Informationssicherheits-managementsystem für kleine und mittlere Unternehmen (KMU)

Leitfaden zur Interpretation und Umsetzung der VdS 10000 für Industrielle Automatisierungssysteme

Herausgeber und Verlag: VdS Schadenverhütung GmbH

Amsterdamer Str. 172-174
D-50735 Köln
Telefon: (0221) 77 66 0; Fax: (0221) 77 66 341

VdS-Richtlinien für die Informationsverarbeitung

Informationssicherheits-managementsystem für kleine und mittlere Unternehmen (KMU)

Leitfaden zur Interpretation und Umsetzung der VdS 10000 für Industrielle Automatisierungssysteme

Das vorliegende Dokument ist nur verbindlich, sofern dessen Verwendung im Einzelfall vereinbart wird; ansonsten ist die Berücksichtigung dieses Dokuments unverbindlich. Die Vereinbarung zur Verwendung dieses Dokuments ist rein fakultativ. Dritte können im Einzelfall auch andere Anforderungen nach eigenem Ermessen akzeptieren, die diesem Dokument nicht entsprechen.

Inhalt

1 Allgemeines

1.1 Anwendungshinweise

Die vorliegenden Richtlinien sind Grundlage für eine Zertifizierung durch VdS Schadenverhütung.

Die Umsetzung der geforderten Maßnahmen bedingt Fachwissen und Erfahrung auf den Gebieten der Informationssicherheit und der Managementsysteme. Die Ausführungen in den vorliegenden Richtlinien 10020 beziehen sich insbesondere auf die Aspekte der Informationssicherheit in Produktionsanlagen. Für deren Anwendung ist es erforderlich, dass auch Fachwissen in Bezug auf die Anforderungen im Produktionsbereich vorliegt. Es ist bei der Umsetzung insbesondere zu beachten, dass im Produktionsbereich die Priorisierung der Schutzziele von denen der IT im restlichen Teil der Organisation abweichen kann. Sind die benötigten Kenntnisse nicht in ausreichendem Maß vorhanden, empfiehlt sich die Inanspruchnahme qualifizierter Dienstleister, die ein Anerkennungsverfahren gemäß VdS 10003 durchlaufen haben.

Verpflichtende Maßnahmen sind durch die Schlüsselworte MUSS/MÜSSEN, DARF NICHT/DÜRFEN NICHT/DÜRFEN KEINE gekennzeichnet, empfohlene Maßnahmen durch die Schlüsselworte SOLLTE/SOLLTEN, SOLLTE NICHT/SOLLTEN NICHT, KANN/KÖNNEN, DARF/DÜRFEN.

Die Richtlinien SOLLTEN in bestehende Managementsysteme integriert werden, um potentielle Synergieeffekte zu nutzen.

Insbesondere SOLLTEN sie zusammen mit den Richtlinien VdS 10010 „VdS-Richtlinien zur Umsetzung der DSGVO“ implementiert werden.

Aus Gründen der leichteren Lesbarkeit wird in diesen Richtlinien auf eine geschlechtsspezifische Differenzierung, wie z. B. Teilnehmer/Innen, verzichtet. Es wird durchgängig die männliche Form verwendet. Im Sinne des Gleichbehandlungsgesetztes sind diese Beziehungen als nicht geschlechtsspezifisch zu betrachten.

1.2 Anwendungs- und Geltungsbereich

Diese Richtlinien sind für KMU, den gehobenen Mittelstand, Verwaltungen, Verbände und sonstige Organisationen anwendbar.

Die Richtlinien SOLLTEN auf die gesamte Organisation angewendet werden, ihr Geltungsbereich KANN jedoch technisch, geographisch und/oder organisatorisch eingegrenzt werden.

1.3 Gültigkeit

Diese Richtlinien gelten ab dem 01.04.2020 und ersetzen die VdS-Richtlinien VdS 10020 vom 01.01.2018.

2 Normative Verweise

Diese Richtlinien enthalten datierte und undatierte Verweise auf andere Regelwerke. Die Verweise erfolgen in den entsprechenden Abschnitten, die Titel werden im Folgenden aufgeführt. Änderungen oder Ergänzungen datierter Regelwerke gelten nur, wenn sie durch Änderung dieser Richtlinien bekannt gegeben werden. Von undatierten Regelwerken gilt die jeweils zuletzt veröffentlichte Fassung.

BSI-CS 123	Empfehlungen für Fortbildungs- und Qualifizierungsmaßnahmen im ICS-Umfeld
DIN IEC 62443 VDE 0802	Normreihe IEC 62443 Industrial communication networks – Network and system security
IT-SiG	Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)
VDI/VDE 2182	VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA) Normenreihe VDI/VDE 2182: Informationssicherheit in der industriellen Automatisierung
VdS 10000	Informationssicherheitsmanagementsystem für kleine und mittlere Unternehmen (KMU), Anforderungen

3 Glossar

Sämtliche Begriffe dieser Richtlinie sind gemäß Kapitel 3 der VdS 10000 zu verstehen. Folgende Begriffe für die Anwendung in der Automatisierungstechnik werden konkretisiert bzw. zusätzlich definiert. Zusätzlich definierte Begriffe sind mit einem * gekennzeichnet.

Administrativer Zugang: Administrative Zugänge existieren auch für Automatisierungskomponenten.

Administrator: Im Produktionsbereich ist unter IT-System auch das Automatisierungssystem zu verstehen.

Aktive Netzwerkkomponente: Aktive Netzwerkkomponenten im Produktionsbereich werden in der Regel in industrietauglicher Ausführung verwendet (z. B. Hutschienen-Montage, Versorgung mit 24-V-Gleichspannung, lüfterloser Betrieb).

Automatisierungssystem*: Dient dazu, die in einem technischen System ablaufenden Prozesse selbsttätig zu führen. Ein Automatisierungssystem setzt sich aus Automatisierungskomponenten zusammen.

Automatisierungskomponente*: Teil eines Automatisierungssystems. Automatisierungskomponenten können z. B. speicherprogrammierbare Steuerungen (SPS, Controller), Ein-/Ausgabe-Systeme, Sensoren und Aktoren, Server, Bedien- und Beobachtungsstationen, Engineering-Stationen und das Automatisierungsnetzwerk sein.

Automatisierungsnetzwerk*: Netzwerk über das die Komponenten eines Automatisierungssystems untereinander kommunizieren. Teile des Automatisierungsnetzwerkes (Kommunikation im Feldbereich) unterliegen Echtzeitanforderungen.

Demilitarisierte Zone (DMZ)*: Abgeschotteter Bereich eines Netzwerks, der für das Ein- und Ausschleusen von Daten verwendet werden kann.

Engineering Station/Engineering Workstation*: IT-System zur Konfiguration, Inbetriebnahme und Überwachung eines Automatisierungssystems.

Funktionale Sicherheit*: Bezeichnet den Teil der Sicherheit eines IT-Systems, der von der korrekten Funktion des sicherheitsbezogenen IT-Systems und anderer risikomindernder Maßnahmen abhängt. Nicht zur funktionalen Sicherheit gehören u. a. elektrische Sicherheit, Brandschutz oder Strahlenschutz.

Informationssicherheit: In einer Produktionsumgebung ist die Verfügbarkeit der Produktionsanlage von besonderer Bedeutung.

Informationssicherheitsbeauftragter (ISB): Die Zuständigkeit des ISB umfasst auch den Produktionsbereich.

Informationstechnik (IT): Umfasst die im Produktionsbereich eingesetzte Hard- und Software.

IT-Infrastruktur: Umfasst auch die Einrichtungen im Produktionsbereich.

IT-Ressource: Umfasst auch die Betriebsmittel im Produktionsbereich.

IT-Verantwortlicher: Für die IT-Ressourcen im Produktionsbereich sind entsprechende IT-Verantwortliche zu benennen.

IT-System: Umfasst auch die Anlagen im Produktionsbereich. Hierunter fallen z. B. Automatisierungskomponenten wie Engineering-Stationen, Operator-Konsolen, SPS, Ein-/Ausgabe-Systeme etc.

Kritisches IT-System: Automatisierungssysteme können zu den kritischen IT-Systemen gehören, sofern sie die Bedingungen gem. Abschnitt 9.3. erfüllen.

Kritische Verbindung: Verbindungen im Produktionsbereich können zu den kritische Verbindungen gehören, sofern sie die Bedingungen gemäß Abschnitt 9.3 erfüllen.

Mehr-Faktor-Authentifizierung*: Nachweis der Identität mit Hilfe von mehreren unabhängigen Merkmalen.

Mobiles IT-System: Ob es sich bei einem IT-System um ein mobiles IT-System handelt, wird durch seinen Einsatzzweck bestimmt, nicht durch seine Bauart. So gilt z. B. ein Notebook, das stationär als Workstation betrieben wird, nicht als mobiles IT-System. Die Beschreibung betrifft auch Automatisierungskomponenten, deren Einsatzzweck durch Mobilität und die Anwendung im Produktionsbereich gekennzeichnet ist. Typische mobile Automatisierungskomponenten sind z. B. Notebooks, Smartphones, Tablets oder Digitalkameras, die im Produktionsbereich eingesetzt werden.

Operator-Station/Operator-Konsole/Konsole/Leitstation*: Unter diesen Begriffen ist der Teil eines Automatisierungssystems zu verstehen, mit dem der technische Prozess bedient und beobachtet werden kann. Darüber hinaus stellt die Operator-Station auch Diagnosefunktionen für die Überwachung des Automatisierungssystems zur Verfügung.

Produktionsanlage*: Abgeschlossene Anlage in einer Organisation, auf der Güter produziert/verarbeitet werden. Die Produktionsanlage umfasst neben den physischen Anlagenteilen (wie z. B. Pressen, Transportanlagen oder Werkzugmaschinen) auch die benötigte Informationstechnik.

Produktionsbereich*: Teil einer Organisation, welcher direkt mit der Produktion der Güter beschäftigt ist.

Hinweis: In diesem Dokument wird aus Vereinfachungsgründen teilweise die verkürzte Fassung „in der Produktion“ verwendet.

Produktionsverantwortlicher*: Leiter der Produktion, bzw. das für die Produktion zuständige Management.

Schichtzugang (Gruppen-Account)*: Zugang zu einem IT-System oder Automatisierungssystem, bei dem sich mehrere Mitarbeiter einer Schicht einen Zugang (Account) teilen. Ein Schichtzugang findet im allgemeinen Anwendung in einem räumlich eingegrenzten Umfeld, z. B. in Leitwarten.

4 Organisation der Informationssicherheit

4.1 Verantwortlichkeiten

4.1.1 Zuweisung und Dokumentation

2. Hierbei sind auch die Ressourcen im Produktionsbereich zu berücksichtigen.

4.1.4 Delegieren von Aufgaben

Diese Festlegung ermöglicht eine Delegation von Aufgaben im Produktionsbereich an Mitarbeiter, die in diesem Gebiet über besondere Erfahrungen verfügen.

4.3 Informationssicherheitsbeauftragter (ISB)

Der ISB trägt die Verantwortung für die gesamte Organisation, um eine organisationsweite Implementierung der Informationssicherheit zu gewährleisten. Dies schließt den Produktionsbereich ein. Insbesondere die Schnittstelle zwischen dem Produktionsbereich und der restlichen Organisation ist hierbei von besonderer Bedeutung. Die Automatisierungssysteme im Produktionsbereich (Produktionsanlagen) fallen unter diesen Punkt.

Der ISB MUSS darauf hinwirken, dass die in der Leitlinie zur Informationssicherheit (IS-Leitlinie) definierten Ziele der Informationssicherheit auch im Produktionsumfeld erreicht werden.

Er KANN Aufgaben delegieren (siehe Abschnitt 4.1.4).

4.4 Informationssicherheitsteam (IST)

In produzierenden Organisationen gibt es i. d. R. die Rolle des Produktionsverantwortlichen. Der Produktionsverantwortliche oder ein von ihm benannter Mitarbeiter MUSS Mitglied des IST sein. Eine Delegation dieser Aufgabe ist möglich. In jedem Fall MUSS der Produktionsbereich im IST repräsentiert sein.

4.5 IT-Verantwortliche

In Organisationen existieren häufig mehrere IT-Infrastrukturen (IT im Verwaltungsbereich, Netzwerktechnik, Telefonanlage, Automatisierungssystem, Gebäudeleittechnik), die von unterschiedlichen Organisationseinheiten betreut werden. Die VdS 10000 kann aufgrund ihres generischen Ansatzes auf die gesamte IT-Infrastruktur angewandt werden. Um ihre Umsetzung in den einzelnen IT-Infrastrukturen fachlich fundiert zu gewährleisten, fordert die VdS 10000 einen oder mehrere IT-Verantwortliche zu benennen.

4.10 Externe

Die Mitarbeiter von Systemintegratoren und die sonstigen Inbetriebnahme- und Service-Mitarbeiter fallen in die beschriebene Kategorie der Externen.

5 Leitlinie zur Informationssicherheit (IS-Leitlinie)

Diese IS-Leitlinie MUSS so ausgeführt werden, dass der gesamte Bereich der Organisation abgedeckt ist. Dies schließt den Produktionsbereich ein.

6 Richtlinien zur Informationssicherheit (IS-Richtlinien)

6.3 Regelungen für Nutzer

Die Mitarbeiter zur Bedienung von Automatisierungssystemen (Operatoren) fällt in die Kategorie Nutzer. Das Bedienen und Beobachten sowie das Engineering von Automatisierungssystemen fällt in die Kategorie der IT-Nutzung.

2.a Eine private Nutzung der IT im Produktionsbereich wird untersagt.

3.a Dies betrifft auch die Automatisierungskomponenten sowie Hard- oder Software, die z. B. zu Zwecken der Diensterbringung, Diagnose, Konfiguration oder Inbetriebnahme von freien Mitarbeitern oder Dienstleistern kurzzeitig in der IT-Infrastruktur der Organisation eingesetzt wird.

Die Integration von IT-Systemen KANN große Auswirkungen auf die Produktion haben (z. B. Störungen verursachen).

Die Freigabe durch einen Administrator SOLL sicherstellen, dass die entsprechenden Basisschutzmaßnahmen (siehe Abschnitt 10.3) umgesetzt werden.

Es KANN im Produktionsbereich auch eine Festlegung erfolgen, dass die Integration eine IT-Systems nicht zulässig ist.

3.c Dies betrifft auch Schutzeinrichtungen für den Personenschutz, z. B. Sensoren und Zuhaltungen an Schutzzäunen (IT-System mit funktionaler Sicherheit).

Ausnahmen KÖNNEN im Organisationsalltag z. B. für bestimmte Nutzer, Nutzergruppen, IT-Systeme oder IT-Systeme-Gruppen sinnvoll und notwendig sein.

7 Mitarbeiter

7.3 Beendigung oder Wechsel der Tätigkeit

3. Schichtzugänge, zu denen der Mitarbeiter Zugriff hatte, sind ebenfalls anzupassen.

8 Wissen

8.1 Aktualität des Wissens

1. Die Hersteller von Automatisierungssystemen liefern teilweise Informationen über bekannt gewordene Schwachstellen ihrer Produkte. Diese sind auf der Webseite des Herstellers einsehbar. Teilweise wird auch ein E-Mail-Service angeboten. Es wird empfohlen, diese Informationen zu nutzen. Darüber hinaus stellen auch staatliche Stellen (z. B. das Bundesamt für Sicherheit in der Informationstechnik, BSI https://www.bsi.bund.de oder das ICS-CERT https://www.us-cert.gov/ics) Informationen in Bezug auf bekannte Schwachstellen von Automatisierungskomponenten zur Verfügung.

8.2 Schulung und Sensibilisierung

4. Einen Anhalt über die erforderlichen Inhalte gibt z. B. der BSI-Standard CS 123.

9 Identifizieren kritischer IT-Ressourcen

Der ISB MUSS die kritischen IT-Ressourcen im Produktionsbereich der Organisation ermitteln und jährlich prüfen, ob die Aufstellung der kritischen IT-Ressourcen aktuell ist und sie bei Bedarf anpassen.

9.1 Prozesse

Produktionsprozesse KÖNNEN zu den zentralen Prozessen oder zu den Prozessen mit hohem Schadenspotential gehören.

Der Produktionsbereich MUSS bei der Ermittlung der zentralen Prozessen und der Prozesse mit hohem Schadenpotential analysiert werden.

9.2 Informationen

Auch im Produktionsbereich KÖNNEN kritische Informationen verarbeitet, übertragen und/oder gespeichert werden.

Der Produktionsbereich MUSS bei der Ermittlung der kritischen Informationen analysiert werden.

9.3 IT-Ressourcen

Auch im Produktionsbereich KÖNNEN kritische IT-Ressourcen (insbesondere kritische Automatisierungskomponenten, kritische Automatisierungssysteme, kritische Verbindungen und kritische Individualsoftware) vorliegen.

Der Produktionsbereich MUSS bei der Ermittlung der kritischen IT-Ressourcen analysiert werden.

10 IT-Systeme

Automatisierungskomponenten sind IT-Systeme und MÜSSEN die Anforderungen der folgenden Abschnitte erfüllen.

10.3 Basisschutz

Die Maßnahmen des Basisschutzes werden u. U. nicht bei allen Automatisierungskomponenten vollständig umzusetzen sein.

Wenn einzelne Maßnahmen des Basisschutzes für Automatisierungskomponenten aufgrund fehlender Funktionalität nicht umgesetzt werden können, SOLLTE dem dadurch entstehenden Risiko durch eine Risikoanalyse und -behandlung (siehe Anhang A 2) begegnet werden.

Wenn einzelne Maßnahmen des Basisschutzes für Automatisierungskomponenten nicht umgesetzt werden, obwohl eine entsprechende Funktionalität vorhanden ist, MUSS dem dadurch entstehenden Risiko durch eine Risikoanalyse und -behandlung (siehe Anhang A.2) begegnet werden.

In der Regel verfügen Automatisierungssysteme über eine eigene Uhrzeitführung, die den Echtzeitanforderungen des Systems genügt. Damit Protokolldaten ggf. übergreifend (in der

gesamten Organisation) ausgewertet werden können, MÜSSEN die Uhrzeiten synchronisiert sein. Im Automatisierungssystem wird dies z. B. über eine externe Zeitbasis umzusetzen sein.

10.3.6 Starten von fremden Medien

Ein BIOS-Passwort ist für Automatisierungskomponenten in der Regel nicht realisierbar.

10.3.7 Authentifizierung

Diese Maßnahme betrifft z. B. die Anmeldung an Engineering- oder Operator-Stationen aber auch die Anmeldung an Web-Interfaces von Automatisierungskomponenten.

3. Diese Maßnahme erfordert nicht zwingend, dass für jedes IT-System individuelle Authentifizierungsmerkmale vergeben werden. Wichtig ist die Entfernung/Änderung der voreingestellten Standard-Authentifizierungsmerkmale.

10.3.8 Zugänge und Zugriffe

Diese Forderung wird u. U. nicht von allen Automatisierungskomponenten unterstützt (Web-Interfaces).

10.4 Zusätzliche Maßnahmen für mobile IT-Systeme

Mobile Automatisierungskomponenten sind mobile IT-Systeme und MÜSSEN die Anforderungen der folgenden Abschnitte erfüllen.

10.5 Zusätzliche Maßnahmen für kritische IT-Systeme

Kritische Automatisierungskomponenten sind wie kritische IT-Systeme zu behandeln. Folgende Maßnahmen MÜSSEN zusätzlich für alle kritischen Automatisierungskomponenten umgesetzt werden.

Wenn Maßnahmen nicht umgesetzt werden, MUSS dem dadurch entstehenden Risiko durch eine Risikoanalyse und -behandlung (siehe Anhang A 2) begegnet werden.

10.5.3 Robustheit

Bei kritischen IT-Systemen MUSS eine Trennung von Produktivsystemen und Entwicklungs- bzw. Testsystemen umgesetzt sein.

Jeder aktivierte Dienst, der einen Netzwerkzugriff auf das IT-System ermöglicht, stellt ein Risiko dar, da durch diesen ein Kompromittieren des IT-System möglich sein KANN.

Ungenutzte Netzwerkdienste MÜSSEN unzugänglich gemacht werden.

10.5.5 Änderungsmanagement

Änderungen sind z. B. Konfigurationsänderungen, Installieren neuer Software, Einspielen von Updates oder Änderungen an der Hardware.

Es ist nicht definiert, wie Tests und Freigaben erfolgen müssen, sondern es wird lediglich eine vom Produktivsystem getrennte Testumgebung gefordert. Obwohl Änderungen an kritischen IT-Systemen vor ihrer Umsetzung in einer Testumgebung geprüft und freigegeben werden müssen, können sie noch immer zu Störungen oder zu Ausfällen der Produktivsysteme führen. Deshalb MUSS ein Mechanismus vorhanden sein, der in diesem Fall die

Rückkehr zum ursprünglichen Zustand (und damit zum Regelbetrieb) innerhalb der maximal tolerierbaren Ausfallzeit (MTA) sicherstellt, sofern keine Ersatzsystem oder -verfahren verfügbar sind (siehe Abschnitt 10.5.9).

Der geforderte Mechanismus KANN eine Teilmenge des entsprechenden Wiederanlaufplans für das kritische IT-System (siehe Abschnitt 17.3) sein.

10.5.8 Überwachung

Diese Funktion wird für Automatisierungssysteme bzw. für die einzelnen Automatisierungskomponenten in der Regel über die Operator-Station oder die Engineering-Station zur Verfügung gestellt.

Die Ressourcen kritischer Automatisierungskomponenten (z. B. Speicherplatz, Prozessorauslastung, Verbindungen) SOLLTEN überwacht werden, damit sich anbahnende Probleme und Störungen schon im Vorfeld erkannt und beseitigt werden können.

10.5.9 Ersatzsysteme und -verfahren

Automatisierungssysteme sind z. T. in hochverfügbaren Ausführungen verfügbar (1 aus 2 Redundanz). In vielen Fällen wird bei kritischen IT-Systemen im Automatisierungsbereich eine hochverfügbare, redundante Ausführung zum Einsatz kommen.

10.5.10 Kritische Individualsoftware

Dies gilt auch für kritische Individualsoftware, die für den Einsatz im Produktionsbereich vorgesehen ist.

11 Netzwerke und Verbindungen

Die Maßnahmen dieses Kapitels MÜSSEN für alle Automatisierungsnetzwerke umgesetzt werden.

11.1 Netzwerkplan

1. physikalische Netzwerkstruktur

   a. Diese KÖNNEN z. B. Switche oder Router sein.
   b. Diese KÖNNEN z. B. Kabel, Funkstrecke oder optische Verbindungen sein.

2. logische Netzwerkstruktur

   b. Diese KÖNNEN z. B. VPN-Tunnel sein.
   d. Unter einem weniger oder nicht vertrauenswürdigen Netzwerk ist z. B. ein Netzwerk zu verstehen, das nicht unter der administrativen Kontrolle der Organisation steht. Hierunter fallen in der Regel die Netze von Providern, Dienstleistern, Partnern und das Internet.

11.3 Netzübergänge

1. Die Umsetzung dieser Maßnahme setzt voraus, dass die angestrebten Verkehrsbeschränkungen definiert sind. Die Verkehrsbeschränkungen werden durch Abschnitt 11.4.2 und Abschnitt 11.4.3 vorgegeben: Diese Maßnahmen fordern, dass nur die unbedingt benötigten Verbindungen erlaubt sein dürfen (Whitelist).

Ob die Verkehrsbeschränkungen wirksam umgesetzt wurden, KANN anhand der Durchsicht der Konfiguration oder anhand eines Port-Scans geprüft werden.

11.4 Basisschutz

11.4.2 Segmentierung

Die Segmentierung MUSS so gestaltet werden, dass der Produktionsbereich von den restlichen Teilen der Organisation separiert wird.

Die Notwendigkeit einer weiteren Segmentierung innerhalb des Produktionsbereichs MUSS geprüft werden.

11.4.4 Netzwerkkopplung

In der Praxis fordert diese Maßnahme eine verschlüsselte Verbindung und die Authentifizierung der Teilnehmer (wie dies z. B. ein VPN umsetzt) oder die Definition des zwischengeschalteten Netzes als vertrauenswürdig (wie z. B. das MPLS-Netzwerk des Providers).

12 Mobile Datenträger

Es KANN im Produktionsbereich auch eine Festlegung erfolgen, dass der Einsatz von mobilen Datenträgern nicht zulässig ist. In diesem Fall KANN es notwendig sein, alternative Möglichkeiten wie das Einschleusen von Daten über spezielle IT-Systeme (Datenschleuse) oder über eine demilitarisierte Zone (DMZ) zu etablieren.

13 Umgebung

Die Maßnahmen dieses Kapitels MÜSSEN für alle Automatisierungskomponenten und das Automatisierungsnetzwerk umgesetzt werden.

15 Zugänge und Zugriffsrechte

Dies betrifft auch die Zugänge zu Automatisierungskomponenten.

16 Datensicherung und Archivierung

Die Automatisierungssysteme sind in die Datensicherung und Archivierung einzubeziehen.

16.2 Archivierung

Dies betrifft auch die Archivdaten von Automatisierungssystemen.

16.3 Verfahren

1. Dies betrifft auch die Archivdaten von Automatisierungssystemen.
2. Dies betrifft auch die Archivdaten von Automatisierungssystemen.

Dies betrifft auch die Archivdaten von Automatisierungssystemen.

16.4 Weiterentwicklung

Dies betrifft auch die Archivdaten von Automatisierungssystemen.

16.5 Basisschutz

16.5.1 Speicherorte

Dies betrifft auch die Archivdaten von Automatisierungssystemen.

16.5.2 Server

Dies betrifft auch die Server des Automatisierungssystems.

16.6 Zusätzliche Maßnahmen für kritische IT-Systeme

Automatisierungssysteme KÖNNEN kritische IT-Systeme sein.

16.6.2 Verfahren

Automatisierungssysteme KÖNNEN kritische IT-Systeme sein.

17 Störungen und Ausfälle

Diese Bestimmungen schließen Störungen und Ausfälle im Produktionsbereich ein.

18 Sicherheitsvorfälle

Diese Bestimmungen schließen Sicherheitsvorfälle im Produktionsbereich ein.