf. genutzten Services wie etwa ERP, MES, BDE etc.
- **temporär verbundene Systeme** (gelb umrandet), dazu zählen Instandhaltungsrechner und vom Bediener genutzte Geräte wie USB-Sticks für Sicherungen
- **nicht vertrauenswürdige externe Netze** (rot umrandet), z. B. Internet-Anbindungen
- **externe Systeme** (blau umrandet), z. B. Lademagazine, Handlingsysteme, Roboter, Messmaschinen

Deutlich zu erkennen ist der Aufbau aus mehreren Systemkomponenten und die verschiedenen Schnittstellen, über die diese untereinander und mit der Peripherie kommunizieren. Enthalten sind alle APIs und Plug-ins, der Zugriffspunkt der Servicetechniker des Herstellers und Integrators sowie deren Laptops, nicht jedoch des Betreibers. Zusätzlich werden die über eine Internetverbindung angebotenen Möglichkeiten zur Fernwartung und die Cloud-basierten Apps, z. B. zur vorbeugenden Wartung, sowie die lokalen Zugriffsmöglichkeiten über den USB-Schnittstelle oder die Backup-Funktionalität im Anwendungsbereich berücksichtigt.

4

3.4 Assets und Schutzbedarf

Im vierten Schritt der Methode werden die einzelnen Assets und ihr jeweiliger Schutzbedarf betrachtet.

3.4.1 Definition und Beispiele von Assets

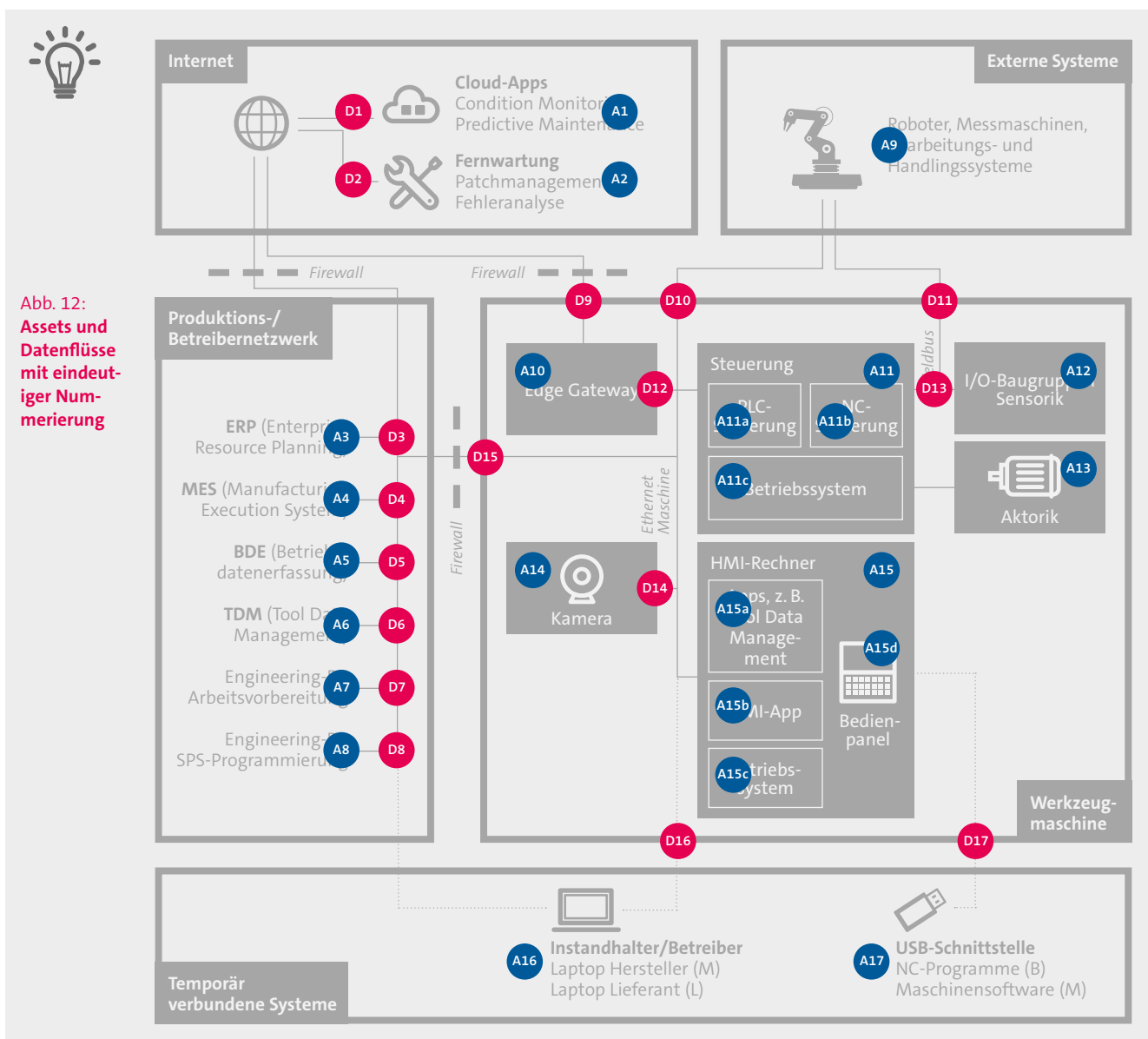
Eine nur an Sicherheitszonen orientierte Analyse ist zu grob für die Zielsetzung einer sicheren Anlage. Eine weitere Verfeinerung der Darstellung aus → Abb. 11 stellt daher die Ausweisung einzelner Assets dar.



Nach diesem Schritt sind alle **Komponenten mit einem Schutzbedarf („Assets“)** in der Werkzeugmaschine selbst und im unmittelbaren Umfeld **definiert und gekennzeichnet**.

Assets lassen sich aus dem gezeigten Entwurfsbild (→ Abb. 12) ableiten, indem jede Komponente, Verbindung und jeder Datenfluss gekennzeichnet und tabellarisch erfasst werden. Jedes Asset erhält dann eine eindeutige Nummer, um es im späteren Verlauf identifizieren zu können. Bei der Vergabe der Nummern bieten sich **Präfixe** an, um **Assets** **A** von **Datenflüssen** **D** zu unterscheiden.

Die vergebenen Nummern werden im Diagramm eingezeichnet, das Ergebnis für die vorliegende Beispiel-WZM zeigt → Abb. 12.



3.4.2 Ermittlung der Schutzbedarfe

Die auf diese Weise definierten Assets weisen eventuell unterschiedlich ausgeprägte Schutzbedarfe auf, welche einzeln bewertet werden müssen. Zu diesem Zweck wird eine Risikoanalyse für alle Assets durchgeführt. Zur Vorgehensweise orientiert man sich an der Norm ISO/IEC 27005 und legt dabei im ersten Schritt die Schutzbedarfe der Assets fest. Die Bewertung des Schutzbedarfs jedes Assets erfolgt anhand der in → *Tabelle 2* definierten drei Schutzziele:

Schutzziel	Engl. Bezeichnung	Inhaltliche Bedeutung
Vertraulichkeit	Confidentiality (C)	Vertrauliche Daten dürfen ausschließlich einem definierten Empfängerkreis (Personen oder Maschinen) zugänglich sein
Integrität	Integrity (I)	Daten dürfen nicht ohne Nachverfolgung bzw. Protokollierung verändert werden können
Verfügbarkeit	Availability (A)	Beschreibt den zeitlichen Horizont, innerhalb dessen auf die Daten zugegriffen werden muss (kurzfristig, mittelfristig, langfristig)

Tabelle 2:
Schutzziele
nach ISO/IEC
27005

Bei der Bewertung (oder Beurteilung) des Schutzziels kann z. B. eine Staffelung in drei Schutzklassen (gering, mittel, hoch) erfolgen, die die jeweilige Anforderungsstufe an den Schutzbedarf beschreibt. Ein allgemeines Klassifikationskriterium bei der Verwendung von Schutzklassen ist der (potenzielle) Schaden (z. B. finanziell oder wirtschaftlich) oder die Gefährdung, welche bei einer möglichen Verletzung eines oder mehrerer Schutzziele zu erwarten ist.

Die Gründe für die Einstufung sollten zur späteren Nachvollziehbarkeit in einem Kommentar notiert werden.

Nach diesem Schritt sind **Schutzbedarfe** in drei Kategorien (Confidentiality, Integrity, Availability) für alle Assets definiert.



Die nachfolgende Tabelle zeigt beispielhaft einige der definierten Assets und deren angenommenen Schutzbedarf:



Asset-ID	Asset	C	I	A	Kommentar/Begründung
A3	ERP-Plug-in	Hoch	Hoch	Hoch	Notwendig zur Steuerung der Produktion.
A16	Laptop Hersteller	Hoch	Hoch	Hoch	Vertraulich, da ggf. Herstellerkennwörter gespeichert sind. Je nach Dringlichkeit des Service-Einsatzes hohe Verfügbarkeit notwendig.
A1	Cloud Apps (Condition Monitoring)	Mittel	Hoch	Gering	Nur geringe Anforderungen an Verfügbarkeit, da Produktionsdaten im Edge Gateway gepuffert werden. Ggf. andere Bewertung, wenn Adaptive Control mit Cloud-Apps verwendet wird.
A10	Edge-Gateway	Mittel	Hoch	Hoch	Annahme: Produktionsrelevant, daher hohe Verfügbarkeit.
A14	Kamera	Mittel	Gering	Mittel	Zur Dokumentation des Produktionsprozesses. Annahme: Ausfall führt nicht zu unmittelbarem Produktionsausfall.
A17	USB-Schnittstelle	Mittel	Hoch	Mittel	Mittlere Vertraulichkeit, da mehrere Personen Zugriff haben. Mittlere Verfügbarkeit, da ein Zugriff nur unregelmäßig erfolgt.
A17	Schnittstelle Sicherung Maschinensoftware	Mittel	Hoch	Mittel	Backups können auch einen Tag später gemacht werden.

Tabelle 3:
Beispielhafte
Definitionen
von Schutz-
bedarfen
für Assets

Die Betrachtung erfolgt jeweils in allen drei Schutzzielen (Confidentiality, Integrity, Availability), in den Kommentaren sind Hinweise zur Begründung einzelner Eigenschaften aufgeführt.

5

3.5 Bedrohungsanalyse und Produktrisiko

Im fünften Schritt der Methode werden Bedrohung und Risiko für die Assets bewertet.

3.5.1 Allgemeine Beschreibung der Bedrohungsanalyse

Die Bedrohungsanalyse ist ein Werkzeug, um systematisch einen Überblick über alle Bedrohungen (entsprechend der Definition aus [Abschnitt 2.1.2](#)) zu erhalten, die auf ein System wirken. Zur Durchführung gibt es verschiedene Verfahren. Eine geeignete Methodik sollte allgemein die folgenden Kriterien erfüllen:

- **Vollständigkeit:** Gewissheit, dass alle Bedrohungen gefunden werden.
- **Wiederholbarkeit:** Eine später durchgeführte Bedrohungsanalyse muss zum selben Ergebnis kommen. Das Gleiche gilt, wenn die zweite Analyse durch ein anderes Team durchgeführt wird.
- **Wirtschaftlichkeit:** In der Praxis ist es nicht möglich, beliebig hohen Aufwand in Bedrohungsanalyse zu investieren. Die methodische Vorgehensweise muss daher auch einen Rahmen festlegen, um die Ziele der Vollständigkeit und Wiederholbarkeit in angemessener Zeit zu erreichen.

Ein Verfahren, das die genannten Kriterien erfüllt, ist die von Microsoft entwickelte **S.T.R.I.D.E.-Methodik**, welche in [Abschnitt 3.5.2](#) beschrieben wird.



Im ersten Teil des fünften Schrittes sind die vormals definierten Assets auf ihre Anfälligkeit hinsichtlich verschiedenster Kriterien hin untersucht.

3.5.2 Die S.T.R.I.D.E.-Methodik

Der Name „S.T.R.I.D.E.“ stellt eine Abkürzung der darin berücksichtigten Bedrohungskategorien dar. Die Methodik basiert darauf, dass sich jede Bedrohung einer der folgenden Kategorien zuordnen lässt:

- **Spoofing**
Bezeichnet die unbefugte Verwendung der Identität von Benutzern oder Prozessen. Das einfachste Beispiel für Spoofing ist die unbefugte Verwendung der Anmeldeinformationen (z. B. Benutzername und Passwort) von anderen Benutzern.
- **Tampering**
Bezeichnet unbefugtes Verändern, Manipulieren oder Löschen von Ressourcen und Daten. Dazu zählt beispielsweise die Manipulation übertragener Daten über das Internet oder unzulässiges Verändern oder Löschen gespeicherter Daten, z. B. in einer Datenbank.
- **Repudiation**
Bedrohung aufgrund fehlender Nachweisbarkeit von Handlungen oder Manipulationen. Handlungen oder Manipulationen können keinem Nutzer eindeutig nachgewiesen werden bzw. alle Nutzer können einen entsprechenden Zugriff bestreiten. Ein Beispiel wäre, wenn mehrere Benutzer Zugriff auf einen gemeinsamen Account (z. B. „admin“) haben, so dass eine einzelne Handlung nicht einem einzelnen Nutzer zugeordnet werden kann.
- **Information Disclosure**
Die Offenlegung vertraulicher Informationen: Entwenden oder Abrufen von Informationen, die als vertraulich angesehen werden.
- **Denial of Service (DoS)**
Die Verfügbarkeit oder Zuverlässigkeit einer Anwendung wird dauerhaft oder zeitlich befristet so beeinflusst, dass die reguläre Nutzung nicht mehr möglich ist. Beispiele umfassen etwa die Nichterreichbarkeit von Webservern oder Datenbanken, oft hervorgerufen durch zu viele gleichzeitige Zugriffe und damit einhergehende Überlastung der Rechner.
- **Elevation of Privilege**
Ein nicht privilegierter Benutzer mit eingeschränkten Rechten verschafft sich höhere Zugriffsrechte und kann so weitere Systemkomponenten kompromittieren, ggf. sogar administrative Zugriffsrechte erlangen.

Eine S.T.R.I.D.E.-Analyse wird nun dergestalt durchgeführt, dass systematisch **verschiedene Angriffsszenarien aus allen Kategorien auf die zuvor definierten Assets angewendet** werden, zumindest dort, wo dies möglich ist. Anders ausgedrückt erfolgt also eine vollfaktorielle Applikation der Angriffsmethoden auf die Assets; siehe zur Erklärung auch die in → *Abb. 13* dargestellte Schematik.

Angriffsvarianten	Assets				
	Asset 1	Asset 2	Asset 3	...	Asset n
Spoofing – Variante 1					...
Spoofing – Variante 2			Nicht anwendbar	Nicht anwendbar	...
...	Nicht anwendbar				...
Spoofing – Variante n					...
Tampering – Variante 1		Nicht anwendbar			...
Tampering – Variante 2					...
...	...	...	...	...	...

Abb. 13:
Schematische
Darstellung
der
S.T.R.I.D.E.-
Methodik



Nahezu jeder denkbare Angriff kann einer der genannten Kategorien zugeordnet werden, bei entsprechenden Vielzahl von Angriffsvarianten kann so eine sehr vollständige Sicherheitsanalyse erfolgen. Das Ziel der S.T.R.I.D.E.-Analyse ist es damit, einen möglichst vollständigen Überblick der Bedrohungssituation zu erlangen.

Als Ergebnis einer S.T.R.I.D.E.-Analyse können sich für die gezeigte Muster-WZM u.a. folgende Schlussfolgerungen ergeben (nur einige ausgewählte Beispiele):



Asset	Kategorie	Analyseergebnis
A10, A11, A15 (Edge Gateway, Steuerung, HMI-Rechner)	Information Disclosure	Es wird ein nicht-kundenspezifisches Masterpasswort für eine Produktserie verwendet. Diese Masterpasswörter werden veröffentlicht z. B. über Webseiten wie Shodan. Jeder, der in Kenntnis dieser Masterpasswörter kommt und der vor Ort ist, kann dadurch Zugriff auf die Maschine erlangen.
A16 (Laptop Lieferant)	Spoofing Tampering Repudiation	Häufig verwalten Servicetechniker die Zugangsdaten in einer ungesicherten Datei (z. B. Excel). Wird der Laptop des Technikers gestohlen oder werden die Zugangsdaten ausgespäht, kann der Zugriff auf alle Maschinendaten ggf. sogar über Fernwartungszugänge erfolgen.
A11b (NC-Steuerung)	Tampering Repudiation	Aufgrund schwacher oder fehlender Autorisierung besteht die Möglichkeit einer nicht offensichtlichen (nicht sofort auffälligen) Manipulation von Maschinendaten und Werkzeugparametern (z. B. Schnittgeschwindigkeit, Toleranzverschiebungen). Dies kann zu Werkstückausschuss bis hin zur Beschädigung der Maschine führen. Aufgrund fehlender Nachvollziehbarkeit kann dies auch zu Problemen mit der Gewährleistung führen.
A11c, A15c (Betriebssystem)	Denial of Service	Angriffe auf neu entdeckte, nicht gepatchte Sicherheitslücken im Betriebssystem; z. B. Verschlüsselungstrojaner können zur dauerhaften Beeinträchtigung der Verfügbarkeit der Maschine führen.

3.5.3 Bewertung von Bedrohungen

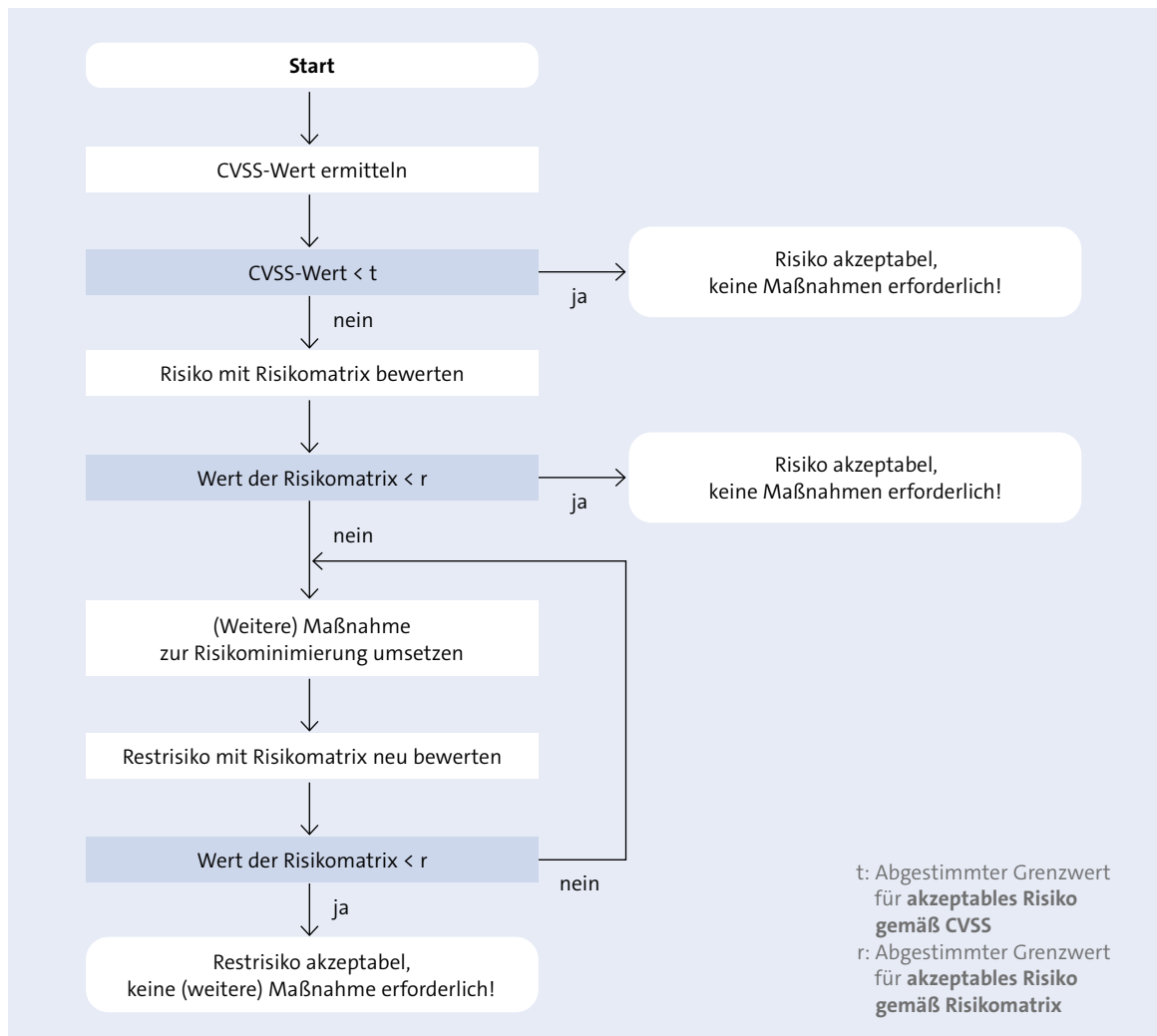
Eine anschließende Bewertung dieser Bedrohungen (z. B. nach einem anerkannten Scoring-Verfahren und anhand der Risiken) erlaubt es dann, wirklich **relevante Bedrohungen** zu identifizieren.

Zur Methodik werden hier zwei Verfahren vorgestellt:

- die Bewertung nach Common Vulnerability Scoring System (CVSS) (→ *Abschnitt 3.5.4*) sowie
- die Anwendung einer Risikomatrix (→ *Abschnitt 3.5.5*).

Beide Verfahren stehen grundsätzlich gleichberechtigt nebeneinander. Sie unterscheiden sich zwar in der Vorgehensweise, lassen sich aber in günstiger Weise kombinieren – eine empfohlene Arbeitsweise zur Kombination beider Methoden ist in → *Abb. 14* gezeigt.

Abb. 14:
Ablauf-
diagramm zur
Bewertung
von Be-
drohungen



Der dargestellte Ablauf kombiniert die CVSS-Methode in der Weise mit der Risikomatrix, dass zunächst anhand von CVSS eine Vorbewertung der Risiken erfolgt. Ein Vorteil von CVSS liegt hier in einer weitgehenden Objektivierung der Kriterien. Im nächsten Schritt erfolgt dann zur Kontrolle eine Bewertung anhand einer Risikomatrix, so dass nun mit zwei etablierten Bewertungsverfahren eine Bewertung durchgeführt und dokumentiert worden ist. Nach den definierten Maßnahmen zur Senkung der Risiken erfolgt dann (ggf. iterativ) eine Neubewertung anhand der Risikomatrix.

Die genannte Vorgehensweise stellt keine Verpflichtung, sondern lediglich eine Empfehlung dar – es müssen auch nicht zwangsläufig beide Verfahren eingesetzt werden. Grundsätzlich muss eine entsprechende Bewertung vor allem gut nachvollziehbar sein.

Aus Sicht des zeitlichen Ablaufs ist dringend zu empfehlen, die Bedrohungsanalyse und Risikobewertung zu Beginn der Produktentwicklung durchzuführen. Nur dann besteht die Chance, Bedrohungen beim Ent-

wurf zu berücksichtigen. Oft genügen kleine Änderungen an der Architektur, die zudem in dieser frühen Planungsphase noch relativ einfach möglich sind, um „Security by Design“ und eine gestaffelte Sicherheitsarchitektur zu realisieren. Die Bedrohungsanalyse muss aktualisiert werden, wenn sich Änderungen an der Architektur ergeben. Die Behandlung von Bedrohungen, die erst später erkannt werden, z. B. während der Implementierung, ist oft deutlich aufwändiger. Dies liegt daran, dass ggf. zusätzliche Funktionalität integriert werden muss, um Sicherheitslücken der Architektur auszugleichen. In einigen Fällen sind aber keine Ausgleichsmaßnahmen möglich.

Sollten während der Implementierung noch Änderungen an der Architektur notwendig sein, muss die Bedrohungsanalyse ebenfalls aktualisiert werden. Einige Bedrohungen lassen sich nur durch Ausgleichsmaßnahmen des Betreibers behandeln. In manchen Fällen kann es auch sein, dass keine geeignete Maßnahme existiert oder diese so aufwändig ist, dass die effizienteste Behandlung im Tragen des Risikos besteht. Sowohl die Maßnahmen für den Betreiber als auch die unvermeidlichen Risiken müssen dokumentiert und mit den Integratoren und Betreibern abgestimmt werden.

Im zweiten Teil des fünften Schrittes wurden die vormals definierten Assets einer Risikoeinschätzung mittels CVSS und/oder Risikomatrix unterzogen.



3.5.4 Das CVSS-Bewertungssystem

CVSS steht für „Common Vulnerability Scoring System“ und bezeichnet einen Industriestandard zur Bewertung des Schweregrades von möglichen oder tatsächlichen Sicherheitslücken in IT-Systemen.

Eine detaillierte Einführung zum Thema CVSS liefert etwa → [4]. Allgemein gesprochen stellt CVSS eine Methodik bereit, anhand derer die Gefahr, die von einer Sicherheitslücke ausgeht, quantifiziert werden kann. Für die praktische Umsetzung gibt es als Hilfestellung entsprechende Online-Tools (Rechner) (→ [5]).

Abb. 15:
Online-Rechner für einen CVSS-Score
Quelle: → [5]

Bewertet wird anhand mehrerer Kriterien, welche dann in ihrer Gesamtheit in einen CVSS-Score einfließen. Die Kriterien umfassen (vgl. → Abb. 15):

- den Angriffsvektor (Attack Vector, AV) – z. B. über das Netzwerk oder physisch (= vor Ort)
- die Komplexität des Angriffs (Attack Complexity, AC)
- ob für den Angriff besondere Rechte erforderlich sind (Privileges Required, PR)
- ob eine Benutzerinteraktion erforderlich ist (User Interaction, UI), z. B. das Ausführen eines Mailanhangs
- das Zielobjekt (Scope, S): Hier wird unterschieden, ob das Angriffsziel gleichzeitig auch das Einfallstor ist („unchanged“) oder ob von dort weitergesprungen wird („changed“). Ein solches „changed“-Szenario wäre z. B. ein Angriff auf Rechner A, um über das Netz an Rechner B zu kommen.
- die bereits in → Abschnitt 3.4.2 definierten Anforderungen:
 - Vertraulichkeit (Confidentiality, C)
 - Integrität (Integrity, I)
 - Verfügbarkeit (Availability, A)

Aus den Angaben zu entsprechenden Einschätzungen resultiert dann der CVSS-Score. So können potenzielle Sicherheitslücken nach verschiedenen Kriterien, sogenannten Metriken, bewertet und miteinander verglichen werden, so dass eine Prioritätenliste für Gegenmaßnahmen erstellt werden kann.

3.5.5 Risikomatrix nach IEC 62443-3-2

Ergänzend zu einer Bewertung nach CVSS wird hier eine Risikomatrix eingesetzt. Die Quantifizierung der Risiken erfolgt über die Beziehung zwischen Eintrittswahrscheinlichkeit, möglichem Schaden und Risiko – in Abhängigkeit von Eintrittswahrscheinlichkeit und Schaden ergibt sich ein Punktwert, welcher das Ausmaß des Risikos abbildet. In → Abb. 16 ist ein Beispiel einer Risikomatrix abgebildet, wie diese im Normenteil IEC 62443-3-2 abgebildet ist. In der Praxis kann die Organisation das Beispiel durch eine eigene Risikomatrix ersetzen.

Abb. 16:
Risikomatrix
nach IEC
62443-3-2

Schaden		Eintrittswahrscheinlichkeit				
		Vernachlässigbar 1	Unwahrscheinlich 2	Möglich 3	Wahrscheinlich 4	Sicher 5
Sehr niedrig	1	1	2	3	4	5
Niedrig	2	2	4	6	8	10
Mittel	3	3	6	9	12	15
Hoch	4	4	8	12	16	20
Kritisch	5	5	10	15	20	25

3.5.6 Exemplarische Bedrohungsanalyse

Es folgt ein zusammengefasstes Beispiel für eine vollständige Bedrohungsanalyse.

Die Bedrohungen werden anhand des Schweregrads und des Risikos beurteilt. Hierzu werden das Bewertungssystem für Sicherheitslücken nach CVSS (→ *Abschnitt 3.5.4*) sowie die Risikomatrix (→ *Abschnitt 3.5.5*) angewendet.

Eine beispielhafte Analyse der USB-Schnittstelle mittels CVSS zeigt → *Abb. 17*, eine Anwendung der Risikomatrix darauf → *Abb. 18*.



Base Score **6.6** (Medium)

Attack Vector (AV)
 Network (N) Adjacent (A) **Local (L)** Physical (P)

Attack Complexity (AC)
Low (L) High (H)

Privileges Required (PR)
None (N) Low (L) High (H)

User Interaction (UI)
 None (N) **Required (R)**

Scope (S)
Unchanged (U) Changed (C)

Confidentiality (C)
 None (N) **Low (L)** High (H)

Integrity (I)
 None (N) Low (L) **High (H)**

Availability (A)
 None (N) **Low (L)** High (H)

Abb. 17:
Online-Tool
zur Bewertung
mittels
CVSS am
Beispiel USB-
Schnittstelle

Schaden		Eintrittswahrscheinlichkeit				
		Vernachlässigbar 1	Unwahrscheinlich 2	Möglich 3	Wahrscheinlich 4	Sicher 5
Sehr niedrig	1	1	2	3	4	5
Niedrig	2	2	4	6	8	10
Mittel	3	3	6	9	12	15
Hoch	4	4	8	12	16	20
Kritisch	5	5	10	15	20	25

Abb. 18:
Risikobewer-
tung eines
Angriffs über
die USB-
Schnittstelle

Asset	Kategorie	Beschreibung
A17 (USB-Schnittstelle)	Information Disclosure	Über die USB-Schnittstelle können die gesamten Produktionsdaten und NC-Programme abgezogen und unberechtigten Dritten zugänglich gemacht werden. Dies kann zu Verlust von Know-how und Verletzung des geistigen Eigentums des Betreibers führen.

Bewertung der Bedrohungen			
CVSS-Score	Risiko-Eintrittswahrscheinlichkeit	Schaden	Risikowert laut Risikomatrix
6,6	Wahrscheinlich	Hoch	16 → Risiko nicht akzeptabel, Maßnahmen wie im Folgekapitel beschrieben müssen ergriffen werden

Tabelle 4:
Zusammen-
fassung der
Bewertung
der USB-
Schnittstelle

6

3.6 Security-Anforderungen und -Maßnahmen

Im sechsten Schritt der Methode sind die Security-Anforderungen mit entsprechenden Maßnahmen zu belegen.

Für die unterschiedlichen Security Levels (SL-C 1 bis 4) sind in den Normenteilen 3-3 und 4-2 **Anforderungen** an Fähigkeiten für Systeme (3-3) bzw. Komponenten (4-2) hinterlegt. In den Normen sind diese Anforderungen hierarchisch aufgebaut: Unterschieden werden grundlegende Anforderungen (Foundational Requirements, FR), Systemanforderungen (System Requirements, SR) und darin enthaltene weitergehende Anforderungen (Requirement Enhancement, RE) (→ Abb. 19).

Abb. 19:
Hierarchie
der Anforderun-
gen in IEC
62443-3-3



Die jeweiligen Anforderungen unterscheiden nach angestrebtem Security Level. Dieser wurde im zweiten Schritt (→ Kapitel 3.2) definiert, entweder für die gesamte Anlage oder auf Asset-Basis.



Nach dem sechsten Schritt sind für die betrachteten Assets zum jeweils erforderlichen Security Level passende Maßnahmen zur Reduktion der Gefährdung aufgeführt.

In der Norm sind zwar keine konkreten Maßnahmen im Detail vorgegeben, aus den gegebenen Anforderungen lassen sich aber zum Teil Maßnahmen zur Bedrohungsabschwächung ableiten.

Beispielhaft sei hier die in der IEC 62443-3-3, Kapitel 5.3.1 definierte Anforderung zitiert. Eingearbeitet in die grundlegende Anforderung FR 1 („Identifizierung und Authentifizierung“), Unterkategorie SR 1 („Identifizierung und Authentifizierung von menschlichen Nutzern“), wird hier gefordert:

„Das Automatisierungssystem muss die Fähigkeit bieten, alle menschlichen Nutzer zu identifizieren und zu authentifizieren. Diese Fähigkeit muss an allen Schnittstellen, die menschlichen Nutzern Zugang zum Automatisierungssystem gewähren, die Identifizierung und Authentifizierung durchsetzen, so dass die Trennung von Aufgaben und das Prinzip der minimal erforderlichen Rechte entsprechend den anzuwendenden IT-Sicherheitsleitlinien und -Vorgehensweisen unterstützt wird.“

Dazu ist im Folgeabschnitt 5.3.2 eine Begründung angegeben:

„Alle menschlichen Nutzer müssen für alle Arten eines Zugriffs auf das Automatisierungssystem identifiziert und authentifiziert werden. Die Authentifizierung der Identität dieser Nutzer sollte durch die Verwendung solcher Methoden wie z. B. Passwörter, Token, biometrische Merkmale oder, bei Multifaktor-Authentifizierung, eine Kombination dieser Methoden erfolgen [...]“

Es ist ersichtlich, dass aus diesen Ausführungen direkt einige Maßnahmen abgeleitet werden können (Passwörter, Token, biometrische Merkmale ...). **Dieser Schritt muss immer mit Blick auf die eigene Anlage**

erfolgen – industrielle Automatisierungssysteme und Maschinen sind so unterschiedlich, dass hier keine allgemein gültigen Ratschläge gegeben werden können. Die Norm bietet aber eine Vielzahl von Anregungen, die aufgegriffen werden können.

Bezogen auf die im vorausgehenden Beispiel genannte USB-Schnittstelle könnten etwa folgende Maßnahmen vorgeschlagen werden:

- Nutzung der USB-Schnittstelle darf erst nach Benutzeranmeldung mit Passwort möglich sein (eindeutige Authentifizierung).
- Ereignisprotokollierung beim Export von Daten, um die Nutzung des USB-Ports nachvollziehen zu können.
- Je nach Kritikalität: Erzwingen von Verschlüsselung auf externen Medien.

3.7 Restrisiko

Im siebten Schritt der Methode ist das Restrisiko nach Umsetzung der definierten Maßnahmen zu bewerten.

Durch die Umsetzung von Maßnahmen ändert sich die Eintrittswahrscheinlichkeit und/oder das Schadenspotenzial von Bedrohungen. Ziel einer erneuten Risikobewertung ist es nun, das **nach Umsetzung** der vorgeschlagenen Maßnahmen verbleibende Restrisiko (Netto-Risiko) zu ermitteln.

Nach dem siebten Schritt sind für die bewerteten Assets die nach Umsetzung von Abhilfemaßnahmen noch verbleibenden Risiken quantifiziert.



Wie man anhand des gewählten Beispiels „USB-Schnittstelle“ erkennen kann, verbleiben immer Restrisiken, die durch den Hersteller nicht vollständig beseitigt werden können. Um diese Risiken weiter zu reduzieren, müssen etwa vom Betreiber weitere Ausgleichsmaßnahmen umgesetzt werden, oder das Risiko muss akzeptiert werden. Die transparente Kommunikation der Ergebnisse an den Betreiber ist daher zwingend notwendig, um diese Akzeptanz (oder auch entsprechende weitere Maßnahmen) zu erreichen.



Tabelle 5:
Zusammenfassung der Bewertung der USB-Schnittstelle nach Ergreifen von Maßnahmen

Asset	Kategorie	Beschreibung	
A17 (USB-Schnittstelle)	Information Disclosure	Über die USB-Schnittstelle können die gesamten Produktionsdaten und NC-Programme abgezogen und unberechtigten Dritten zugänglich gemacht werden. Dies kann zu Verlust von Know-how und Verletzung des geistigen Eigentums des Betreibers führen.	

Bewertung der Bedrohungen			
CVSS-Score	Risiko-Eintrittswahrscheinlichkeit	Schaden	Risikowert laut Risikomatrix
6,6	Wahrscheinlich	Hoch	16

Maßnahmen			
• Nutzung der USB-Schnittstelle darf erst nach Benutzeranmeldung mit Passwort möglich sein (eindeutige Authentifizierung). • Ereignisprotokollierung beim Export von Daten, um die Nutzung des USB-Ports nachvollziehen zu können. • Je nach Kritikalität: Erzwingen von Verschlüsselung auf externen Medien.			

Erneute Bewertung mit Risikomatrix nach Umsetzung der Maßnahmen			
	Risiko-Eintrittswahrscheinlichkeit	Schaden	Risikowert laut Risikomatrix
	Unwahrscheinlich	Hoch	8

8

3.8 Dokumentation

Im achten Schritt der Methode sind die ausgeführten Schritte und deren Ergebnisse zu dokumentieren.

Sämtliche durchgeführten Schritte sollten nachvollziehbar dokumentiert werden. Eine entsprechende Dokumentation erleichtert auch dem Kunden gegenüber die Argumentation und dient als Nachweis einer sicheren Entwicklungsmethodik.

Einen wesentlichen Teil der Dokumentation stellen dabei die erstellten Tabellen der verschiedenen Assets mit deren Schutzbedarfen/Maßnahmen etc. dar.

Grundsätzlich sollte die Dokumentation den Anspruch erfüllen, die durchgeführte Absicherung des Entwicklungsprozesses nachvollziehbar und transparent zu machen, indem z. B. auch Begründungen für Festlegungen aufgeführt werden.



Nach dem achten Schritt sind die Schritte 1 bis 7 zusammengefasst und dokumentiert, idealerweise auch von einer nicht mit der Analyse befassten Person gegengeprüft.

4. Betrachtungen über die gesamte Nutzungsdauer

4.1 Grundsätzliches

In den Ausführungen zur Schutzstrategie aus → *Kapitel 2.3* wurde bereits deutlich, dass mit einem auf hohe OT-Security hin ausgerichteten Entwicklungsprozess allein noch kein ausreichendes Schutzniveau erzielt werden kann, insbesondere nicht auf Dauer. Es bedarf daher zusätzlicher begleitender Maßnahmen für die oftmals jahrzehntelange Betriebsphase. Diese umfassen kundenseitige Handlungen, können aber auch durch den Hersteller der Werkzeugmaschine vorbereitet und unterstützt werden. Vorschläge für die Kundenseite finden sich bereits in → [1], das vorliegende Dokument widmet sich daher vorrangig den Möglichkeiten und ggf. sogar Verpflichtungen des Werkzeugmaschinenherstellers.

Die Gründe für die Notwendigkeit von Schutzmaßnahmen zur Betriebszeit sind vielschichtig, insbesondere vier Ursachen sollen hier herausgestellt werden:

1. Unterschiedliche Produktlebenszyklen

IT-Systeme und damit auch die dazugehörigen Umgebungen und Sicherheitstechnologien sind im Vergleich zu Werkzeugmaschinen deutlich kürzeren Produktlebenszyklen unterworfen. Mit hoher Wahrscheinlichkeit ergeben sich also wesentliche Erkenntnisse zu (ggf. auch bereits länger bestehenden) Sicherheitslücken und auch technologische Weiterentwicklungen während der Betriebszeit der Maschine, auf die reagiert werden muss.

2. Große Variantenvielfalt

Eine Werkzeugmaschine stellt ein komplexes und vielfach für den Kunden maßgeschneidertes System dar, welches aus einer Vielzahl von Zulieferkomponenten und unterschiedlichen Einheiten aufgebaut ist. Jede maßgebliche Veränderung einer dieser Komponenten, z. B. durch Software-Patches bedarf einer erneuten Absicherung der Funktion des Gesamtsystems, welche durch den Hersteller nicht ohne weiteres leistbar ist.

3. Architektur von IT-Komponenten

Allgemein bestehen digitale Produkte heutzutage nicht mehr nur aus selbstentwickelten Komponenten, sondern es wird eine Vielzahl an Fremdkomponenten in der Form von Bibliotheken, Frameworks und Betriebssystemen mit den Produkten ausgeliefert. Diese Komponenten binden ihrerseits weitere Komponenten ein. In jeder dieser (auch transitiv) eingebundenen Abhängigkeiten können Sicherheitslücken enthalten sein, die Auswirkungen auf die Sicherheit unserer Produkte haben können (z. B. „Log4j“).

4. Betriebliche und funktionale Gründe

Bestimmte Maßnahmen, welche aus einer isolierten IT-Sicherheitsperspektive hilfreich oder sogar notwendig erscheinen, lassen sich für Werkzeugmaschinen im betrieblichen Alltag nur unkomfortabel oder schlicht gar nicht umsetzen. Ein Beispiel wären die (auch arbeitsrechtlich relevanten) Anforderungen im Bereich des Datenschutzes, welche einer Speicherung personenbezogener Zugriffsdaten im Wege stehen – die aber aus reinen Sicherheitserwägungen heraus wünschenswert wäre. Es müssen daher andere Wege gefunden werden, die entsprechenden Systeme abzusichern.

4.2 Maßnahmen und Herangehensweise

Es liegt mit in der Verantwortung des Werkzeugmaschinenherstellers, die Aufrechterhaltung eines hohen Grades an Security auch nach Auslieferung zu ermöglichen. Daher müssen mindestens bis zum Ende des zugesicherten Supportzeitraums (End of Service) entsprechende Prozesse etabliert werden, die die Behandlung von Sicherheitslücken und die Bereitstellung von Sicherheitsupdates ermöglichen.

4.2.1 Management von Sicherheitslücken

Sicherheitslückenmanagement bedeutet, einen geregelten Prozess zum Umgang mit möglichen Sicherheitslücken in Produkten zu betreiben. Aus der Perspektive eines Maschinenbauunternehmens besteht es daher im Wesentlichen darin, **Sicherheitslücken in den eingebetteten Komponenten** zu identifizieren, diese zu dokumentieren und deren Auswirkungen auf das Produkt zu behandeln.

Dazu ist es notwendig, ein Verzeichnis aller eingebetteten Bibliotheken, Komponenten, Betriebssysteme etc. und deren Versionsstände zu erstellen und aktuell zu halten (Software-Inventar, Komponentenregister). Für jede dieser Komponenten muss dann eine Strategie festgelegt werden, wie man von Sicherheitslücken Kenntnis erlangt.

- Im Falle **eigenentwickelter Software** kann diese Aufgabe ggf. durch die eigenen Entwickler abgedeckt werden – zumindest auf oberer Ebene sind diesen die eingesetzten Software-Komponenten ja bekannt bzw. wurden von diesen ausgewählt. Wichtig ist hier aber auch ein Blick auf weitere unterlagerte Abhängigkeiten – diese sollten ebenfalls untersucht und dokumentiert werden und können ggf. auch ausschlaggebend für oder wider den Einsatz einer bestimmten Komponente sein.
- Für **zulieferte Systeme** müssen entsprechende Regelungen mit den Lieferanten gefunden werden. Diese sollten (ggf. durch entsprechende Vertragswerke) aufgefordert werden, Teilkomponenten zu benennen und den Maschinenbauer über Sicherheitslücken in der eigenen oder verbundenen Software zu informieren.

Es empfiehlt sich die Etablierung eines PDCA-(Plan-Do-Check-Act-)Prozesses mit fortschreitend iterierter Risikobewertung in festen Zeitabständen (z. B. einmal jährlich aktualisierte Einschätzung). Zusätzlich sollte infolge von Ereignissen wie dem Bekanntwerden großer Sicherheitslücken oder größerer Wechsel der eingesetzten Software-Komponenten, z. B. Betriebssystemupdates (etwa Windows 10 statt Windows 7, Linux statt Windows ...), eine entsprechende Neubewertung stattfinden.

4.2.2 Umgang mit Sicherheitsupdates

Wenn Sicherheitslücken, die die eingesetzte Software betreffen, identifiziert werden, muss der Maschinenhersteller in der Lage sein, Sicherheitsupdates rechtzeitig in geeigneter Weise zur Verfügung zu stellen und bekanntzugeben.

Im Sinne des Maschinenbetreibers muss dabei aber sichergestellt sein, dass Patches den ordnungsgemäßen Betrieb des Produktes nicht beeinträchtigen. Dies lässt sich häufig nur durch vorherige Tests, etwa Regressionstests, sicherstellen. Weiterhin ist es aufgrund der komplexen Struktur der aufeinander abgestimmten Komponenten einer Werkzeugmaschine möglich und auch wahrscheinlich, dass der Betreiber eine entsprechende Hochrüstung nicht eigenständig, sondern nur mit Hilfe des Werkzeugmaschinenherstellers oder ggf. sogar nur mit Unterstützung des Steuerungsherstellers angehen kann.

Den Betreibern muss im Rahmen von Sicherheitsupdates auch entsprechende Dokumentation zur Verfügung gestellt werden. Diese muss folgende Informationen beinhalten:

- die betroffene Software und die Version, für die das Update gilt
- eine Installationsanleitung und eine Beschreibung der Auswirkungen, die die Installation hat, z. B. geändertes Verhalten oder die Notwendigkeit eines Neustarts
- Prüfmöglichkeiten, die es dem Betreiber erlauben, die Integrität des Updates sicherzustellen und die erfolgreiche Installation zu überprüfen
- eine Beschreibung möglicher Risiken, die entstehen, wenn das Update nicht installiert wird

Oft ist es notwendig, dass Patches für abhängige Komponenten oder Betriebssysteme zur Verfügung gestellt oder deren Installation empfohlen werden muss. In diesem Fall müssen dem Betreiber folgende Informationen zur Verfügung gestellt werden:

- ob die Software mit dem Sicherheits-Update für die abhängige Komponente oder das Betriebssystem kompatibel ist.
- empfohlene Abschwächungsmaßnahmen für den Fall, dass das Update vom Hersteller nicht zur Anwendung freigegeben ist

Sollte eine Security-getriebene Hochrüstung von Werkzeugmaschinen gemäß den zuvor genannten Kriterien nicht möglich, extrem aufwändig oder auch aus Gründen einer maximalen Verfügbarkeit nicht gewollt sein, so können alternativ die im folgenden → *Kapitel 5* empfohlenen Methoden für das „brown field“ dabei helfen, einen höheren Sicherheitsstandard zu erreichen.

4.3 Unterstützung durch Systemlieferanten

4.3.1 Rolle der Systemlieferanten

Aus der Perspektive OT-Security stellt für den Werkzeugmaschinenbauer der Hersteller des Steuerungssystems den wichtigsten Partner dar, auch nach Auslieferung der Maschine. Hierzu muss angemerkt werden, dass die Hersteller und Lieferanten von Steuerungssystemen für Werkzeugmaschinen sich neben ihrer Rolle als Software- und Hardware-Hersteller ebenfalls in der Rolle eines Systemintegrators wiederfinden: In modernen Steuerungssystemen werden vielfach „zugelieferte“ Software-Komponenten eingesetzt, für die ein entsprechendes Monitoring im Sinne von → *Kapitel 4.2* dann auf Seite der Steuerungs-Hersteller umgesetzt werden muss.

Aus Sicht eines Werkzeugmaschinenbauers ist hier besonders relevant, dass der Systemlieferant sich in das eigene Sicherheitslücken-Management eingliedert und entsprechende Informationen bereitstellt. Außerdem sollten Freigaben bspw. für Betriebssystemupdates erfolgen, so dass diese bereits aufseiten des Steuerungs-Lieferanten auf Kompatibilität zum eigenen System getestet worden sind, da dies für einen Werkzeugmaschinenhersteller kaum leistbar ist.

4.3.2 Unterstützungsangebote

Seitens vieler Systemlieferanten sind Hinweise und verschiedene Veröffentlichungen verfügbar, die weitere Hilfestellung beim konkreten Steuerungssystem geben. An dieser Stelle sei dazu auf die jeweiligen Webseiten der Hersteller verwiesen.

5. Behandlung des „brown field“

5.1 Ausgangslage

Werkzeugmaschinen stellen langlebige Investitionsgüter dar, die oft jahrzehntelang betrieben werden – einen Großteil der Anlagen in einer typischen Fertigung stellen daher zwangsläufig ältere Anlagen dar. Unter dem Gesichtspunkt OT/IT-Security zählen dazu auch nur wenige Jahre (oder gar Monate!) alte Maschinen, welche vielleicht sogar schon zum Zeitpunkt der ersten Inbetriebnahme beim Kunden nicht mehr auf dem neusten Stand bspw. seitens des Betriebssystems waren, da allein die Liefer- und Transportzeiten länger sein können als der zeitliche Abstand von Sicherheitspatches.

Auch für Baureihen, welche zwar zum aktuellen Lieferprogramm zählen, deren Entwurfs- und Entwicklungsprozess aber zu großen Teilen schon länger zurückliegt und welche daher nicht mehr im beschriebenen Sinne abgesichert werden können oder sollen, müssen Wege zur Absicherung jenseits des Entwurfsprozesses erschlossen werden.

Daraus folgt:

1. Es muss eine Lösung für bestehende Anlagen gefunden werden, diese so zu betreiben, dass die Verfügbarkeit gesichert und dennoch die Vorzüge einer Digitalisierung in der Produktion unter Einbehaltung hoher Sicherheitsstandards umgesetzt werden können.
2. Eine solche Lösung kann als ergänzende Komponente auch Neumaschinen weiter absichern.

Ein erfolgversprechender Ansatz ist die Kapselung der Systeme wie im Folgenden beschrieben.

5.2 Abgrenzung und Kapselung von Systemen

Das im Rahmen des sicheren Entwicklungsprozesses vorgestellte Konzept einer Zonierung kann auch als integraler Bestandteil der begleitenden Maßnahmen zur Betriebszeit angesehen werden. Wird ein Edge Gateway, wie in → Abb. 11 dargestellt, zur Entkopplung der Werkzeugmaschine von wesentlichen Teilen ihrer OT-Umgebung eingesetzt, so engt dies die potenzielle Angriffsfläche erheblich ein. Alles „hinter“ dem Gateway kann dann als Blackbox betrachtet werden.

Praktisch bekommt in einer solchen Architektur vor allem die Schnittstelle nach außen, also das Gateway, eine hohe Security-Relevanz: Kritische Sicherheitslücken müssen hier umgehend (d. h. innerhalb von Stunden oder Tagen, nicht Wochen oder Monaten) erkannt und behoben werden. Diese Aufgabe können ggf. spezielle Dienstleister übernehmen, welche auf das Device Management der von ihnen vertriebenen Geräte spezialisiert sind. Das dahinterliegende – ggf. sehr komplex aufgebaute – Steuerungssystem ist dann auf diesem Pfad nicht mehr in gleicher Weise Bedrohungen über die Netzwerk-Schnittstelle ausgesetzt. Dieser Aufbau bietet also einen Lösungsansatz für das Problem, dass die hohe Komplexität in Hard- und Software einer typischen Steuerungsumgebung für Werkzeugmaschinen in der Praxis die Applikation von Sicherheitspatches erschwert oder unmöglich macht. Das Gateway hingegen ist unabhängig von der Maschine und kann daher relativ einfach aktuell gehalten werden. Entsprechende Gateways (mit automatischen Update-Mechanismen) sind seitens der Steuerungshersteller und weiterer Anbieter verfügbar.



Ein solcher Aufbau schützt nur die Netzwerk-Schnittstelle und nicht andere Eintrittspfade (Wechsel-datenträger, anderweitig angebundene Anlagen ...) und kann daher nur *eine*, wenn auch wichtige Komponente eines Sicherheitsschirmes darstellen.

Beispiel: Eine 5 Jahre alte, NC-gesteuerte Werkzeugmaschine, integriert in die IT-Umgebung eines kleineren produzierenden Betriebes, soll abgesichert werden.



Ist-Situation Werkzeugmaschine:

- HMI auf Basis von Microsoft Windows 7.
 - Windows-Patch-Level mit Stand der Auslieferung, also 5 Jahre alt.
- HMI läuft auf einem Industrie-PC mit zwei Netzwerk-Ports.
 - Der erste Port des Industrie-PC ist mit einem Netzwerk innerhalb der Werkzeugmaschine verbunden, dieses wird genutzt zur Kommunikation der Steuerungskomponenten untereinander.
 - Der zweite Port des Industrie-PC ist mit dem Firmennetzwerk des Betreibers zum Austausch von NC-Programmen verbunden (Windows-Dateifreigabe/SMB-Protokoll).
 - Im HMI sind die beiden Ports logisch über eine entsprechende Konfiguration des Steuerungsherstellers getrennt.
- Weitere Maschinenkomponenten (z. B. Sensor-Gateways, Prozessüberwachung) sind am maschinen-internen Netzwerk angebunden und kommunizieren mit den Steuerungskomponenten.
- NC-Steuerung und SPS laufen auf einem proprietären Betriebssystem (Linux-Derivat), der Werkzeugmaschinenhersteller hat auf diese Betriebssysteme keinen Zugriff.
- Ein Virens Scanner ist vom Steuerungshersteller nicht freigegeben, dieser könnte zu einer Verlangsamung der Bedienoberfläche oder unklaren Fehlfunktionen führen.
- Remote-Service läuft über lokal auf dem HMI installierte Client-Software.

Ist-Situation Firmennetz:

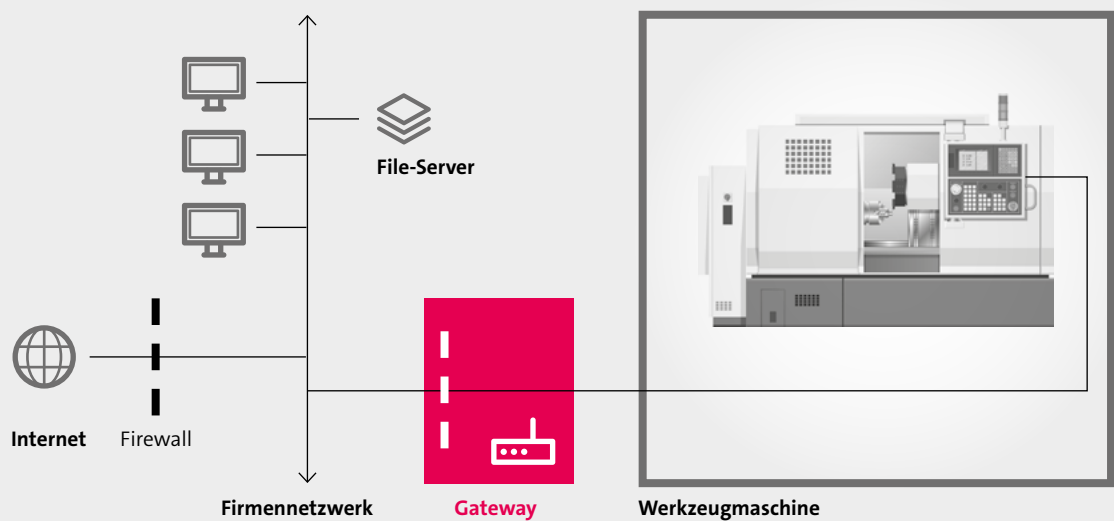
- Das Firmennetz ist durch einen Router mit integrierter Firewall aus dem Consumerbereich vom Internet entkoppelt.
- Anbindung der Maschine an das Internet indirekt über die Firmen-Firewall im Router.
- Keine LAN-Segmentierung innerhalb des Firmennetzes, die Produktionsmaschinen sind alle im gleichen Netzwerksegment wie andere IT-Geräte, etwa der File-Server des Unternehmens.

Bedrohungen:

- Microsoft Windows 7 ist aus heutiger IT-Sicht veraltet und nicht mehr auf einen zeitgemäßen Stand an IT-Security zu bringen:
 - Das System ist von Microsoft abgekündigt.
 - Es ist im Beispiel auf einem sehr alten Patch-Stand und daher besonders verwundbar für viele in den letzten Jahren aufgetretene Sicherheitslücken.
 - Es können nicht einmal alle aktuell verfügbaren Sicherheitspatches für das Betriebssystem eingespielt werden, weder durch den Betreiber noch durch den Werkzeugmaschinenhersteller, da die Patches nicht vollständig auf Kompatibilität mit der HMI-Software des Steuerungsherstellers sowie ggf. eigenentwickelter HMI-Software geprüft sind.
 - Ein Update des Betriebssystems auf die aktuelle Windows-Version ist aufgrund von Hardwaregrenzen und Kompatibilitätsproblemen der eingesetzten Software ebenfalls nicht möglich.
- Sollte der Industrie-PC kompromittiert werden, könnte über diesen Weg (oder direkt über einen angeschlossenen Service-Rechner) die NC/SPS selbst als Angriffsziel in den Fokus geraten. Die Software auf der NC/SPS kann nicht ohne weiteres aktualisiert werden, da hier erhebliche Aufwände und ggf. Inkompatibilitäten zu erwarten sind.
- Weitere Komponenten im Maschinennetz, wie eine Prozessüberwachung o. Ä., können auf dem gleichen Weg kompromittiert werden.

- Der Industrie-PC hängt direkt am Firmennetz und ist ausschließlich durch Windows-interne Mechanismen von der Zone des Maschinennetzwerks getrennt. Diese Mechanismen sind wie beschrieben als unsicher zu betrachten.
- Ein Angriff ausgehend vom Firmennetz würde die Maschine mit hoher Wahrscheinlichkeit erfolgreich kompromittieren. Ein solcher Angriff könnte beispielsweise durch weitere, ggf. auch kurzfristig im Firmennetz vorhandene Geräte wie Service-Laptops durch Lieferanten ohne deren Wissen oder auch durch von Trojanern befallene Geräte innerhalb des Firmennetzes erfolgen.
- Umgekehrt könnte im Falle einer Kompromittierung der Maschine, egal auf welchem Wege, ein Angriff auf alle im Firmennetz erreichbaren Ziele erfolgen.
- Die Maschine kann als „Rückzugsgebiet“ für Schadsoftware dienen, welche dann immer wieder das Firmennetz angreift. Ein solches Szenario ließe sich voraussichtlich nur durch komplette Wiederherstellung bzw. Neuinstallation des Industrie-PC lösen.

Abb. 20:
Strukturbild
des Beispiel-
szenarios
(mit
Gateway)



Maßnahme: Gateway

- Durch die Abkapselung des Industrie-PC vom Firmennetz über ein Gateway mit Firewall-Funktion kann die Werkzeugmaschine „hinter“ dem Gateway als eine Zone (Blackbox) betrachtet werden.
- Ein entsprechendes Gateway kann auch im Feld jederzeit nachgerüstet werden.
- Die Systemsicherheit hinsichtlich der LAN-Schnittstelle (!) wird so durch das Gateway gewährleistet und ist damit maßgeblich unabhängig von Patch-Level und installierter Software auf der Werkzeugmaschine.
- Bestimmend für die Systemsicherheit ist das Gateway; dieses sollte daher (ggf. durch einen spezialisierten Anbieter) permanent aktuell gehalten werden.
- Die Kommunikation innerhalb des lokalen Maschinen-Netzwerks (z. B. zwischen Prozessüberwachung und Steuerung) ist in keiner Weise beschränkt oder beeinträchtigt, wird jedoch auch nicht überwacht.
- Sämtliche erwünschten Zugriffe auf die Maschine aus dem Firmennetz und umgekehrt müssen im Gateway explizit freigegeben werden.

Im dargestellten Fall betrifft dies:

- Windows-Dateifreigaben zur Übertragung von NC-Programmen auf die Maschine
- Bildschirmfreigabe für den Remote-Service

Die genauen Freigaben richten sich nach den eingesetzten Protokollen und der Zugriffsrichtung (z. B. Firmennetz → Maschine oder umgekehrt).



Zu beachten ist aber für den geschilderten Anwendungsfall: Es kann weiterhin eine Kompromittierung des Systems durch externe Service-Rechner oder die USB-Schnittstelle erfolgen! Hier sind ggf. weitere Schutzmaßnahmen zu implementieren, ggf. auch organisatorische (z. B. Verbot von USB-Sticks an der Maschine).

6. Literatur

Index	Literaturstelle	Beschreibung
[1]	VDW: IT-Sicherheit an Werkzeugmaschinen – Maßnahmen zur einfachen Umsetzung. Whitepaper, 2020. → https://vdw.de/wp-content/uploads/2021/03/pub_IT-Sicherheit-an-Werkzeugmaschinen_VDW.pdf	Maßnahmensammlung für Anwender und Betreiber zur Erhöhung der IT-Sicherheit beim Betrieb von Werkzeugmaschinen, auf Anfrage beim VDW auch als Druckexemplar erhältlich
[2]	ZVEI: Orientierungsleitfaden für Hersteller zur IEC 62443. Whitepaper, 2017.	Orientierungsleitfaden
[3]	VDMA: Leitfaden IEC 62443 für den Maschinen- und Anlagenbau. Überarbeitete Ausgabe, 2021.	Einführung in die IEC 62443 mit vielen Hinweisen zur Bewertung von Anlagen, auf Anfrage beim VDMA erhältlich
[4]	Andreas Kurtz: Von niedrig bis kritisch: Schwachstellenbewertung mit CVSS. → https://heise.de/-5031983 (Stand: 25.01.2021)	Artikel zur Beschreibung des CVSS-Systems
[5]	Forum of Incident Response and Security Teams (FIRST): Common Vulnerability Scoring System Version 3.1 Calculator. → https://www.first.org/cvss/calculator/3.1 (Stand: 18.01.2022)	Online-Rechner für das CVSS-Scoring-System

© Copyright 2022

Herausgeber

Verein Deutscher Werkzeugmaschinenfabriken e. V. (VDW)
Fachverband Werkzeugmaschinen und
Fertigungssysteme im VDMA
Lyoner Straße 18
60528 Frankfurt am Main
Tel. +49 69 756081-0
Fax +49 69 756081-11
E-Mail vdw@vdw.de
Internet www.vdw.de
Twitter www.twitter.com/VDWonline
YouTube www.youtube.com/metaltradefair

Vorsitzender

Franz-Xaver Bernhard,
Maschinenfabrik Berthold Hermle AG, Gosheim

Geschäftsführer

Dr. Wilfried Schäfer

Autoren

Arbeitskreis „Steuerungs- und Systemtechnik“ des
VDW-Forschungsinstituts, unter fachlicher Beratung
von Prof. Dr. Felix Hackelöer, Institut für Automation
& Industrial IT (AIT), TH Köln, sowie Bernd Gehring,
Peter Schmidt und Tilo Renz, ditis Systeme, Zweig-
niederlassung der JMV SE & Co. KG, Ulm

Gestaltung

Klaus Bietz \ visuelle Kommunikation, Frankfurt am Main

Druck

Druck- und Verlagshaus Zarbock GmbH & Co. KG

Stand

10/2022

Bildnachweis

Adobe Stock

