

**Sicherheitsrichtlinie
für Fabrikautomationssysteme**

Einleitung

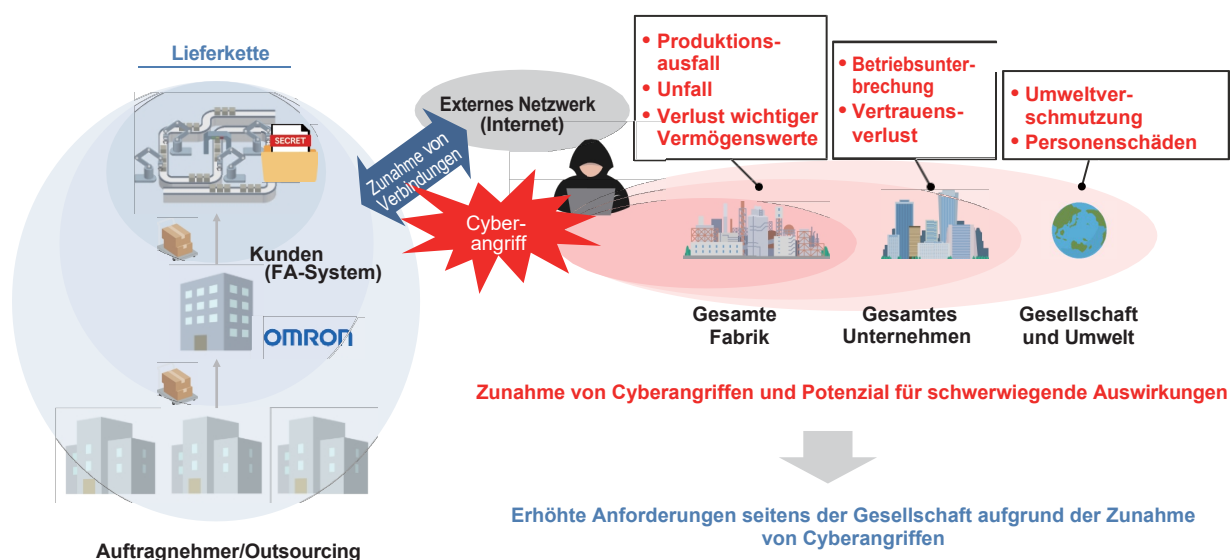
Hintergrund und Ziele

In den letzten Jahren haben Hersteller Initiativen zur Nutzung von IT-/IoT-Technologien und Daten in ihren Produktionsstätten vorangetrieben, um die Produktivität und Qualität zu verbessern. Mit der Zunahme der Verbindungen zur Außenwelt, einschließlich des Internets, der Komplexität der Lieferkette und der ständig wachsenden Bedeutung von Produktsicherheit und -qualität sowie Daten in Geräten der Fabrikautomation (im Folgenden als FA bezeichnet) hat die Zahl der Angriffe zugenommen, die sich gegen FA-Systeme selbst richten oder Organisationen und FA-Systeme mit unzureichenden Sicherheitsmaßnahmen in der Lieferkette als Sprungbrett nutzen. Dementsprechend erlassen Länder Gesetze und Vorschriften zur Cybersicherheit, die Hersteller und Betreiber von FA-Systemen, FA-Systeme und FA-Systemkomponenten abdecken, während Branchen wie die Steuerungssystemindustrie*¹, die Halbleiterindustrie*² und die Automobilindustrie*³ ihre Sicherheitsanforderungen standardisieren. Damit wächst auch die gesellschaftliche Nachfrage nach Cybersicherheit

*1. IEC 62443-Reihe

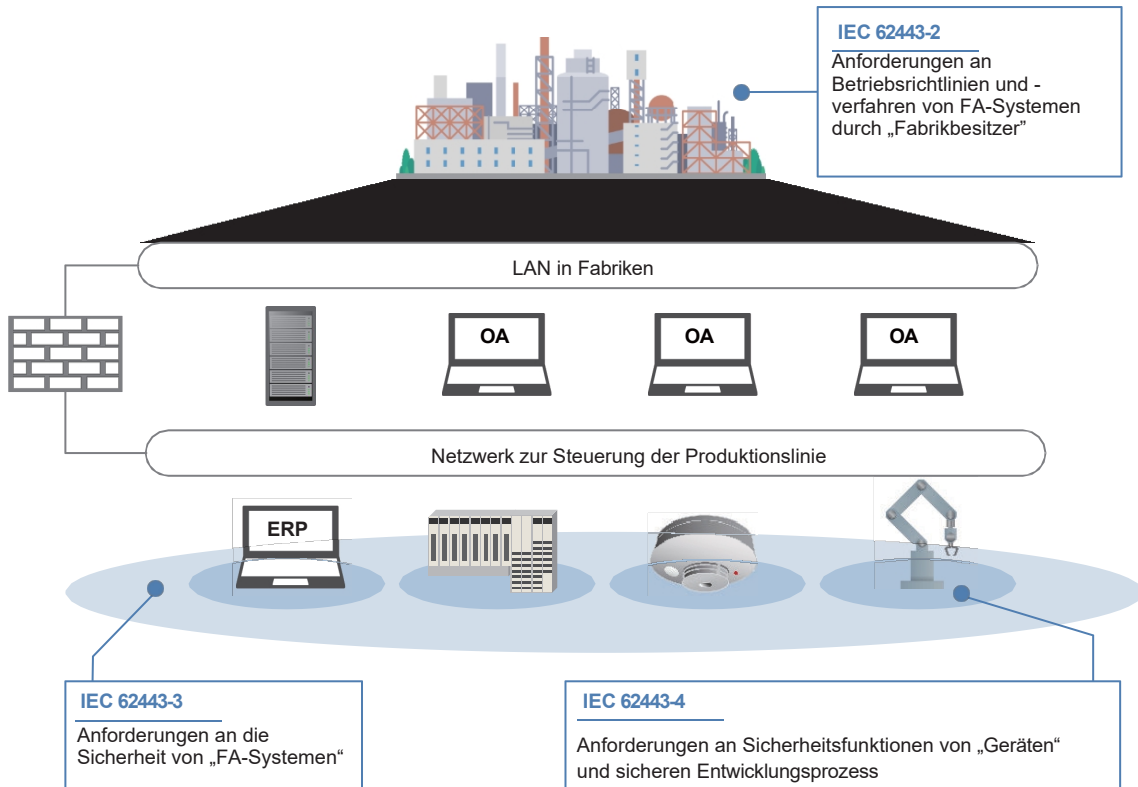
*2. SEMI E169 Leitfaden für die Sicherheit von Geräteinformationssystemen (EISS), E187 Spezifikation für die Cybersicherheit von Fab-Geräten, E188 Spezifikation für die Integration von Malware-freien Geräten usw.

*3. UN-R155: Cybersicherheit und Cybersicherheits-Managementsystem (CSMS), ISO/SAE 21434:2021 Straßenfahrzeuge – Cybersicherheitstechnik usw.



Insbesondere die Fertigungsindustrie nutzt und erwirbt Zertifizierungen für die IEC 62443-Reihe, die als internationale Normen für die Cybersicherheit von Steuerungssystemen formuliert wurde, und viele Unternehmen und Industrieorganisationen beziehen sich auf diese Normen. Die IEC 62443 definiert eine Vielzahl von Anforderungen an die Sicherheit von Steuerungssystemen, von Anforderungen an das Sicherheitsmanagement, die Unternehmen erfüllen sollten, bis hin zu Anforderungen an Sicherheitsfunktionen, über die Systeme verfügen sollten.

IEC 62443-2 definiert Richtlinien und Verfahren für den Fabrikbetrieb für Fabrikbesitzer. Darüber hinaus definiert IEC 62443-3 Sicherheitsanforderungen, die Integratoren von Steuerungssystemen beim Bau von Produktionsanlagen anwenden sollten. Darüber hinaus definiert IEC 62443-4 Anforderungen an Sicherheitsfunktionen und sichere Entwicklungsprozesse für Lieferanten von Steuerungskomponenten.



Vor diesem Hintergrund ist sich die OMRON Corporation bewusst, wie wichtig es ist, Menschen, Anlagen und Produkte in Ihren Fabriken vor Cyberangriffen zu schützen und zu einem stabilen Betrieb in der Produktion und zum Schutz Ihrer Anlagen in Ihren Fabriken sowie zur sicheren Nutzung von Daten an Ihren Produktionsstandorten beizutragen. Der Zweck dieses Dokuments besteht darin, Ihnen ein Verständnis für die Sicherheitsinitiativen von OMRON in Bezug auf seine FA-Produkte zu vermitteln und Sicherheitsmaßnahmen vorzuschlagen, die die Benutzer der FA-Produkte selbst ergreifen sollten.

Zielgruppe

Dieses Dokument ist für die Verwendung bei der Umsetzung von Sicherheitsmaßnahmen in den folgenden Organisationen vorgesehen.

Organisation	Definition
Fabrikbesitzer	Der Eigentümer der gesamten Fabrik einschließlich FA-Systemen
Systemintegrator	Eine Organisation, die für die Einführung von FA-Systemen zuständig ist
Automatisierungslieferant	Ein Hersteller, der Steuerungsgeräte für FA-Systeme entwickelt, produziert und wartet

Haftungsausschluss

Die Empfehlungen, die wir unseren Kunden in diesem Dokument geben, basieren auf den Ergebnissen unserer Analysen und Untersuchungen. Da geeignete Sicherheitsmaßnahmen je nach Kundenumgebung variieren, garantieren diese Empfehlungen nicht die Verhinderung aller Sicherheitsverletzungen in Kundenumgebungen. Bitte berücksichtigen Sie dieses Dokument und führen Sie Analysen und geeignete Gegenmaßnahmen entsprechend der Kundenumgebung selbst durch.

INHALT

Einleitung	1
Hintergrund und Ziele	1
Zielgruppe	2
Haftungsausschluss	2
Revisionsverlauf	5

Abschnitt 1 Produktsicherheitsinitiativen bei OMRON

1-1 Grundlegende Richtlinien zur Produktsicherheit	1-2
1-2 Aufbau einer Organisationsstruktur für die Produktsicherheit	1-3
1-2-1 Stärkung der Organisation zur Förderung unternehmensweiter Aktivitäten und Aktivitäten zur Produktsicherheit	1-3
1-2-2 Stärkung der Governance und Organisation	1-3
1-3 Bereitstellung von Produkten und Dienstleistungen, die Sicherheitsaspekte berücksichtigen	1-5
1-3-1 Implementierung des sicheren Lebenszyklus von FA-Produkten	1-5
1-3-2 Empfehlung für eine umfassende Verteidigung	1-6
1-3-3 Sicherung der Lieferkette	1-6
1-3-4 Einhaltung von Gesetzen und Normen	1-6
1-4 Reaktionen auf Schwachstellen und Vorfälle	1-8
1-4-1 Einrichtung einer Kontaktstelle (PSIRT) für Schwachstellen und Vorfälle	1-8
1-4-2 Reaktionen auf Sicherheitslücken und Vorfälle	1-8
1-5 Bereitstellung von Sicherheitsinformationen zu Produkten und Dienstleistungen	1-9
1-5-1 Bereitstellung von Informationen zu Sicherheitslücken und Sicherheitshinweisen	1-9
1-5-2 Offenlegung von Richtlinien zur Cybersicherheit und Produktsicherheit	1-9
1-5-3 Zusammenarbeit mit Sicherheitsbehörden (Koordinierungsorganisationen)	1-9

Abschnitt 2 Notwendigkeit und Zweck von Sicherheitsmaßnahmen

2-1 Notwendigkeit von Sicherheitsmaßnahmen	2-2
2-2 Zweck der Sicherheitsmaßnahmen	2-3
2-2-1 Zu schützende Elemente	2-3
2-2-2 Verfahren zur Risikobewertung	2-4

Abschnitt 3 Durchführung der Risikobewertung

3-1 Klärung der Risikoziele	3-2
3-1-1 Festlegung der Analyseziele	3-2
3-1-2 Identifizierung von Anwendungsfällen	3-3
3-1-3 Festlegen der Wichtigkeit einer Sicherheitszone	3-3
3-2 Risikobewertung	3-5
3-2-1 Identifizierung von Vermögenswerten	3-5
3-2-2 Identifizierung von Bedrohungen	3-6
3-2-3 Risiken bewerten	3-7
3-3 Konzept der Risikominderungsmaßnahmen	3-9
3-3-1 Festlegung von Risikominderungsmaßnahmen	3-9
3-3-2 Maßnahmen, die während des gesamten Lebenszyklus zu ergreifen sind	3-9
3-3-3 Sicherheit durch Design	3-10
3-3-4 Tiefgreifende Verteidigung	3-10

Abschnitt 4 Sicherheitsmaßnahmen

4-1	Bedrohungen für FA-Systeme	4-2
4-2	Sicherheitsmaßnahmen in FA-Systemen	4-3
4-2-1	Sicherheitsmaßnahmen für die Mensch- und Prozessebene	4-4
4-2-2	Sicherheitsmaßnahmen für die physische Ebene	4-6
4-2-3	Sicherheitsmaßnahmen für die technische Ebene	4-6

Anhänge

A-1	Verwandte Materialien	A-2
------------	------------------------------------	------------

Revisionsverlauf

Ein Revisionscode erscheint als Suffix zur Katalognummer auf der Vorder- und Rückseite dieses Dokuments.

Kat.-Nr. P162-E1-03

↑
Revisionscode

Revisionscode	Datum	Überarbeiteter Inhalt
01	August 2023	Originalproduktion
02	März 2025	<ul style="list-style-type: none">• Sicherheitsmaßnahmen in FA-Systemen hinzugefügt.• Fehler korrigiert.
03	Januar 2026	Fehler korrigiert.

1

Produktsicherheitsinitiativen bei OMRON

Um sichere Produkte zu entwickeln und anzubieten, ist OMRON bestrebt, eine Organisationsstruktur aufzubauen, die die Produktsicherheit fördert, und setzt sich für die sichere Implementierung von Produkten während des gesamten Produktlebenszyklus ein.

1-1	Grundlegende Richtlinien zur Produktsicherheit	1-2
1-2	Aufbau einer Organisationsstruktur für die Produktsicherheit	1-3
1-2-1	Stärkung der Organisation zur Förderung unternehmensweiter und produktspezifischer Sicherheit	1-3
1-2-2	Stärkung der Governance und Organisation	1-3
1-3	Bereitstellung von Produkten und Dienstleistungen, die Sicherheitsaspekte berücksichtigen berücksichtigen	1-5
1-3-1	Implementierung des FA Product Secure Lifecycle	1-5
1-3-2	Empfehlung für eine umfassende Verteidigung	1-6
1-3-3	Sicherung der Lieferkette	1-6
1-3-4	Einhaltung von Gesetzen und Normen	1-6
1-4	Reaktionen auf Schwachstellen und Vorfälle	1-8
1-4-1	Einrichtung einer Kontaktstelle (PSIRT) für Sicherheitslücken und Vorfälle	1-8
1-4-2	Reaktionen auf Schwachstellen und Vorfälle	1-8
1-5	Bereitstellung von Sicherheitsinformationen zu Produkten und Dienstleistungen	1-9
1-5-1	Bereitstellung von Informationen zu Sicherheitslücken und Sicherheitshinweisen	1-9
1-5-2	Offenlegung von Richtlinien zur Cybersicherheit und Produktsicherheit	1-9
1-5-3	Zusammenarbeit mit Sicherheitsbehörden (Koordinierungsorganisationen)	1-9

1-1 Grundlegende Richtlinien zur Produktsicherheit

OMRON arbeitet an den folgenden Maßnahmen zur Produktsicherheit, um Produkte und Dienstleistungen anzubieten, die Sicherheitsvorkehrungen gegen Cyberangriffe umsetzen.

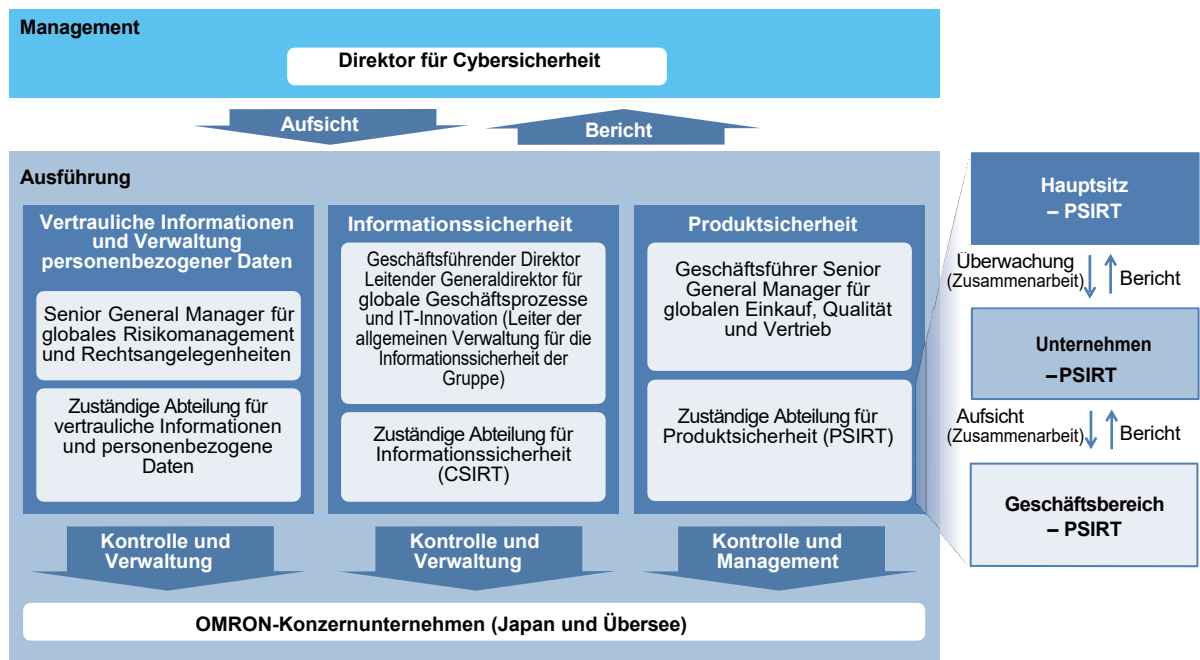
<p><i>1-2 Aufbau einer Organisationsstruktur für Produktsicherheit auf Seite 1-3</i></p>	<p>OMRON hat ein Kooperationssystem zwischen der Zentrale und den Geschäftsbereichen eingerichtet, um Maßnahmen zur Produktsicherheit zu fördern, und arbeitet daran, die Organisation durch Schwachstellenmanagement von Produkten und Dienstleistungen, Stärkung der internen Governance und Schulung der Mitarbeiter zu stärken.</p>
<p><i>1-3 Bereitstellung von Produkten und Dienstleistungen unter Berücksichtigung der Sicherheit auf Seite 1-5</i></p>	<p>OMRON arbeitet an Sicherheitsmaßnahmen gegen Cyberangriffe während des gesamten Produktlebenszyklus, einschließlich Planung, Entwicklung, Betrieb/Wartung und Entsorgung.</p>
<p><i>1-4 Reaktionen auf Schwachstellen und Vorfälle auf Seite 1-8</i></p>	<p>OMRON sammelt umfassend Informationen über Schwachstellen seiner Produkte und Dienstleistungen und ergreift zeitnah Gegenmaßnahmen gegen entdeckte Schwachstellen. Im Falle eines Vorfalls richtet OMRON umgehend ein Reaktionssystem ein, führt die erforderlichen internen und externen Meldungen durch, legt Informationen offen, untersucht die Ursache und verhindert eine Wiederholung.</p>
<p><i>1-5 Bereitstellung von Sicherheitsinformationen zu Produkten und Dienstleistungen auf Seite 1-9</i></p>	<p>OMRON legt Bewertungskriterien und Reaktionsverfahren für Sicherheitslücken fest, die von externen Organisationen und Kunden gemeldet oder durch Selbstdiagnoseergebnisse ermittelt wurden, arbeitet mit den entsprechenden Organisationen zusammen und informiert seine Kunden zeitnah über Sicherheitslücken.</p>

Jede dieser Initiativen wird in den folgenden Abschnitten vorgestellt.

1-2 Aufbau einer Organisationsstruktur für Produktsicherheit

1-2-1 Stärkung der Organisation zur Förderung unternehmensweiter und produktbezogener Sicherheitsmaßnahmen

OMRON hat die Stärkung der Cybersicherheit als unternehmensweite Priorität positioniert und eine treibende Organisation für jeden Bereich der *Verwaltung vertraulicher Informationen und personenbezogener Daten*, der *Informationssicherheit* und der *Produktsicherheit* aufgebaut. Das Unternehmen fördert Maßnahmen zur Lösung von Cybersicherheitsproblemen und Initiativen für zukünftige Verbesserungen.



Um Initiativen im Zusammenhang mit der *Produktsicherheit* zu fördern und zu verwalten, verfügt OMRON über eine Organisation namens ^{PSIRT}*1, die die Produktsicherheit in allen Geschäftsbereichen und Abteilungen verwaltet. PSIRTs sind auf verschiedenen Ebenen vom Hauptsitz bis zu den Geschäftsbereichen angesiedelt und arbeiten eng zusammen, um die Produktsicherheit für die gesamte OMRON-Gruppe zu gewährleisten.

*1. PSIRT (Product Security Incident Response Team)

1-2-2 Stärkung der Governance und Organisation

OMRON stärkt seine interne Governance und Organisation durch Mitarbeiterschulungen, um die Sicherheit der FA-Produkte und -Dienstleistungen für seine Kunden zu verbessern.

Initiativen für die Unternehmensführung

- OMRON hat die *OMRON-Konzernrichtlinien für Produktsicherheit* formuliert, in denen sicherheitsrelevante Richtlinien festgelegt sind, die von den Mitarbeitern zu befolgen sind, und informiert die Mitarbeiter regelmäßig darüber.
- Auf der Grundlage dieser Richtlinien arbeitet OMRON an der kontinuierlichen Verbesserung sicherheitsbezogener Initiativen.

Initiativen zur Stärkung der Organisation

- OMRON hat eine Kompetenzkarte für die Sicherheitsmaßnahmen erstellt, die das Unternehmen bei der Entwicklung und Bereitstellung von FA-Produkten durchführt, und ist bestrebt, die Kompetenzen seiner Mitarbeiter auf dieser Grundlage zu verwalten, einschließlich Schulungen, der Förderung des Erwerbs externer Sicherheitszertifizierungen durch die Mitarbeiter und der Einrichtung eines internen Zertifizierungssystems.
- OMRON fördert regelmäßige Sicherheitsschulungen zu den neuesten Sicherheitstrends für die Leiter der Abteilungen, die mit Sicherheitsmaßnahmen befasst sind.

1-3 Bereitstellung von Produkten und Dienstleistungen, die Sicherheitsaspekte berücksichtigen

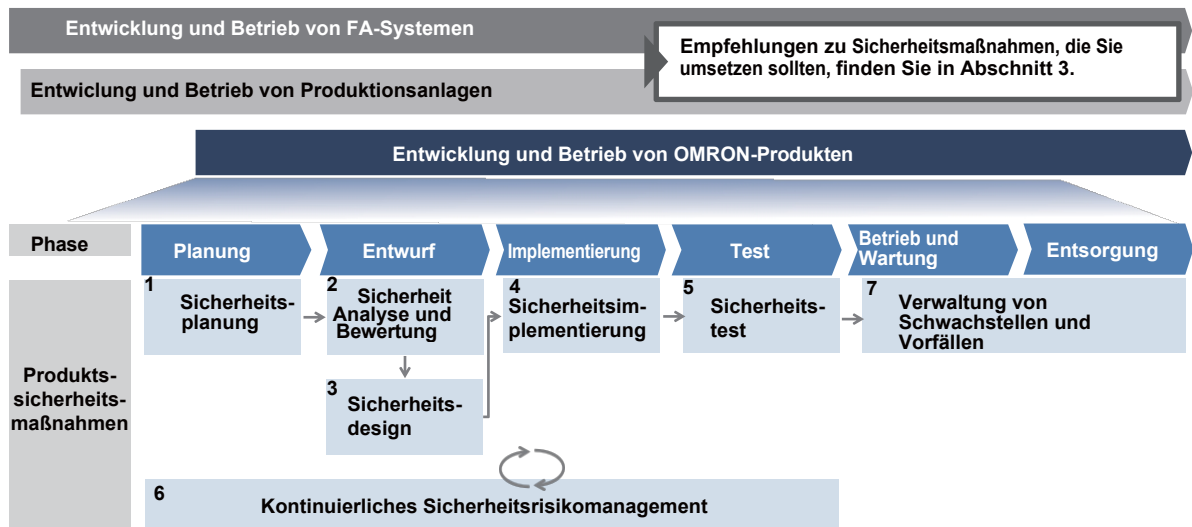
1-3-1 Implementierung eines sicheren Lebenszyklus für FA-Produkte

OMRON entwickelt FA-Produkte unter Berücksichtigung von Sicherheitsrisiken bereits in der Produktplanungs- und -entwurfsphase auf der Grundlage des Konzepts „Secure by Design**1“, um sicherzustellen, dass seine Kunden die Produkte sicher und zuverlässig verwenden können. Um dies zu erreichen, ist OMRON der Ansicht, dass es neben den Produktsicherheitsmaßnahmen in jeder Entwicklungsphase wichtig ist, den Status der Reaktion auf Sicherheitsrisiken unabhängig von der Phase zu überprüfen und zu verwalten.

Darüber hinaus führt OMRON auch nach der Auslieferung seiner FA-Produkte an die Kunden weiterhin Maßnahmen zur Reaktion auf Sicherheitsrisiken während des gesamten Produktlebenszyklus durch, bis die FA-Produkte vom Kunden sicher betrieben, gewartet und entsorgt werden.

*1. Secure by Design ist das Konzept, ein sicheres System zu entwickeln, indem die Sicherheit des Systems bereits in einer frühen Phase des Entwicklungsprozesses berücksichtigt wird. Es hilft, Schwachstellen und Vorfälle zu verhindern.

Im Folgenden finden Sie einen Überblick über die Aktivitäten von OMRON im Lebenszyklus von FA-Produkten unter Berücksichtigung der Sicherheit.



- Sicherheitsplanung:**
Definieren Sie die Funktionen und Informationsressourcen des zu entwickelnden FA-Produkts sowie die Annahmen für die Reaktion auf Sicherheitsrisiken, wie z. B. die Betriebsumgebung, und planen Sie die nachfolgenden FA-Produktsicherheitsmaßnahmen.
- Sicherheitsanalyse und -bewertung:**
Analysieren und bewerten Sie die Sicherheitsrisiken des zu entwickelnden FA-Produkts auf der Grundlage der in der Sicherheitsplanung definierten Prämissen und legen Sie Reaktionsrichtlinien und Prioritäten fest.
- Sicherheitsdesign:**
Auf der Grundlage der in der Sicherheitsanalyse und -bewertung festgelegten Reaktionsrichtlinien und Prioritäten werden die Sicherheitsanforderungen für die zu entwickelnden FA-Produkte definiert und ein technisches Design zu deren Umsetzung erstellt.
- Sicherheitsimplementierung:**

Wenden Sie sichere Codierung an, um die Einführung von Schwachstellen zu verhindern, die durch das Sicherheitsdesign allein nur schwer zu verhindern sind, und stärken Sie so die Reaktionen auf Sicherheitsrisiken.

5. Sicherheitstest:
Stellen Sie sicher, dass die Reaktionen auf Sicherheitsrisiken im FA-Produkt vollständig und angemessen sind.
6. Kontinuierliches Sicherheitsrisikomanagement
Geben Sie wichtige Punkte für die Überprüfung von Sicherheitsrisiken während der Entwicklung des FA-Produkts an, um sicherzustellen, dass Sicherheitsrisiken ordnungsgemäß identifiziert, analysiert und behandelt werden.
7. Verwaltung von Schwachstellen und Vorfällen:
Erkennen Sie Schwachstellen und Vorfälle durch aktive Informationsbeschaffung oder interne und externe Berichte und verwalten Sie die Situationen kontinuierlich bis zum Abschluss der Maßnahmen.

1-3-2 Empfehlung für eine tiefgreifende Verteidigung

Um die Sicherheit von FA-Systemen beim Kunden zu gewährleisten, empfiehlt OMRON einen Sicherheitsansatz, der auf dem Konzept der Defense in Depth basiert. Dabei werden mehrere Maßnahmen hierarchisch miteinander kombiniert, wie z. B. die Festlegung von Betriebsrichtlinien und -verfahren, die Verhinderung des physischen Eindringens in Fabriken und die Umsetzung technischer Maßnahmen für Netzwerke und Geräte, um die Sicherheit zu erhöhen. Informationen zum Konzept der Defense in Depth finden Sie unter 3-3-4 *Defense in Depth* auf Seite 3-10.

1-3-3 Sicherung der Lieferkette

OMRON betrachtet Schwachstellen in seiner Lieferkette als erhebliches Sicherheitsrisiko und definiert Outsourcing-Auftragnehmer und Lieferanten für Tätigkeiten im Zusammenhang mit der Entwicklung und Bereitstellung seiner FA-Produkte ebenfalls als Ziele des Sicherheitsmanagements.

OMRON setzt die folgenden Maßnahmen zur Sicherheit der Lieferkette um.

Sichere Outsourcing- und Beschaffungsprozesse

Im Bereich Outsourcing und Beschaffung bewertet und verwaltet OMRON Auftragnehmer und Lieferanten anhand geeigneter Prozesse, darunter Auswahl, Vertragsabschluss und Audits unter Berücksichtigung von Sicherheitsaspekten.

Sicherheitsprüfung von extern beschafften Artikeln

Um die Sicherheitsqualität extern beschaffter Artikel zu gewährleisten, arbeitet OMRON mit Auftragnehmern und Lieferanten zusammen, um die Sicherheitsqualität der aus der Lieferkette bezogenen Artikel zu verwalten, indem es sie auffordert, die für die Lieferprüfung und das Schwachstellenmanagement nach der Lieferung erforderlichen Konfigurationsmanagementinformationen bereitzustellen.

1-3-4 Einhaltung von Gesetzen und Normen

OMRON hat sich verpflichtet, sichere FA-Produkte zu entwickeln und anzubieten, indem es nationale und internationale Gesetze und Vorschriften zur Produktsicherheit einhält und interne Sicherheitsprozesse einrichtet, um internationale Standards im Zusammenhang mit der Sicherheit von Steuerungssystemen zu erfüllen.

Als objektiver Beweis dafür, dass OMRON tatsächlich einen Entwicklungslebenszyklus unter Berücksichtigung von Sicherheitsrisiken implementiert hat, haben einige FA-Produkte von OMRON die Zertifizierung nach der internationalen Norm IEC 62443-4-1*¹ und der chinesischen nationalen Norm GB40050*² erhalten.

OMRON verfolgt auch weiterhin die neuesten Sicherheitsgesetze und -standards im In- und Ausland und bemüht sich, rechtzeitig Vorbereitungen zu treffen.

*1. IEC 62443-4-1:2018 (Ausgabe 1.0):

Anforderungen an einen sicheren Produktentwicklungslebenszyklus

*2. GB 40050-2021: Allgemeine Sicherheitsanforderungen für kritische Netzwerkkomponenten

1-4 Reaktionen auf Schwachstellen und Vorfälle

1-4-1 Einrichtung einer Kontaktstelle (PSIRT) für Schwachstellen und Vorfälle

Damit Kunden und Sicherheitsforscher, die Sicherheitslücken in OMRON-Produkten entdecken, diese umgehend an OMRON melden können, hat OMRON das Product Security Incident Response Team eingerichtet. So kann OMRON in Zusammenarbeit mit den zuständigen Geschäftsbereichen und Regierungsorganisationen umgehend Gegenmaßnahmen ergreifen.

URL (Japanisch): <https://www.omron.co.jp/contact/ContactForm.do?FID=00280> URL (Englisch):

<https://www.omron.com/contact/ContactForm.do?FID=00282>

1-4-2 Reaktionen auf Schwachstellen und Vorfälle

OMRON sammelt umfassend Informationen zu Sicherheitslücken seiner Produkte und Dienstleistungen und ergreift zeitnah Gegenmaßnahmen gegen entdeckte Sicherheitslücken.

Wenn es aufgrund eines Cyberangriffs zu einem Vorfall bei den Produkten oder Dienstleistungen kommt, richtet OMRON umgehend ein Reaktionssystem ein, führt die erforderlichen internen und externen Meldungen durch, legt Informationen offen, untersucht die Ursache und verhindert eine Wiederholung.

1-5 Bereitstellung von Sicherheitsinformationen zu Produkten und Dienstleistungen

1-5-1 Bereitstellung von Informationen zu Sicherheitslücken und Sicherheitshinweisen

OMRON veröffentlicht auf seiner Website Informationen zu Sicherheitslücken in OMRON-Produkten und insbesondere bei kritischen Sicherheitslücken Sicherheitshinweise, in denen die Inhalte der Sicherheitslücken, die betroffenen Produkte, mögliche Auswirkungen und Gegenmaßnahmen zusammengefasst sind.

Informationen zu Sicherheitslücken in OMRON-Produkten

URL (Japanisch): https://www.omron.com/jp/ja/inquiry/vulnerability_information/ URL (Englisch): https://www.omron.com/global/en/inquiry/vulnerability_information/

Informationen zu Sicherheitslücken in OMRON FA-Produkten

URL (Japanisch): <https://www.fa.omron.co.jp/product/vulnerability/index.html> URL (Englisch): <https://www.ia.omron.com/product/vulnerability/index.html>

1-5-2 Offenlegung von Richtlinien zur Cybersicherheit und Produktsicherheit

OMRON betrachtet seine Initiativen zur Cybersicherheit als Teil seiner unternehmensweiten Risikomanagementaktivitäten und legt die Einzelheiten dieser Aktivitäten sowie sein Förderungssystem im Folgenden offen.

URL (Japanisch): <https://sustainability.omron.com/jp/compliance/> URL (Englisch): <https://sustainability.omron.com/en/compliance/>

Um sicherzustellen, dass Sie OMRON-Produkte sicher verwenden können, veröffentlicht OMRON seine grundlegenden Richtlinien und Aktivitäten zur Produktsicherheit als Produktsicherheitsrichtlinie.

URL (Japanisch): https://www.omron.com/jp/ja/inquiry/product_security/ URL (Englisch): https://www.omron.com/global/en/inquiry/product_security/

1-5-3 Zusammenarbeit mit Sicherheitsbehörden (Koordinierungsorganisationen)

Um einen schnellen Informationsaustausch und eine rasche Zusammenarbeit bei der Reaktion auf Sicherheitslücken zu gewährleisten, wenn in Produkten von OMRON eine Sicherheitslücke entdeckt wird, arbeitet OMRON mit nationalen und internationalen Koordinierungsorganisationen zusammen, darunter die folgenden.

- CISA (Cybersecurity and Infrastructure Security Agency)^{*1}
URL: <https://www.cisa.gov/>

^{*1} US-Behörde für Cybersicherheit und Infrastruktursicherheit. Eine Verwaltungsbehörde mit Aufgaben wie der Förderung von Cybersicherheitsmaßnahmen in relevanten Regierungsorganisationen und kritischen Infrastrukturen in den Vereinigten Staaten sowie der Förderung von Partnerschaften zwischen Industrie, Wissenschaft und Regierung.

2

Notwendigkeit und Zweck von Sicherheitsmaßnahmen

In diesem Abschnitt werden die Notwendigkeit von Sicherheitsmaßnahmen in FA-Systemen und deren Zweck beschrieben.

2-1	Notwendigkeit von Sicherheitsmaßnahmen	2-2
2-2	Zweck von Sicherheitsmaßnahmen	2-3
2-2-1	Zu schützende Elemente	2-3
2-2-2	Verfahren zur Risikobewertung	2-4

2-1 Notwendigkeit von Sicherheitsmaßnahmen

Um die Sicherheit Ihres FA-Systems zu gewährleisten, sollten Sie zusätzlich zu den von OMRON für seine FA-Produkte getroffenen Maßnahmen auch Sicherheitsmaßnahmen entsprechend Ihren Aufgaben ergreifen.

Zu diesem Zweck ist es wichtig, dass Sie die Sicherheitsrisiken, die mit den von Ihnen angebotenen Diensten, Systemen und Vorgängen verbunden sind, richtig verstehen und bewerten und während des gesamten Lebenszyklus des FA-Systems geeignete Sicherheitsmaßnahmen ergreifen.

2-2 Zweck der Sicherheitsmaßnahmen

Es ist wichtig, den Zweck von Sicherheitsmaßnahmen, Ziele und die Notwendigkeit von Sicherheitsmaßnahmen im Unternehmen mit klaren Begründungen darzulegen und mit Zustimmung der Geschäftsleitung vorzugehen. Ohne diesen Konsens werden andere geschäftliche Anforderungen Vorrang haben, und es wird schwierig, eine einheitliche Ausrichtung und Zusammenarbeit zwischen den Abteilungen zu erreichen. Mögliche Sicherheitsziele sind unter anderem die folgenden.

1. Fortführung des Geschäftsbetriebs und der Produktion
2. Sicherheit der Fabrik und Gewährleistung der Produktqualität
3. Sicherstellung des normalen Betriebs von FA-Systemen
4. Schützen Sie Informationen, Know-how und Daten in Bezug auf Produkte und Produktion
5. Sicherstellung der Sicherheitsqualität von Produkten und Erfüllung der Verantwortlichkeiten als Hersteller
6. Erfüllen Sie soziale Anforderungen aus Normen und externen Vorgaben
7. Wahren Sie das Markenimage Ihres Unternehmens und verhindern Sie den Verlust des Kundenvertrauens

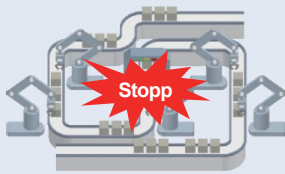


Identifizieren Sie anhand dieser Sicherheitsziele Bedrohungen, die besonders hohe Auswirkungen auf das Geschäft haben, berechnen Sie die Kosten für Gegenmaßnahmen und einigen Sie sich auf Ihre Ziele.

2

2-2-1 Zu schützende Elemente

2-2-1 Zu schützende Elemente

Es ist einfacher, Ziele festzulegen, wenn Sie klären, was im Zusammenhang mit dem Zweck Ihrer Sicherheitsmaßnahmen erhebliche Auswirkungen auf Ihr Unternehmen haben wird. Das Ziel von Sicherheitsmaßnahmen ist es, die drei Elemente der Sicherheit zu gewährleisten, nämlich *die Verfügbarkeit, Integrität und Vertraulichkeit* der von Ihrem Unternehmen angebotenen Vorgänge, Dienstleistungen und Produkte.

	Verfügbarkeit sicherstellen	Gewährleistung der Integrität	Gewährleistung der Vertraulichkeit
Ziel	<p>Verhinderung von Betriebsunterbrechungen bei Produktionsanlagen</p> 	<p>Verhinderung von Ausfällen der Produktionsanlagen aufgrund unbefugter Überschreibung von Einstellungen und Daten</p> 	<p>Verhinderung der Offenlegung wichtiger Informationen wie Produktions-Know-how und Steuerungsprogramme</p> 
Auswirkungen im Falle einer Kompromittierung	<ul style="list-style-type: none"> • Unterbrechung des Geschäftsbetriebs • Lieferverzögerungen • Erhöhte Kosten 	<ul style="list-style-type: none"> • Qualitätsminderung • Verminderte Sicherheit • Negative Auswirkungen auf die Gesundheit • Negative Auswirkungen auf die Umwelt 	<ul style="list-style-type: none"> • Schädigung des sozialen Vertrauens • Verlust von Wettbewerbsvorteilen • Verstoß gegen Gesetze und Vorschriften

Die Schwere der Auswirkungen in Bezug auf *Verfügbarkeit, Integrität* und *Vertraulichkeit* hängt von der Branche, den angebotenen Dienstleistungen und Produkten sowie den zu schützenden Vermögenswerten ab. So variiert beispielsweise das wichtige Sicherheitselement je nach Branche. Darüber hinaus variiert es selbst innerhalb derselben Branche je nach Geschäftsrolle und Prozess. Es ist wichtig, sorgfältig zu überlegen, auf welches Element sich Ihr Unternehmen konzentrieren sollte, und entsprechende Sicherheitsmaßnahmen zu fördern.

Industrie	Zu betonendes Element und Begründung	
Automobil	Schwerpunkt <u>Verfügbarkeit</u>	• Selbst eine kurze Betriebsunterbrechung hat erhebliche Auswirkungen auf Wirtschaft und Gesellschaft.
Infrastruktur	Betonung der <u>Verfügbarkeit</u>	• Selbst kurze Betriebsunterbrechungen haben erhebliche Auswirkungen auf Gesellschaft und Umwelt.
Lebensmittel und Medizin	Schwerpunkt auf <u>Integrität</u>	• Fehlerhafte Produktion hat erhebliche Auswirkungen auf die Gesundheit und Sicherheit der Nutzer.
Gerätehersteller (die Auswirkungen variieren je nach Gerät)	Schwerpunkt <u>Verfügbarkeit</u>	• Selbst eine kurze Betriebsunterbrechung hat erhebliche Auswirkungen auf die Gesellschaft und die Umwelt.
	Schwerpunkt auf <u>Integrität</u>	• Fehlerhafte Produktion hat erhebliche Auswirkungen auf die Gesundheit und Sicherheit der Nutzer.
	Schwerpunkt auf <u>Vertraulichkeit</u>	• Das Durchsickern von Know-how über Geräte hat erhebliche Auswirkungen auf das Geschäft.

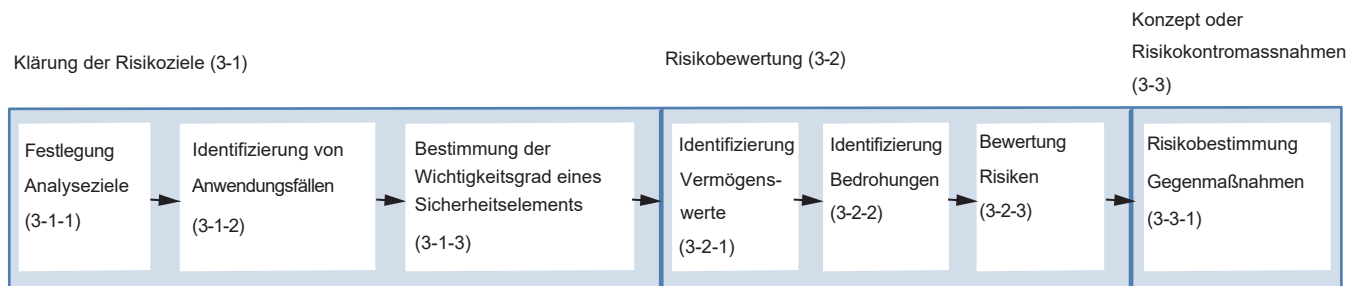
2-2-2 Verfahren zur Risikobewertung

Um einen Konsens über Sicherheitsmaßnahmen zu erzielen, ist es wichtig, eine Risikobewertung durchzuführen, um sicherheitsrelevante Risiken zu klären. Bei der Risikobewertung muss der Kunde Maßnahmen berücksichtigen, die auf der Unternehmensumgebung, den einzuhaltenden Gesetzen und Vorschriften sowie den neuesten Trends bei Bedrohungen basieren. Indem Sie vorrangig auf Bedrohungen reagieren, die ein größeres Risiko für Ihr Unternehmen darstellen, können Sie die Kosteneffizienz Ihrer Sicherheitsmaßnahmen maximieren.

Die Risikobewertung ist der erste Schritt, den Sie für eine angemessene Sicherheitsreaktion unternehmen sollten. Dabei handelt es sich um eine Maßnahme zur Identifizierung von Bedrohungen für das zu schützende System oder das Unternehmen (einschließlich Betrieb und Dienstleistungen), in dem das System verwendet oder betrieben wird, und zur Bewertung der Risiken auf der Grundlage des Ausmaßes der Auswirkungen und der Wahrscheinlichkeit des Eintretens von Schäden, die durch die Bedrohungen verursacht werden.

Die Durchführung einer solchen Risikobewertung ist sowohl für Fabrikbesitzer als auch für Gerätehersteller in vielen Sicherheitsvorschriften und internationalen Normen, wie z. B. IEC 62443, vorgeschrieben. Da die Methoden der Risikobewertung jedoch sehr unterschiedlich sind, ist es notwendig, geeignete Methoden entsprechend den tatsächlichen Gegebenheiten der Organisation (z. B. zu verwaltende Systeme, Produkte und organisatorische Fähigkeiten) auszuwählen oder zu kombinieren.

Führen Sie Risikobewertungen im FA-System gemäß dem folgenden Verfahren durch.



Die konkrete Umsetzung der einzelnen Verfahren wird im nächsten Abschnitt erläutert.

3

Durchführung der Risikobewertung

In diesem Abschnitt wird die Umsetzung der Risikobewertung in einem FA-System ausführlich erläutert.

3

3-1	Klärung der Risikoziele	3-2
3-1-1	Festlegung der Analyseziele.....	3-2
3-1-2	Identifizierung von Anwendungsfällen.....	3-3
3-1-3	Festlegen der Wichtigkeitsebene einer Sicherheitszone.....	3-3
3-2	Risikobewertung	3-5
3-2-1	Identifizierung von Vermögenswerten.....	3-5
3-2-2	Identifizierung von Bedrohungen.....	3-6
3-2-3	Risiken bewerten.....	3-7
3-3	Konzept der Risikominderungsmaßnahmen	3-9
3-3-1	Festlegung von Risikominderungsmaßnahmen.....	3-9
3-3-2	Maßnahmen, die während des gesamten Lebenszyklus zu ergreifen sind.....	3-9
3-3-3	Sicherheit durch Design.....	3-10
3-3-4	Tiefgreifende Verteidigung.....	3-10

3-1 Klärung der Risikoziele

Klärung der Risikoziele, um eine Risikobewertung durchzuführen.

3-1-1 Festlegung der Analyseziele

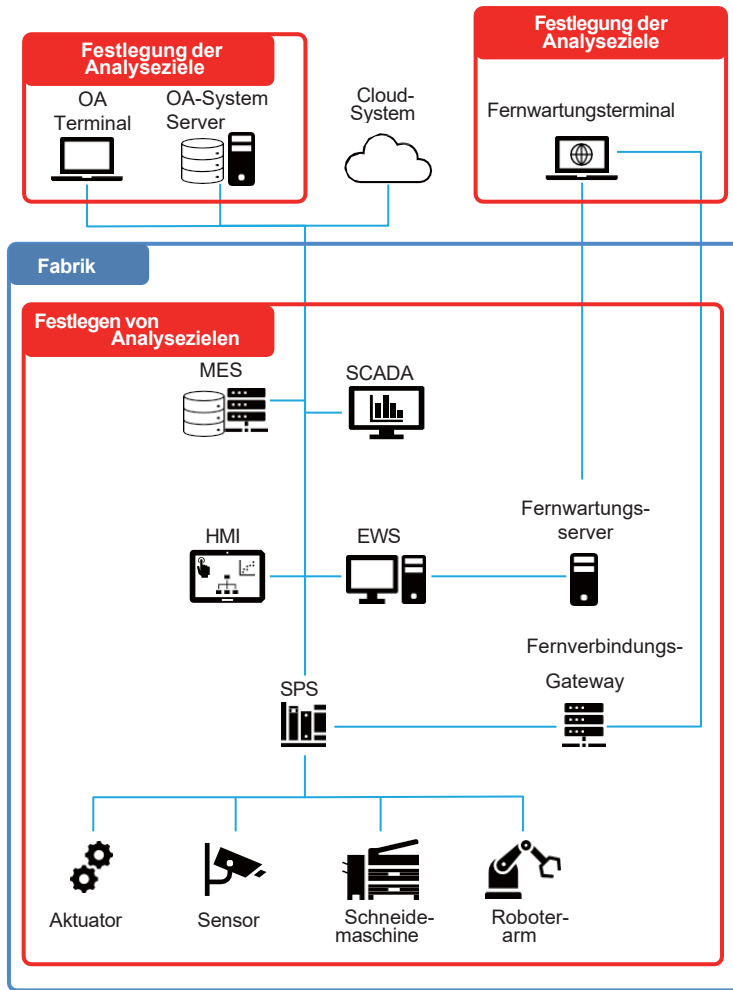
Der erste Schritt im Risikobewertungsprozess besteht darin, die zu bewertenden Zielsysteme festzulegen. Grundsätzlich sollte der Umfang alle Systeme umfassen, die mit dem Geschäft und den Dienstleistungen der Organisation sowie den Geschäftsstandorten, an denen die Organisation tätig ist, in Zusammenhang stehen.

Bei der Festlegung der Analyseziele sollten Sie folgende Perspektiven berücksichtigen.

- Umfang der Organisation und der Geschäftsstandorte (z. B. Fabriken)
- Umfang der Systeme (z. B. IT-Systeme und Produktionsmanagementsysteme)

Nest, klären Sie die Konfiguration der festgelegten Analysezielsysteme. Erstellen Sie eine Liste der Netzwerke, Geräte und Rollen, aus denen das System besteht. Durch das Erlernen der Systemkonfiguration ist es möglich, die Bedingungen (Angriffsmethoden, Pfade usw.) abzuleiten, unter denen Bedrohungen sichtbar werden, und umfassende Gegenmaßnahmen dafür zu entwickeln. Um die Systemkonfiguration zu klären, sollten die folgenden Elemente berücksichtigt werden.

- FA-System, Platzierung der Geräte im Netzwerk und Rollen der Geräte
- Netzwerkkonfiguration
- Physische Bereichszonierung für jedes System
- Bereits vorhandene Cybersicherheitsmaßnahmen



3-1-2 Identifizierung von Anwendungsfällen

Um die mit einem FA-System verbundenen Sicherheitsrisiken zu erfassen und deren Schweregrad zu bewerten, müssen die Anwendungsfälle des FA-Systems (d. h. die durch den Betrieb des FA-Systems ausgeführten Aktivitäten) identifiziert werden.

Durch die richtige Ableitung von Anwendungsfällen ist es möglich, die für Ihr Unternehmen wichtigen Vorgänge und Dienste, die durch das FA-System realisiert werden, zu klären und die Risiken im Falle einer Beeinträchtigung richtig einzuschätzen.

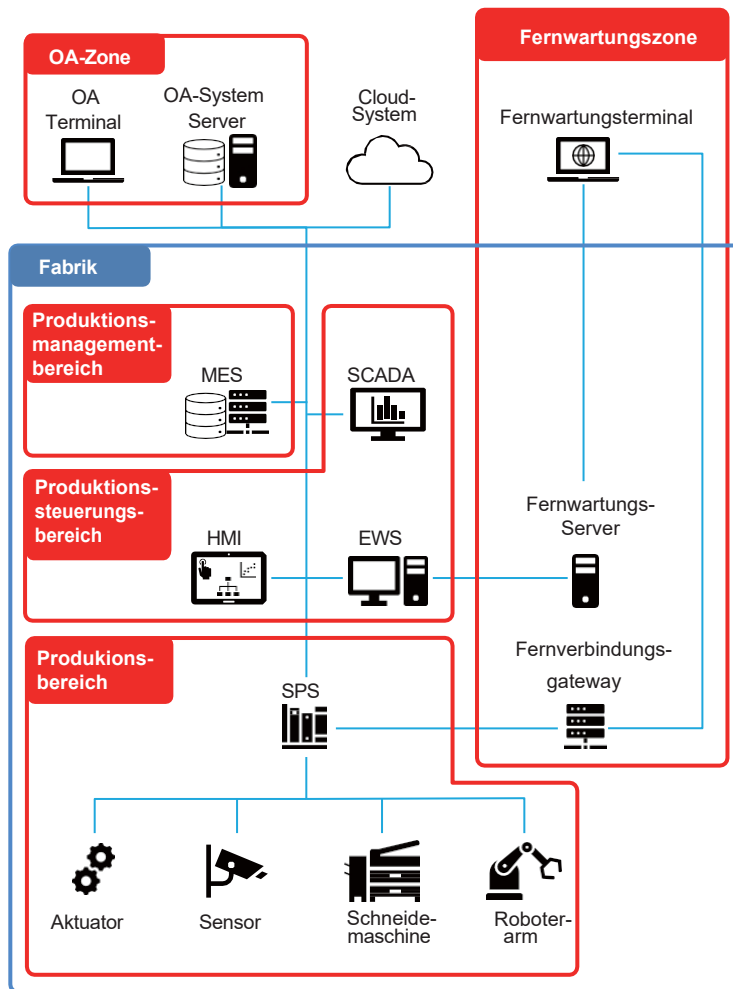
Berücksichtigen Sie bei der Ableitung von Anwendungsfällen die folgenden Aspekte.

Perspektiven für die Ableitung	Wichtige Punkte bei der Ableitung
Inhalt der Abläufe und Dienstleistungen	<ul style="list-style-type: none"> Durch das Geschäft und die Dienstleistungen erreichte Ziele (Status und Output) Spezifische Arbeitsinhalte
Personen, die Tätigkeiten und Dienstleistungen ausführen	<ul style="list-style-type: none"> Die Person in der Organisation/im Subunternehmen, die die Arbeit ausführt Rolle der oben genannten Person
Systeme und Daten im Zusammenhang mit Tätigkeiten und Dienstleistungen	<ul style="list-style-type: none"> Geräte und Systeme, die zur Ausführung der Vorgänge verwendet werden Von den oben genannten Geräten und Systemen verarbeitete Daten

3-1-3 Bestimmung des Wichtigkeitsgrades einer Sicherheitszone

Klassifizieren Sie die Bereiche im FA-System anhand der Inhalte und der Wichtigkeit der Vorgänge in Gruppen, die ein gleichwertiges Maß an Sicherheitsmaßnahmen erfordern. Dies wird als Definition von Sicherheitszonen bezeichnet.

Durch die Definition von Sicherheitszonen ist es möglich, die Bereiche zu identifizieren, in denen Sicherheitsmaßnahmen vorrangig umgesetzt werden sollten, was eine effiziente Umsetzung der Sicherheitsmaßnahmen ermöglicht.



Legen Sie die Sicherheitsstufe für jede Sicherheitszone fest. Die „Sicherheitsstufe“ bezieht sich auf das Ziel der Sicherheitsmaßnahmen, die zum Schutz der in der definierten Sicherheitszone durchgeführten Vorgänge und der dort verwendeten Anlagen erforderlich sind. Die in IEC 62443 definierten Sicherheitsstufen und angenommenen Angreiferprofile sind in der folgenden Tabelle aufgeführt.

Sicherheitsstufe (SL)	Profil des angenommenen Angreifers	Definition
SL0	Keine	Keine besonderen Anforderungen oder Sicherheitsvorkehrungen erforderlich
SL1	Mitarbeiter	Schutz vor unbeabsichtigten oder versehentlichen Verstößen
SL2	Script Kiddies (Angreifer, die allgemein verfügbare Angriffstools verwenden)	Schutz vor vorsätzlichen Angriffen mit einfachen Mitteln, geringen Ressourcen, allgemeinen Fähigkeiten und geringer Motivation
SL3	Professionelle Hacker Insider und ehemalige Mitarbeiter	Schutz vor vorsätzlichen Angriffen mit ausgefeilten Mitteln, mit moderaten Ressourcen, spezifischen Kenntnissen über Steuerungssysteme und moderater Motivation
SL4	Staatlich geförderte Cyberterroristen	Schutz vor vorsätzlichen Angriffen mit ausgeklügelten Mitteln, umfangreichen Ressourcen, spezifischen Kenntnissen über Steuerungssysteme und hoher Motivation.

3-2 Risikobewertung

Identifizieren Sie Bedrohungen für die zu schützenden Vermögenswerte und bewerten Sie das Risiko dieser Bedrohungen.

3-2-1 Identifizieren von Vermögenswerten

Um die zu berücksichtigenden Sicherheitsrisiken und die in einer Risikobewertung zu implementierenden Maßnahmen richtig auszuwählen, definieren Sie die *zu schützenden Vermögenswerte* Ihres Unternehmens.

Zu schützende Vermögenswerte sind Geräte und Daten, deren Verlust der drei Sicherheitselemente (d. h. Verfügbarkeit, Integrität und Vertraulichkeit) durch Cyberangriffe zu Schäden für Ihr Unternehmen oder Ihre Kunden führen könnte. Daher sollten Sie selbst bestimmen, welche Vermögenswerte wertvoll sind.

Auflistung der Vermögenswerte

Identifizieren Sie die physischen Vermögenswerte, Informationsvermögenswerte und funktionalen Vermögenswerte, die in der definierten Systemkonfiguration vorhanden sind, und listen Sie sie als Vermögenswerte des Systems auf. Bei der Ableitung von Vermögenswerten können Sie diese aus verschiedenen Perspektiven analysieren (Vermögenswerteklassifizierung). Um die Analyse zu optimieren, können Sie diese Klassifizierung außerdem nutzen, um die Anzahl der zu analysierenden Vermögenswerte zu reduzieren, indem Sie Vermögenswerte mit gleichen technischen Eigenschaften und gleichem Wichtigkeitsgrad bei Bedarf zusammenfassen.

Beispiele für Arten von Vermögenswerten sind wie folgt.

- Physische Vermögenswerte: Controller, Server, PCs usw.
- Informationsanlagen: Anwenderprogramme, Rezepturdaten, Protokollinformationen usw.
- Funktionale Vermögenswerte: Steuerungsfunktionen, Sicherheitsfunktionen usw.

Bewertung der Wichtigkeit von Vermögenswerten

Bewerten Sie die Bedeutung der Vermögenswerte für die Wirtschaft aus verschiedenen Perspektiven, z. B. unter Berücksichtigung des wirtschaftlichen Schadens, der Auswirkungen auf die Sicherheit und der Unterbrechung des Systembetriebs. Wenn ein Angriff beispielsweise nur einen geringen finanziellen Schaden verursacht, kann er als geringfügige Auswirkung bewertet werden, während ein Angriff, der zu einer langfristigen Unterbrechung des Fabrikbetriebs führt, als erhebliche Auswirkung bewertet werden kann.

Bei den Bewertungskriterien ist es wichtig, verschiedene Perspektiven zu berücksichtigen, beispielsweise die Auswirkungen auf die Fortführung der Produktionstätigkeiten, wirtschaftliche Verluste und die Auswirkungen auf die Gesundheit, Sicherheit und Umwelt der Fabrik. Sie sollten anhand der Situation Ihres Unternehmens entscheiden, welche Perspektive Sie einnehmen möchten.

Die folgende Tabelle zeigt ein Beispiel für die Bewertung der Wichtigkeit aus verschiedenen Sicherheitsperspektiven.

Bewertungswert	Bewertungskriterien
3	<ul style="list-style-type: none"> • Wenn die Anlage angegriffen wird, besteht die Gefahr eines Systemausfalls von einer Woche oder länger. • Wenn Informationen aus dem Vermögenswert nach außen dringen, besteht ein Verlustrisiko von 500 Millionen Yen oder mehr. • Wenn die Anlage angegriffen wird, besteht die Gefahr, dass Mitarbeiter ums Leben kommen.

Bewertungswert	Bewertungskriterien
2	<ul style="list-style-type: none"> • Wenn die Anlage angegriffen wird, besteht das Risiko eines Systemausfalls von 24 Stunden oder mehr, jedoch weniger als einer Woche. • Wenn Informationen aus dem Vermögenswert nach außen gelangen, besteht ein Verlustrisiko von 5 Millionen Yen oder mehr, jedoch weniger als 500 Millionen Yen. • Wenn die Anlage angegriffen wird, besteht die Gefahr schwerer Verletzungen von Mitarbeitern.
1	<ul style="list-style-type: none"> • Selbst wenn ein Vermögenswert angegriffen wird, besteht kein Risiko eines Systemausfalls von 24 Stunden oder mehr. • Wenn Informationen aus dem Vermögenswert nach außen gelangen, besteht kein Risiko eines Verlusts von 5 Millionen Yen oder mehr. • Wenn die Anlage angegriffen wird, besteht keine Gefahr schwerer Verletzungen für die Mitarbeiter.

3-2-2 Identifizierung von Bedrohungen

Es ist notwendig, Bedrohungen zu identifizieren, die die Anlage gefährden könnten, sowie Bedrohungen in Verbindung mit Cyberangriffsmethoden, mit denen diese realisiert werden können. Identifizieren Sie die Bedrohungen umfassend, da dies eine wichtige Maßnahme ist, um angemessene Ziele für Sicherheitsmaßnahmen festzulegen.

Auflisten von Bedrohungen

Identifizieren Sie Bedrohungen für die zu schützenden Vermögenswerte und die Auswirkungen auf die Produktion und das Geschäft, wenn diese Bedrohungen eintreten. Beispiele sind in der folgenden Tabelle aufgeführt.

Asset	Bedrohung	Auswirkungen auf Produktion und Geschäftstätigkeit
Steuerung	Diebstahl des Controllers	<ul style="list-style-type: none"> • Verzögerungen bei der Produktlieferung aufgrund von Produktionsausfällen • Schäden durch Zerstörung von Ausrüstung
Anwenderprogramm	Manipulation von Anwenderprogrammen durch Anschluss eines von außen mitgebrachten Computers	<ul style="list-style-type: none"> • Mangelhafte Qualität und daraus resultierender Imageschaden • Personenschäden aufgrund von Gerätefehlfunktionen
Produktionsrezeptdaten	Verlust von Produktionsrezeptdaten	<ul style="list-style-type: none"> • Verringerung der Wettbewerbsfähigkeit
Benutzereinstellungen	Manipulation der Zugriffskontroll-Einstellungen	<ul style="list-style-type: none"> • Verlust von Know-how durch illegalen Zugriff
Kontrollfunktion	Ausfall der Steuerungsfunktion aufgrund eines Bedienungsfehlers	<ul style="list-style-type: none"> • Verzögerungen bei der Produktlieferung aufgrund von Produktionsausfällen
...

Verschiedene Methoden zur Analyse von Bedrohungen und Angriffsmethoden werden von Branchen, Standards usw. definiert und weisen unterschiedliche Merkmale auf. Um die Qualität der Analyse sicherzustellen, sollten Sie anerkannte Analysemethoden und -rahmenwerke richtig einsetzen und sich mit den Branchenstandards in Bezug auf Ihre Organisation und den Umfang der Analyse vertraut machen.

Beispiele für Analysemethoden sind in der folgenden Tabelle aufgeführt.

Analysemethode	Übersicht
STRIDE	Eine Methode zur Ableitung von Bedrohungen aus den folgenden sechs Leitwörtern, basierend auf der Absicht des Angreifers <ul style="list-style-type: none"> • Spoofing • Manipulation • Leugnung • Offenlegung von Informationen • Denial of Service • Erweiterung von Berechtigungen
Angriffsbaum-Analyse	Verfahren zum Zerlegen und Verdeutlichen des Konfigurationselements einer Angriffsmethode in einem Baumdiagramm

Bewertung der Wahrscheinlichkeit des Eintretens einer Bedrohung

Die Wahrscheinlichkeit des Auftretens einer Bedrohung kann anhand von Indikatoren wie der Schwierigkeit, das für den Angriff erforderliche Wissen und die Technologie zu erwerben, dem Zeitpunkt, zu dem der Angriff durchgeführt werden kann, und der für die Durchführung des Angriffs erforderlichen Zeit bewertet werden. Wenn beispielsweise Angriffsmethoden gegen Schwachstellen von Geräten allgemein bekannt sind und Angriffe jederzeit durchgeführt werden können, sind Angriffe einfach und die Wahrscheinlichkeit des Auftretens einer Bedrohung hoch.

Im Folgenden finden Sie Beispiele für Metriken zur Wahrscheinlichkeit von Bedrohungen.

Wahrscheinlichkeit des Eintretens	Für einen Angriff erforderliche Kenntnisse und Technologien (Werkzeuge usw.)	Erforderliche Zeit und Gelegenheit für einen Angriff
3	<ul style="list-style-type: none"> • Es sind keine Fachkenntnisse erforderlich. • Die erforderliche Technologie ist leicht zu beschaffen. 	<ul style="list-style-type: none"> • Der Zeitaufwand ist gering. • Angriffe können jederzeit durchgeführt werden.
2	<ul style="list-style-type: none"> • Ein gewisses Maß an Fachwissen ist erforderlich. • Die erforderliche Technologie ist bis zu einem gewissen Grad schwer zu beschaffen. 	<ul style="list-style-type: none"> • Der Zeitaufwand ist mittelgroß. • Die Angriffsmöglichkeiten sind begrenzt.
1	<ul style="list-style-type: none"> • Fachwissen ist erforderlich. • Die erforderliche Technologie ist schwer zu beschaffen. 	<ul style="list-style-type: none"> • Der Zeitaufwand ist hoch. • Es gibt nur wenige Angriffsmöglichkeiten.

Bewertung des Ausmaßes der Bedrohung

Bewerten Sie, inwieweit Ihr System betroffen ist, wenn die Sicherheit (Verfügbarkeit, Integrität und Vertraulichkeit) beeinträchtigt ist. Ein Beispiel für Kriterien zur Bewertung der Auswirkungen von Bedrohungen ist unten aufgeführt.

Ausmaß der Bedrohung	Bewertungskriterien
3	Die Auswirkungen der Bedrohung betreffen das gesamte System.
2	Die Auswirkungen der Bedrohung sind auf das System beschränkt.
1	Die Bedrohung hat keine Auswirkungen.

3-2-3 Risikobewertung

Bewerten Sie Sicherheitsrisiken, um zu entscheiden, ob Sicherheitsmaßnahmen gegen die identifizierte Bedrohung umgesetzt werden sollen und welche Priorität diese Maßnahmen haben. Sicherheitsrisiken können bewertet werden, indem die *Bedeutung der Ressource*, die *Wahrscheinlichkeit des Eintretens* einer Bedrohung und das *Ausmaß der Bedrohung* bei ihrem Eintreten miteinander multipliziert werden.



Berechnen Sie den umfassenden Sicherheitsrisikobewertungswert anhand von drei Elementen, nämlich der Bedeutung der Anlage, der Wahrscheinlichkeit des Auftretens einer Bedrohung und dem Ausmaß der Bedrohung. Wenn beispielsweise eine Schwachstelle, die zu einer Produktionsunterbrechung führen könnte, in einem Steuergerät (SPS) verbleibt (d. h. die Bedrohung ist groß) und die Angriffsmethode für die Schwachstelle allgemein bekannt ist (d. h. die Wahrscheinlichkeit des Auftretens ist hoch), kann das Sicherheitsrisiko als hoch eingestuft werden.

Die folgende Tabelle enthält Beispiele für Bewertungskriterien zur Ermittlung von Risikobewertungswerten.

Wichtigkeitsgrad der Anlage	Wahrscheinlichkeit des Auftretens	Ausmaß der Bedrohung	Risikobewertungswert	Beurteilungsbedingungen
3	3	3	A	Wichtigkeitsgrad des Vermögenswerts: 3 Bedrohung × Eintrittswahrscheinlichkeit: 6 bis 9
3	2	3		
3	3	2		
3	2	2	B	Wichtigkeitsgrad des Vermögenswerts: 3 Bedrohung × Eintrittswahrscheinlichkeit: 3 bis 5
3	1	3		
3	3	1		
2	3	3		
2	2	3		
2	3	2	C	Wichtigkeitsgrad des Vermögenswerts: 2 Bedrohung × Eintrittswahrscheinlichkeit: 6 bis 9
3	1	2		
3	2	1		
3	1	1		
2	2	2		
2	1	3		
2	3	1		
1	3	3	D	Wichtigkeitsgrad des Vermögenswerts: 1 Bedrohung × Wahrscheinlichkeit des Eintretens: 7 bis 9
2	1	2		
2	2	1		
2	1	1		
1	2	3		
1	3	2		
1	2	2		
1	1	3		
1	1	3	E	Wichtigkeitsgrad des Vermögenswerts: 2 Bedrohung × Wahrscheinlichkeit des Eintretens: 1 bis 2
1	3	1		
1	1	2		
1	2	1		
1	1	1		
1	1	1	E	Wichtigkeitsgrad des Vermögenswerts: 1 Bedrohung × Eintrittswahrscheinlichkeit: 4 bis 6
1	3	1		
1	1	2		
1	2	1		
1	1	1		

3-3 Konzept der Risikominderungsmaßnahmen

Erwägen Sie spezifische Sicherheitsmaßnahmen gegen Bedrohungen. Beachten Sie auch, dass die Optimierung einzelner Sicherheitsmaßnahmen dazu führen kann, dass diese unzureichend sind. Daher ist es wichtig, umfassende Maßnahmen zu erwägen, die die vier in diesem Abschnitt vorgestellten Perspektiven berücksichtigen:

Risikominderungsmaßnahmen, Maßnahmen, die während des gesamten Lebenszyklus zu ergreifen sind, Sicherheit durch Design und tiefgreifende Verteidigung.

3-3-1 Festlegung von Risikominderungsmaßnahmen

Bestimmen Sie, ob Gegenmaßnahmen gegen Risiken erforderlich sind.

Je nach Sicherheitsstufe der Sicherheitszone sind unterschiedliche Maßnahmen erforderlich. Zonen mit hoher Sicherheitsstufe erfordern Gegenmaßnahmen gegen Bedrohungen mit niedrigen Risikobewertungswerten. Andererseits kann festgelegt werden, dass in Zonen mit niedriger Sicherheitsstufe nur für diejenigen mit hohen Risikobewertungswerten Gegenmaßnahmen ergriffen werden sollten.

Die folgende Tabelle enthält ein Beispiel für die Festlegung der Sicherheitsstufe und des Umfangs der Maßnahmen.

Sicherheitsstufe (SL)	Umfang der Maßnahmen
SL0	Ergreifen Sie Gegenmaßnahmen gegen Risiken von A.
SL1	Ergreifen Sie Gegenmaßnahmen gegen die Risiken A und B.
SL2	Ergreifen Sie Gegenmaßnahmen gegen die Risiken A, B und C.
SL3	Ergreifen Sie Gegenmaßnahmen gegen die Risiken A, B, C und D.
SL4	Ergreifen Sie Gegenmaßnahmen gegen die Risiken A, B, C, D und E.

Teilen Sie die Gegenmaßnahmen gegen Sicherheitsrisiken in die folgenden Kategorien ein.

- Vermeiden: Maßnahmen zur Beseitigung der Ursache einer Bedrohung, z. B. die Entfernung einer Funktion, die ein Risiko darstellt.
- Milderung: Maßnahme zur Verringerung der Wahrscheinlichkeit und der Auswirkungen eines Risikos, z. B. Hinzufügen einer Sicherheitsfunktion
- Transfer: Maßnahme zur Übertragung des Risikos auf eine andere Organisation, z. B. durch Auslagerung des Systembetriebs
- Akzeptieren: Maßnahme zur Akzeptanz des Risikos ohne Ergreifen spezifischer Maßnahmen

3-3-2 Maßnahmen, die während des gesamten Lebenszyklus zu ergreifen sind

Um die Sicherheit von FA-Systemen zu verbessern, muss die Sicherheit während des gesamten Lebenszyklus der FA-Systeme berücksichtigt werden. Die folgende Tabelle gibt einen Überblick über den Lebenszyklus eines FA-Systems und die Sicherheitsmaßnahmen, die in jeder Phase umgesetzt werden sollten.

Lebenszyklus eines FA-Systems	Hauptaktivitäten und Rollenverteilung
Entwurf und Inbetriebnahme	<ul style="list-style-type: none"> • Fabrikbesitzer: Entwicklung von Risikokontrollmaßnahmen für Produktionslinien und Sicherheitsvorschriften • Systemintegrator und Gerätehersteller: Implementierung von Risikominderungsmaßnahmen (Sicherheitsfunktionen) in Geräten und Bereitstellung eines Leitfadens für die sichere Verwendung der Geräte
Betrieb	<ul style="list-style-type: none"> • Fabrikbesitzer: Überwachung des Status der Produktionslinie und der Einhaltung der im Entwurfsprozess festgelegten Sicherheitsvorschriften • Systemintegrator: Überwachen Sie Schwachstelleninformationen von Geräten und wenden Sie Sicherheitsregeln an • Gerätehersteller: Offenlegung von Informationen zu Sicherheitslücken von Geräten

Lebenszyklus eines FA-Systems	Hauptaktivitäten und Rollenverteilung
Wartung	<ul style="list-style-type: none"> • Fabrikbesitzer: Überprüfen Sie die Kontoinformationen, kontrollieren Sie die Audit-Protokolle und aktualisieren Sie die Geräte • Systemintegrator: Aktualisierung der Geräte • Gerätehersteller: Empfehlungen zur Kontoverwaltung und Verfahren zur Aktualisierung der Software (Sicherheitspatches) bereitstellen
Entsorgung	<ul style="list-style-type: none"> • Fabrikbesitzer und Systemintegrator: Löschen Sie vertrauliche Informationen von den Geräten • Gerätehersteller: Anweisungen zur sicheren Entsorgung der Geräte bereitstellen

3-3-3 Sicherheit durch Design

Sicherheit durch Design bezieht sich auf das Konzept, Verzögerungen aufgrund von Nacharbeiten während der Entwicklung zu reduzieren, die Einführungs- und Betriebskosten von Sicherheitsmaßnahmen zu senken und die Wartbarkeit von Sicherheitssystemen zu verbessern, indem bereits in einer frühen Phase des Lebenszyklus eines FA-Systems ein sicherheitsbewusster Ansatz verfolgt wird.

Um das Konzept von Secure by Design zu verwirklichen, definieren Sie Sicherheitsanforderungen auf der Grundlage der Ergebnisse der Risikobewertung und konstruieren Sie ein FA-System unter Verwendung etablierter sicherer Konstruktionsprinzipien.

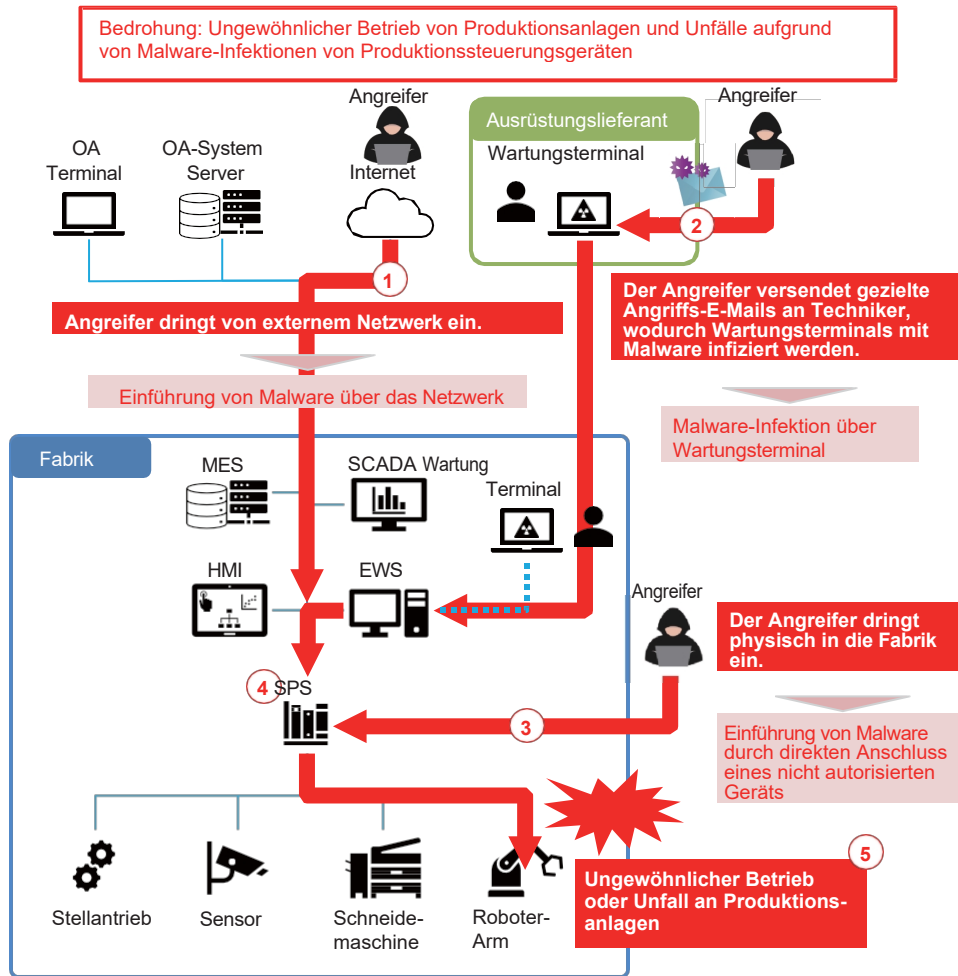
Prinzip	Beschreibung
Secure by Default (Sicherheit durch Standardeinstellungen gewährleisten)	Stellen Sie ein FA-System oder Geräte, aus denen ein FA-System besteht, für die sichere Verwendung mit den Standardeinstellungen bereit.
Sicherheit basierend auf den Systemmerkmalen	Implementieren Sie Sicherheitsmaßnahmen ohne Über- oder Unterversorgung auf der Grundlage der Systemmerkmale, der Wichtigkeit usw., anstatt einheitliche Sicherheitsmaßnahmen für alle Systeme zu implementieren.
Ausgewogenheit zwischen Sicherheit und Komfort	Erreichen Sie gleichzeitig Komfort und erhöhte Sicherheit mit einem System, das auf das Ziel einer „positiven Summe“ abzielt, von der beide Seiten profitieren.
Offenes Design (Vermeidung von Sicherheit durch Verschleierung)	Wenn Sicherheitsmaßnahmen durch verdeckte Design- und Implementierungsinformationen beeinträchtigt werden, gibt es im Falle einer Informationsleckage möglicherweise keine wirksame Abwehrmethode. Verwenden Sie daher bekannte und bewährte sichere Technologien und Methoden, um die Sicherheitsmaßnahmen zu verstärken.
Ausfallsicherheit	Entwerfen Sie ein System so, dass die Sicherheit auch dann gewährleistet ist, wenn ein bestimmtes Gerät, das zur Sicherheit beiträgt, ausfällt oder nicht mehr funktioniert.
Funktionale Trennung und minimale Funktionalität	Beschränken Sie die Funktionen von FA-Systemen auf das aus Sicht des Sicherheitsrisikos erforderliche Minimum, wobei jede Funktion von den anderen getrennt ist (mit begrenzten Abhängigkeiten).
Trennung von Berechtigungen und geringstmögliche Berechtigungen	Vergeben Sie Privilegien im FA-System in minimalen Einheiten, wobei jedes Privileg einer minimalen Anzahl von Benutzern gewährt wird.
End-to-End-Sicherheit	Stellen Sie die Sicherheit sicher, indem Sie die Integrität der zu schützenden Daten über die Kommunikationswege hinweg überprüfen.

3-3-4 Tiefgreifende Verteidigung

Bei der Betrachtung von Sicherheitsmaßnahmen ist es wichtig, mehrere verschiedene Sicherheitsmaßnahmen hierarchisch zu kombinieren, von der Festlegung von Unternehmensrichtlinien und -regeln bis hin zur Implementierung von Ein- und Ausgangs-Kontrollen gegen physisches Eindringen in die Fabrik und Maßnahmen zum Schutz der Geräte, aus denen das Fabriknetzwerk und die Systeme bestehen, um eine robuste Sicherheit zu erreichen.

Wie in der folgenden Abbildung dargestellt, gibt es selbst für eine einzelne Bedrohung (z. B. ungewöhnlicher Betrieb oder Ausfall von Produktionsgeräten aufgrund einer Malware-Infektion eines Produktionssteuerungsgeräts) eine Vielzahl von Angriffsmethoden. Um die Sicherheit zu gewährleisten, müssen Sie daher nicht nur technische Maßnahmen für die

Systeme, sondern auch Maßnahmen gegen Risiken für *die Personen*, die die Systeme nutzen, und gegen das Risiko von Angreifern *physisches* Eindringen in Bereiche, in denen sich die Geräte befinden.



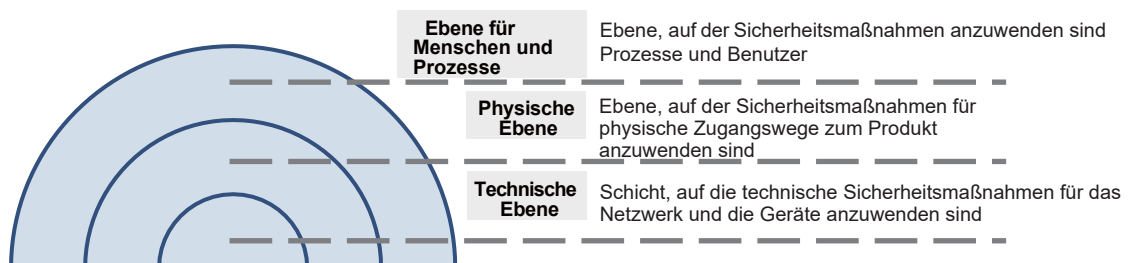
3-3 Konzept der Risikominderungsmaßnahmen

3

3-3-4 Tiefenverteidigung

Basierend auf diesem Konzept wird die Kombination mehrerer Maßnahmen zur Erreichung einer robusten Sicherheit als „Defense in Depth“ bezeichnet. In diesem Leitfaden werden die mehrschichtigen Sicherheitsmaßnahmen wie folgt definiert.

- Sicherheitsmaßnahmen für Organisationen und Personen (Maßnahmen auf der Ebene der Menschen und Prozesse)
- Sicherheitsmaßnahmen gegen physisches Eindringen und Kontakt (Maßnahmen auf physischer Ebene)
- Sicherheitsmaßnahmen für Netzwerke und Geräte (Maßnahmen auf technischer Ebene)



Die folgende Tabelle zeigt die Klassifizierung von Sicherheitsmaßnahmen gegen die oben genannten Beispiele für Bedrohungen und Angriffe aus drei Perspektiven, nämlich *Menschen*, *physisch* und *technisch*.

Angriffsmethode und Schaden	Maßnahmen im Zusammenhang mit Menschen	Physische Maßnahmen	Technische Maßnahmen
1 Der Angreifer nutzt eine fehlerhafte FW-Konfiguration aus, um von einem externen Netzwerk aus einzudringen	Durchführung von Sicherheitsschulungen (FW-Konfiguration und -Betrieb)	-	Einführung von Firewalls Schnittstellen mit externen Netzwerken
2 Angreifer versendet gezielte Angriffs-E-Mails an Techniker, wodurch Wartungsterminals mit Malware infiziert werden.-	Durchführung von Sicherheitsschulungen (gezielte Angriffs-E-Mails, Wartungsarbeiten)	Kontrolle mitgebrachter Geräte und Sicherheitsüberprüfung	
3 Angreifer dringt physisch in die Fabrik ein.	Durchführung von Sicherheitsschulungen (Zugangs- und Ausgangskontrolle)	Zugangs- und Ausgangskontrolle für Fabriken und Bereiche, in denen die Geräte installiert sind	Zulassung von Verbindungen nur zu legitimen Geräten (Geräteüberprüfung)
4 Produktionsanlagen sind mit Malware infiziert.	-	-	Überprüfung der Eingabedaten für Geräte
5 Ungewöhnlicher Betrieb oder Unfall an Produktionsanlagen.	-	-	Einführung von Anti-Malware-Software
			Erkennen von Gerätefehlern (Temperatur usw.)

Die Sicherheitsmaßnahmen werden im nächsten Abschnitt beschrieben.

4

Sicherheitsmaßnahmen

In diesem Abschnitt werden die Sicherheitsmaßnahmen in FA-Systemen beschrieben.

4

4-1	Bedrohungen für FA-Systeme	4-2
4-2	Sicherheitsmaßnahmen in FA-Systemen	4-3
4-2-1	Sicherheitsmaßnahmen für die Mensch- und Prozessebene	4-4
4-2-2	Sicherheitsmaßnahmen für die physische Ebene	4-6
4-2-3	Sicherheitsmaßnahmen für die technische Ebene	4-6

4-1 Bedrohungen für FA-Systeme

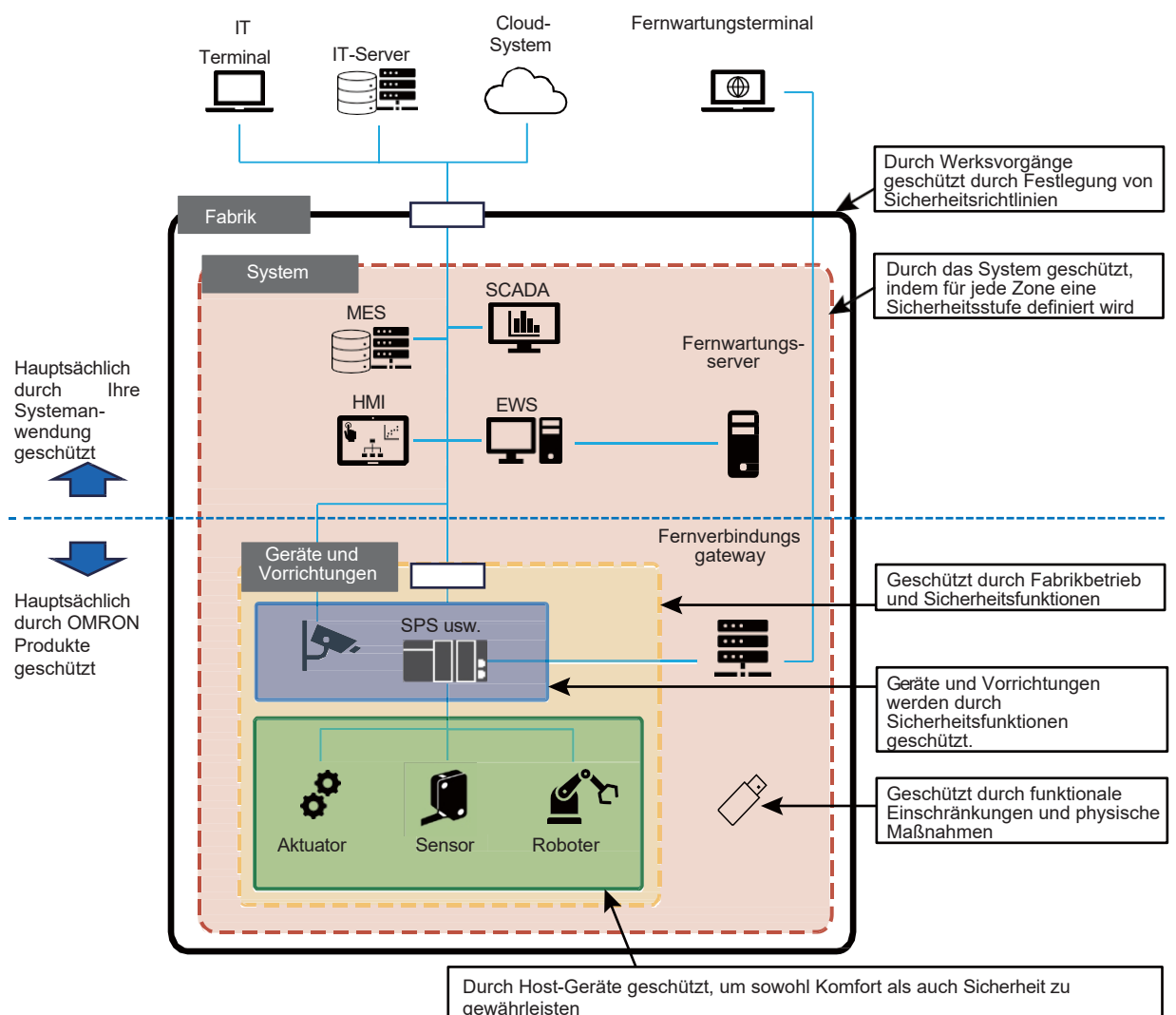
FA-Systeme sind den in der folgenden Tabelle aufgeführten Bedrohungen ausgesetzt. Um Ihre Vermögenswerte und Produktionsaktivitäten zu schützen, sollten Sie sich mit den Merkmalen dieser Bedrohungen vertraut machen und geeignete Maßnahmen ergreifen.

Art der Bedrohung	Beschreibung der Bedrohung
Spoofing	<p>Spoofing ist ein Angriff, bei dem versucht wird, sich durch Vortäuschen einer vertrauenswürdigen Identität als Benutzer oder System unrechtmäßig Zugriffsrechte zu verschaffen. Beispielsweise kann man Sie auf eine gefälschte Website weiterleiten, um Ihre Anmeldedaten zu stehlen, oder sich als echte Person ausgeben, um an Informationen zu gelangen.</p> <p>Maßnahmen dagegen sind die Verwendung sicherer Passwörter und die Einführung einer Multi-Faktor-Authentifizierung.</p>
Manipulation	<p>Manipulation ist ein Angriff, bei dem versucht wird, Informationen zu verändern, um die Gültigkeit von Daten zu untergraben. Beispielsweise kann dabei der Inhalt von Websites überschrieben oder Informationen in Datenbanken manipuliert werden. Dies kann zur Verbreitung falscher Informationen oder zu Systemfehlfunktionen führen.</p> <p>Maßnahmen dagegen sind die Einführung eines Mechanismus zur Überprüfung der Datenintegrität, die Verschärfung der Zugriffskontrolle oder die Aufzeichnung eines Änderungsverlaufs.</p>
Leugnung	<p>Leugnung ist die Handlung von Angreifern, die ihre Taten nicht zugeben, um sich der Verantwortung zu entziehen. Beispielsweise können Angreifer nach einem unbefugten Zugriff behaupten, dass sie dies nicht getan haben, indem sie die Protokolle löschen.</p> <p>Maßnahmen dagegen sind die ordnungsgemäße Aufzeichnung eines Betriebsprotokolls, die Kombination mit einer Zugriffskontrolle , um die Identifizierung des Bedieners zu ermöglichen, und die Verwendung digitaler Signaturen, um die Authentizität der Daten zu gewährleisten.</p>
Offenlegung von Informationen	<p>Die Offenlegung von Informationen ist ein Angriff, bei dem illegal auf vertrauliche Informationen zugegriffen und diese gestohlen werden. Die Offenlegung von Kundeninformationen, Geschäftsgeheimnissen usw. kann nicht nur zu wirtschaftlichen Verlusten, sondern auch zu einer Schädigung der sozialen Glaubwürdigkeit führen.</p> <p>Maßnahmen dagegen sind die Implementierung einer gründlichen Zugriffskontrolle, die Verschlüsselung von Daten und die die Installation von Sicherheitssoftware.</p>
Denial-of-Service	<p>Ein Denial-of-Service-Angriff ist ein Angriff, bei dem ein System übermäßig belastet wird, um seine Dienste zu unterbrechen. Dadurch kann das angegriffene System keine Dienste mehr bereitstellen, was zu Betriebsstörungen führt.</p> <p>Maßnahmen dagegen sind unter anderem der Einsatz einer Firewall zum Blockieren unbefugter Zugriffe, die Implementierung Lastverteilung zur Reduzierung der Systemlast und die Einführung eines Intrusion Detection Systems zur frühzeitigen Erkennung von Angriffen.</p>
Erweiterung von Berechtigungen	<p>Privilegienausweitung ist ein Angriff, bei dem illegal Systemprivilegien erlangt und anschließend Vorgänge mit Administratorrechten durchgeführt werden. Dadurch können Angreifer wichtige Daten manipulieren, Systeme zerstören usw.</p> <p>Maßnahmen dagegen sind unter anderem, keine unnötigen Privilegien zu vergeben, Sicherheitsupdates , um Schwachstellen zu beheben, und die Einführung einer Multi-Faktor-Authentifizierung.</p>

4-2 Sicherheitsmaßnahmen in FA-Systemen

In diesem Abschnitt werden Sicherheitsmaßnahmen vorgestellt.

Das Grundkonzept der Sicherheitsmaßnahmen ist die Defense in Depth. Im Rahmen des Defense in Depth-Konzepts werden Sicherheitsmaßnahmen in jeder Ebene umgesetzt. In der Fabrikebene ist es üblich, Sicherheitsrichtlinien festzulegen und Vermögenswerte durch Fabrikabläufe zu schützen. In der Systemebene wird ein System aufgebaut, indem für jede Zone eine Sicherheitsstufe definiert wird, und Vermögenswerte im gesamten System geschützt werden, wobei auch die betrieblichen Aspekte berücksichtigt werden. Darüber hinaus werden Maßnahmen für das Netzwerk ergriffen, wie z. B. Kommunikationszugriffskontrolle, Filterung und Installation einer Firewall. Bis zu diesem Punkt werden diese Maßnahmen mit Ihrem System und Ihrer Anwendung durchgeführt. Geräte und Vorrichtungen nutzen ihre integrierten Sicherheitsfunktionen effektiv, um den Betrieb der Geräte oder Steuerungen und die in den Geräten oder Vorrichtungen enthaltenen Vermögenswerte zu schützen.



Darüber hinaus sollten Sie Bedrohungen in zwei Kategorien einteilen, nämlich Bedrohungen von externen Quellen und Bedrohungen durch interne Mitarbeiter.

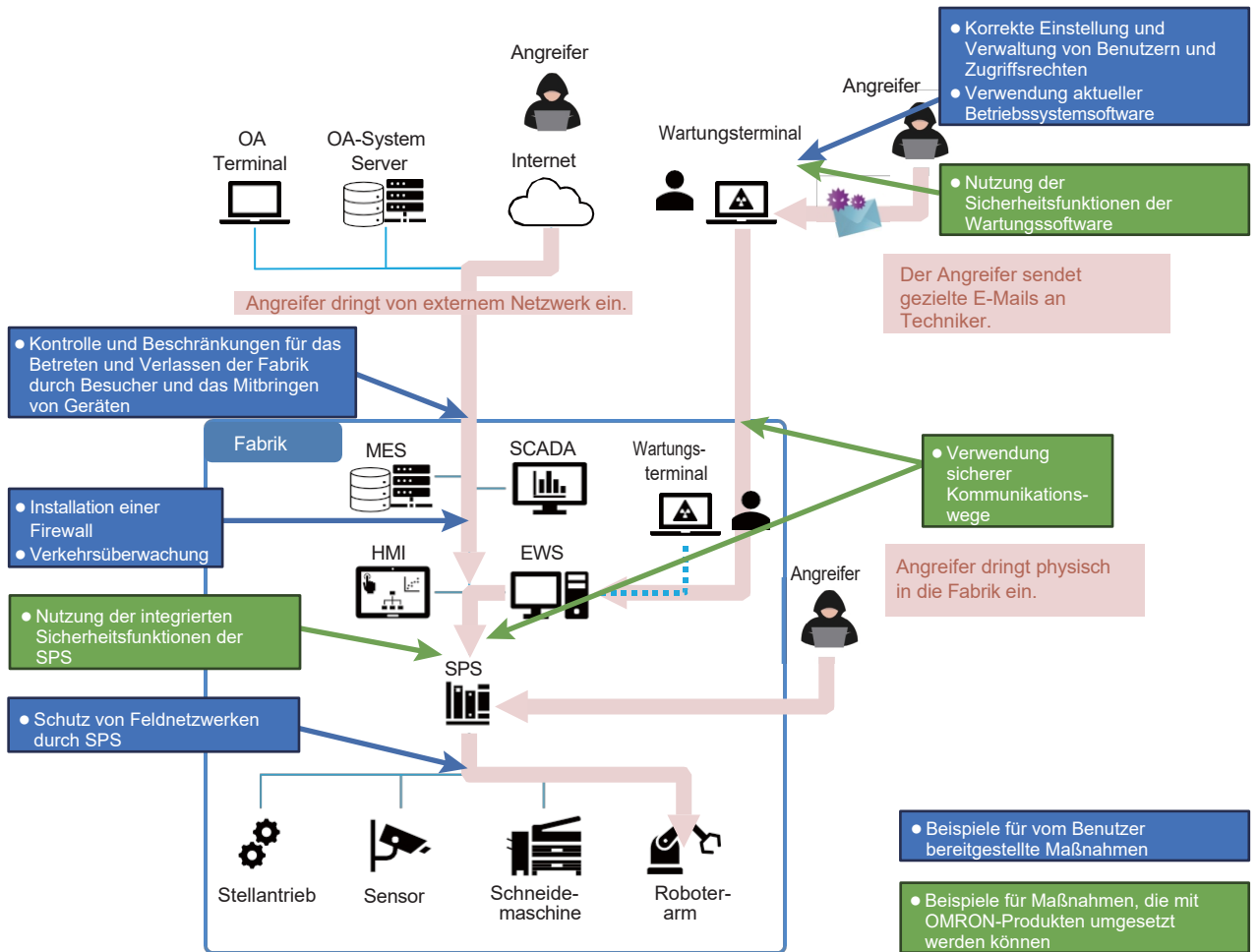
Für Bedrohungen von externen Quellen sollten Sie Sicherheitsmaßnahmen zur Prävention, Abschreckung, Erkennung und Verfolgung auf der Prozessebene, der physischen Ebene und der technischen Ebene ergreifen.

Das Grundkonzept der Sicherheitsmaßnahmen umfasst die folgenden drei Punkte.

- Verhindern von Eindringversuchen (Zugangsmaßnahmen)

- Verhinderung der Ausbreitung von Schäden (interne Maßnahmen)
- Verhinderung der Offenlegung (Ausgangsmaßnahmen)

Kombinieren Sie die in diesem Dokument beschriebenen Maßnahmen, um mehrschichtige Sicherheitsmaßnahmen ordnungsgemäß zu ergreifen.



4-2-1 Sicherheitsmaßnahmen für die Mensch- und Prozessebene

Für interne Mitarbeiter gilt es als wirksam, das Bewusstsein durch Schulungen zu schärfen, die Erkennungs- und Nachverfolgungsfunktionen durch Systemprüfungen, gegenseitige Kontrollen durch mehrere Personen usw. zu verbessern und den Kontroll- und Ausgleichseffekt durch Inspektionen und Audits zu verstärken. Dieser Abschnitt enthält Beispiele für Sicherheitsmaßnahmen für Prozesse und Benutzer.

Maßnahmen	Beschreibung
Korrekte Einstellung der Zugriffsrechte	<p>FA-Systeme enthalten eine große Menge an Informationen, die als Vermögenswerte geschützt werden sollten, wie z. B. Produktions-Know-how, Produktionsdaten, Produktinformationen usw. In einer Umgebung, in der eine große Anzahl nicht näher bezeichneter Personen auf Informationsressourcen zugreifen kann, besteht ein hohes Risiko der Offenlegung von Informationen aufgrund menschlicher Fehler oder böswilliger Manipulationen.</p> <p>Es ist wichtig, die „Vertraulichkeit“ zu schützen, indem Methoden zur Verwaltung von Zugriffsrechten und zur Speicherung vertraulicher Informationen festgelegt sowie Verwaltungsregeln erstellt werden, um zu verhindern, dass andere Personen als bestimmte Personen auf die Informationen zugreifen können. Daten und Dateien, die auf tragbaren Geräten wie PCs oder externen Medien gespeichert sind, sind besonders einem höheren Risiko der Offenlegung ausgesetzt. Es ist von entscheidender Bedeutung, vorbeugende Maßnahmen zu ergreifen, wie z. B. die Verschlüsselung wichtiger Daten, um das Ausmaß des Schadens im Falle einer Offenlegung zu begrenzen.</p>

Maßnahmen	Beschreibung
Verhindern der Weitergabe von IDs und Passwörtern	<p>In einem FA-System, an dem mehr als eine Person beteiligt ist, macht die gemeinsame Nutzung einer einzigen ID und eines Passworts durch mehrere Personen es unmöglich, den Angreifer zu verfolgen und zu identifizieren, selbst wenn eine böswillige Handlung oder ein böswilliger Zugriff vorliegt.</p> <p>Legen Sie für jeden Benutzer eine eigene ID und ein eigenes Passwort fest, um sicherzustellen, dass nur der richtige Benutzer das System bedienen kann</p> <p>System bedienen kann.</p>
Verhindern der Verwendung derselben IDs und Passwörter	<p>Die Verwendung derselben Benutzer-IDs und Passwörter in Subsystemen eines FA-Systems oder in anderen Systemen als dem FA-System ermöglicht es Angreifern, mit Hilfe von Benutzer-IDs und Passwörtern, die sie auf illegale Weise erworben haben, auf alle Tools und Geräte zuzugreifen.</p> <p>Durch die Festlegung unterschiedlicher Passwörter für jedes Tool oder Gerät können Sie im Falle einer Passwortoffenlegung die Ausbreitung des Schadens verhindern. Da dies die Verwaltung von Benutzer-IDs und Passwörtern kompliziert macht, besteht eine realistische Lösung darin, eine Liste mit Benutzer-IDs und Passwörtern zu erstellen, en-</p> <p>Verschlüsseln oder schützen Sie es mit einem Passwort und bewahren Sie es an einem Ort mit beschränktem Zugriff auf.</p>
Verwenden Sie schwer zu erratende Passwörter und ändern Sie diese regelmäßig	<p>Passwörter, die der Benutzer-ID sehr ähnlich sind, leicht zu erratende Passwörter wie Geburtsdaten oder englische Wörter aus allgemeinen Wörterbüchern oder kurze Passwörter, die nur wenige Zeichenarten enthalten, können leichter durch Wörterbuchangriffe oder Brute-Force-Angriffe geknackt werden.</p> <p>Legen Sie schwer zu erratende Passwörter fest, die mindestens acht Zeichen lang sind und mehrere Zeichentypen enthalten, und ändern Sie diese regelmäßig. Wir empfehlen die Verwendung eines Passwort-Managers oder eines ähnlichen Tools, das komplexe Passwörter generiert.</p>
Überwachung des Zugriffsprotokolls	<p>Ein Zugriffsprotokoll ist eine Aufzeichnung der Zugriffe auf Server, Netzwerkgeräte usw. Es enthält detaillierte Informationen darüber, wer wann und wie auf welche Ressource zugegriffen hat.</p> <p>Die Überwachung des Zugriffsprotokolls ist eine wichtige Maßnahme, mit der Sie unbefugte Zugriffe erkennen, Anzeichen für Malware-Infektionen finden und verfolgen sowie das Ausmaß der Infektion bestimmen können. Indem Sie die Nutzung des Systems erfassen, können Sie ungewöhnliche Zugriffe von verdächtigen IP-Adressen und Anfragen erkennen, die vom normalen Muster abweichen.</p>
Geräte und Software auf dem neuesten Stand halten	<p>Die Aktualisierung von Geräten und Software in Steuerungssystemen und Anlagen trägt zur Verbesserung der Sicherheit bei. Schwachstellen in Geräten und Software können für Angriffe ausgenutzt werden.</p> <p>Aktualisieren Sie Ihre Geräte und Software, um bekannte Schwachstellen zu beheben und die Sicherheit und Leistung zu verbessern.</p>
Durchführen eines Virenskans vor dem Anschließen eines Geräts an die Anlage	<p>Verhindern Sie Malware-Infektionen, wenn Sie externe Medien wie USB-Speichersticks mit Steuerungssystemen und Geräten verwenden.</p>
Klare Festlegung von Verantwortlichkeiten und Strafen	<p>Eine klare Festlegung in den Arbeitsvorschriften, dass die Mitarbeiter für die Ausführung von Vorgängen gemäß den Sicherheitsrichtlinien verantwortlich sind und dass bei Verstößen Strafen verhängt werden, hat eine kontrollierende Wirkung auf das interne Personal.</p> <p>Die gegenseitige Überprüfung von Vorgängen durch mehrere Personen hat ebenfalls eine kontrollierende Wirkung.</p>
Durchführung von Sicherheitsschulungen	<p>Die Durchführung von Schulungen zur Notwendigkeit von Sicherheitsmaßnahmen, zur Art der Bedrohungen, zu den verwendeten Geräten und deren Verwaltungsmechanismen trägt dazu bei, eine unsachgemäße Verwendung und die Unterlassung von Sicherheitsmaßnahmen zu verhindern, Betrugsfälle zu reduzieren usw., was zu einer höheren Sicherheitsstärke der Kontrollsysteme und -geräte führt.</p> <p>Es ist wichtig, Bildungslehrpläne entsprechend den Aufgaben und Rollen der Mitarbeiter zu erstellen und die Schulungen regelmäßig und kontinuierlich gemäß dem Plan durchzuführen.</p>
Bemühungen zur Aufrechterhaltung eines Arbeitsumfelds, das die Gesundheit der Mitarbeiter fördert und ihre psychische Gesundheit schützt	<p>Die Aufrechterhaltung eines Arbeitsumfelds, das Gesundheitsprobleme aufgrund schlechter Arbeitsbedingungen oder Überlastung verhindert, trägt dazu bei, Arbeitsfehler zu vermeiden.</p> <p>Darüber hinaus trägt die Entwicklung eines Systems oder Mechanismus zur Bewältigung von Stress und Unzufriedenheit der Mitarbeiter dazu bei, Angriffe durch interne Mitarbeiter zu verhindern.</p>

4-2-2 Sicherheitsmaßnahmen für die physische Ebene

Treffen Sie Sicherheitsmaßnahmen für physische Zugangswege zu Produkten. Die wichtigsten Maßnahmen für die physikalische Ebene sind Prävention und Schutz.

Beispiele für diese Maßnahmen sind unten aufgeführt.

Maßnahmen	Beschreibung
Verhindern Sie das illegale Eindringen von Angreifern in die Fabrik und die Bereiche, in denen Geräte installiert sind.	<p>Verhindern Sie, dass Angreifer in die Fabrik- und Anlageninstallationsbereiche eindringen und dann direkt einen USB-Speicherstick usw. an Geräte anschließen.</p> <p>Teilen Sie zunächst die physischen Bereiche entsprechend der Sicherheitsstufe ein und legen Sie klar fest, wer Administrator und wer Zugangsberechtigt für die einzelnen Bereiche ist. In der Regel werden die physischen Bereiche in drei Zonen unterteilt: einen allgemeinen Bereich, den neben internen Mitarbeitern auch Besucher betreten und verlassen dürfen, einen Geschäftsbereich, in dem interne Mitarbeiter Vollzeit arbeiten, und einen Sicherheitsbereich, in dem wichtige Informationsressourcen gespeichert sind.</p> <p>Legen Sie als Nächstes die Ein- und Ausgangssteuerungsmethode für jede Zone sowie die Verriegelungs- und Authentifizierungsmethoden fest. Für die Ein- und Ausgangssteuerung stehen neben Kartenlesegeräten, Fingerabdruckererkennung, Gesichtserkennung und ähnlichen Systemen auch Sichtkontrollen, Kontrollen durch Sicherheitspersonal usw. zur Verfügung.</p> <p>Wählen Sie die am besten geeignete Methode oder eine Kombination dieser Methoden unter Berücksichtigung der für den Bereich erforderliche Sicherheitsstufe und die Betriebs- und Verwaltungskosten.</p>
Verhindern, dass Geräte berührt werden	<p>Verhindern Sie die physische Bedienung von Geräten, indem Sie Bedienfelder verriegeln, Kommunikationsanschlüsse abdecken usw. Dadurch werden unbefugte Vorgänge in der Fabrik und in den Geräteinstallationsbereichen verhindert.</p> <p>Außerdem sollten Wartungsterminal-PCs und mitgebrachte Geräte kontrolliert und eingeschränkt werden, um zu verhindern, dass</p> <p>, dass sie nicht bedient werden können.</p>
Ständige Überwachung der Situation mit Überwachungskameras	<p>Es reicht nicht aus, nur Maßnahmen zur Verhinderung illegaler Eindringversuche zu ergreifen, um alle Arten von Betrug zu verhindern, wie z. B. illegale Handlungen von Personen mit ordnungsgemäßen Berechtigungen, Spoofing von Personen mit ordnungsgemäßen Berechtigungen durch Personen, die sich illegal IC-Karten beschafft haben, und das gemeinsame Betreten von Angreifern mit autorisierten Personen. Darüber hinaus kann es zu Einschränkungen aufgrund von Problemen bei Betrieb und Verwaltung, Kosten und Installationsplatz im Zusammenhang mit dem Ein- und Ausgangs-Kontrollsystem kommen. In solchen Fällen hilft die ständige Überwachung der Ein- und Ausgangs-Situation sowie der Arbeitsleistung in jeder Zone mithilfe von Überwachungskameras, illegale Handlungen einzudämmen.</p>

4-2-3 Sicherheitsmaßnahmen für die technische Ebene

Ergreifen Sie technische Sicherheitsmaßnahmen für Netzwerke und Geräte. Beispiele für solche Maßnahmen sind unten aufgeführt.

Maßnahmen	Beschreibung
Implementierung der Authentifizierung	<p>Überprüfen Sie die Gültigkeit von Bedienern, angeschlossenen Geräten und verarbeiteten Daten, um unbefugten Zugriff und unbefugte Vorgänge zu verhindern. Es gibt drei Authentifizierungsmethoden: Authentifizierung durch Biometrie (was Sie sind); Authentifizierung durch Smartphone, IC-Karte oder Sicherheitstoken (was Sie haben); und Authentifizierung durch PIN-Code, Antwort auf eine Geheimfrage oder andere Informationen, die nur der Benutzer kennt (was Sie wissen). Die Authentifizierung durch die Kombination von zwei oder mehr dieser Methoden wird als Multi-Faktor-Authentifizierung bezeichnet und bietet ein höheres Sicherheitsniveau. Um die Stärke der Authentifizierung zu erhöhen, wird häufig auch die Zwei-Faktor-Authentifizierung verwendet.</p> <p>Darüber hinaus ist die Kombination dieser Authentifizierungsmethoden mit einer Funktionssperre wirksam gegen Brute-Force-Angriffe.</p> <p>In den letzten Jahren haben sich WLAN-Bridge-Geräte und LAN-Switches, die EAP, ein Protokoll zur Benutzerauthentifizierung, unterstützen, weit verbreitet. Wenn ein von außen eingebrachter Client-PC usw. versucht, eine Verbindung zu einem LAN herzustellen, überprüft das Authentifizierungsgerät die Gültigkeit und Sicherheit des Geräts, bevor es die Verbindung zum LAN herstellt.</p>

Maßnahmen	Beschreibung
Verwendung sicherer Kommunikation Wege	<p>Es wird darauf hingewiesen, dass einige Kommunikationsprotokolle zwischen dem Host-PC und Geräten Schwachstellen aufweisen, z. B. die Übertragung von Kommunikationsdaten im Klartext, das Fehlen eines Sitzungsmanagementmechanismus usw., und somit das Risiko der Offenlegung und Manipulation von Informationen bergen.</p> <p>Um dies zu verhindern, sollten Sie hochsichere Dienste mit Verschlüsselungsfunktionen verwenden, wie z. B. SSH (Secure Shell), SFTP (SSH File Transfer Protocol), OPC UA und HTTPS. VPNs führen Verschlüsselungen und andere Verarbeitungen mithilfe von mehrschichtigen Protokollen durch, wodurch der Kommunikationspfad selbst sicher ist, ohne dass man sich auf die Anwendung in der oberen Schicht verlassen muss.</p> <p>Darüber hinaus kann der Controller über ein Dateiübertragungsprotokoll usw. von außen Operationen ausführen, da er externe Medien verwenden kann. Damit Dateien jedoch auf externen Medien gespeichert werden können, müssen Sie die Einrichtung von Passwörtern für die Dateien selbst, die Authentifizierung für Dateioperationen usw. in Betracht ziehen. Protokolle wie FTP sind beispielsweise wichtige Kommunikationsprotokolle für die Bearbeitung von Dateien auf externen Medien. Obwohl bei FTP in vielen Fällen die Passworteinstellung normalerweise deaktiviert ist, können Sie ein sicheres Passwort festlegen und damit unbefugte Operationen mit den Dateien verhindern. Um Operationen von außen zu verhindern, müssen Sie Maßnahmen wie die Deaktivierung der FTP-Funktion selbst ergreifen.</p> <p>die FTP-Funktion selbst zu aktivieren.</p>
Einführung eines Intrusion Detection Systems (IDS) oder Intrusion Prevention Systems (IPS)	<p>Ein Intrusion Detection System (IDS) ist ein System, das Ereignisse in einem Netzwerk oder auf einem Host in Echtzeit überwacht, Eindringlinge und Angriffe erkennt und den Administrator benachrichtigt. Das IDS verfügt über eine Datenbank mit Angriffsmustern (Signatures) und gleicht diese mit tatsächlichen Ereignissen ab, um Angriffe zu erkennen, aufzuzeichnen und den Benutzer zu warnen, die Schwachstellen im Betriebssystem ausnutzen, Dateien manipulieren usw.</p> <p>Es gibt zwei Arten von Intrusion Detection Systemen: Netzwerk-Intrusion Detection Systeme (NIDS), die ein Überwachungsgerät mit dem zu überwachenden Netzwerksegment verbinden, und Host-Intrusion Detection Systeme (HIDS), die auf dem zu überwachenden Host (Webserver, DB-Server, Mailserver usw.) installiert und verwendet werden.</p> <p>Das Intrusion Prevention System (IPS) übernimmt und erweitert die Angriffsblokierfunktion des NIDS. Es ermöglicht Inline-Verbindungen, die nicht autorisierte Pakete vollständig blockieren.</p>
Isolierung von Netzwerken von Steuerungssystemen und Geräten von IT-Netzwerken	<p>Installieren Sie für Netzwerke von Steuerungssystemen und -geräten eine Firewall (um nicht verwendete Kommunikationsports zu blockieren und Kommunikationshosts zu beschränken). Stellen Sie sicher, dass die Netzwerke von IT-Netzwerken isoliert sind und dass Verbindungen zu den Steuerungssystemen innerhalb der Firewall hergestellt werden.</p>
Aktivieren der Sicherheitsfunktionen von Geräten in Steuerungssystemen und Anlagen	<p>Schützen Sie Ihre wichtigen Anlagen und Produktionsaktivitäten durch die ordnungsgemäße Verwendung der in den im System oder in den Geräten verwendeten Sicherheitsfunktionen. OMRON FA-Produkte bieten verschiedene Sicherheitsfunktionen. Verwenden Sie diese Funktionen ordnungsgemäß, um Ihre wichtigen Anlagen und Produktionsaktivitäten zu schützen.</p> <p>Wenn die Verwendung der Sicherheitsfunktionen aus betrieblichen oder anderen Gründen nicht möglich ist, ergreifen Sie andere Maßnahmen.</p> <p>Einzelheiten zu den Sicherheitsfunktionen der Geräte und Software von OMRON sowie Informationen zu deren Verwendung und Betrieb finden Sie in den Sicherheitshinweisen und Benutzerhandbüchern der einzelnen Produkte für Sicherheitsmaßnahmen.</p>
Installation von Sicherheitssoftware	<p>Installieren und warten Sie die neueste kommerzielle Antivirensoftware auf PCs, die mit Steuerungssystemen verbunden sind.</p>



Anhänge



A-1	Verwandte Materialien	A-2
-----	-----------------------------	-----



A-1 Verwandte Materialien

Die folgende Tabelle enthält eine Übersicht über Dokumente, die mit diesem Dokument in Zusammenhang stehen.

Herausgeber	Dokumentname, Übersicht und zugehörige Abschnitte dieses Dokuments
IEC/ISA99	IEC 62443-1 Allgemeine und gemeinsame Angelegenheiten für alle Dokumente
	Enthält Erläuterungen zu Konzepten, Modellen, Begriffen usw., auf die in der Reihe IEC 62443 häufig Bezug genommen wird, sowie sieben grundlegende Anforderungen (FRs) für FA-Systeme.
IEC/ISA99	IEC 62443-2 Sicherheitsrichtlinien und -verfahren für Organisationen, die Systeme entwickeln und betreiben
	Enthält Sicherheitsanforderungen für Richtlinien und Verfahren für das Management und den Betrieb von Organisationen, die an FA-Systemen beteiligt sind.
IEC/ISA99	IEC 62443-3 Sicherheitsanforderungen für Systeme
	Bietet Anforderungen an Sicherheitsfunktionen, Design von Sicherheitsfunktionen und Technologie für FA-Systeme.
IEC/ISA99	IEC 62443-4 Sicherheitsanforderungen für Komponenten
	Enthält den Sicherheitsentwicklungsprozess und die Anforderungen an die Sicherheitsfunktionen für jede Komponente, aus der ein FA-System besteht.

Hinweis: Verwenden Sie dieses Dokument nicht zum Betrieb des Geräts.

OMRON Corporation Industrial Automation Company

Kyoto, JAPAN

Kontakt: www.ia.omron.com

Autorisierter Händler:

Regionaler Hauptsitz

OMRON EUROPE B.V.

Wegalaan 67-69, 2132 JD Hoofddorp
Niederlande

Tel.: (31) 2356-81-300 Fax: (31) 2356-81-388

OMRON ELECTRONICS LLC

2895 Greenspoint Parkway, Suite 200
Hoffman Estates, IL 60169 USA

Tel.: (1) 847-843-7900 Fax: (1) 847-843-7787

OMRON ASIA PACIFIC PTE. LTD.

438B Alexandra Road, #08-01/02 Alexandra
Technopark, Singapur 119968

Tel.: (65) 6835-3011 Fax: (65) 6835-3011

OMRON (CHINA) CO., LTD.

Raum 2211, Bank of China Tower, 200
Yin Cheng Zhong Road,
PuDong New Area, Shanghai, 200120, China

Tel.: (86) 21-6023-0333 Fax: (86) 21-5037-2388

©OMRON Corporation 2023-2026 Alle Rechte vorbehalten. Im
Interesse der Produktverbesserung
können sich die technischen Daten ohne vorherige Ankündigung ändern.

Kat.-Nr. P162-D1-03

0126