SIEMENS

Ausgabe 02/2025

KONFORMITÄTSERKLÄRUNG ERES

SIMATIC

SIMATIC PCS 7 V10.0

Elektronische Aufzeichnungen / Elektronische Unterschriften

siemens.com/pharma

SIEMENS

SIMATIC

SIMATIC PCS 7 V10.0 Konformitätserklärung ERES

Produktinformation

Elektronische Aufzeichnungen /
Elektronische Unterschriften (ERES)

02/2025
A5E54273651-AA

Rechtliche Hinweise

Warnhinweiskonzept

Dieses Handbuch enthält Hinweise, die Sie zu Ihrer persönlichen Sicherheit sowie zur Vermeidung von Sachschäden beachten müssen. Die Hinweise zu Ihrer persönlichen Sicherheit sind durch ein Warndreieck hervorgehoben, Hinweise zu alleinigen Sachschäden stehen ohne Warndreieck. Je nach Gefährdungsstufe werden die Warnhinweise in abnehmender Reihenfolge wie folgt dargestellt.

⚠ **GEFAHR**
bedeutet, dass Tod oder schwere Körperverletzung eintreten **wird**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

⚠ **WARNUNG**
bedeutet, dass Tod oder schwere Körperverletzung eintreten **kann**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

⚠ **VORSICHT**
bedeutet, dass eine leichte Körperverletzung eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

ACHTUNG
bedeutet, dass Sachschaden eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

Beim Auftreten mehrerer Gefährdungsstufen wird immer der Warnhinweis zur jeweils höchsten Stufe verwendet. Wenn in einem Warnhinweis mit dem Warndreieck vor Personenschäden gewarnt wird, dann kann im selben Warnhinweis zusätzlich eine Warnung vor Sachschäden angefügt sein.

Qualifiziertes Personal

Das zu dieser Dokumentation zugehörige Produkt/System darf nur von für die jeweilige Aufgabenstellung **qualifiziertem Personal** gehandhabt werden unter Beachtung der für die jeweilige Aufgabenstellung zugehörigen Dokumentation, insbesondere der darin enthaltenen Sicherheits- und Warnhinweise. Qualifiziertes Personal ist auf Grund seiner Ausbildung und Erfahrung befähigt, im Umgang mit diesen Produkten/Systemen Risiken zu erkennen und mögliche Gefährdungen zu vermeiden.

Bestimmungsgemäße Verwendung von Siemens-Produkten

Beachten Sie Folgendes:

⚠ **WARNUNG**
Siemens-Produkte dürfen nur für die im Katalog und in der zugehörigen technischen Dokumentation vorgesehenen Einsatzfälle verwendet werden. Falls Fremdprodukte und -komponenten zum Einsatz kommen, müssen diese von Siemens empfohlen bzw. zugelassen sein. Der einwandfreie und sichere Betrieb der Produkte setzt sachgemäßen Transport, sachgemäße Lagerung, Aufstellung, Montage, Installation, Inbetriebnahme, Bedienung und Instandhaltung voraus. Die zulässigen Umgebungsbedingungen müssen eingehalten werden. Hinweise in den zugehörigen Dokumentationen müssen beachtet werden.

Marken

Alle mit dem Schutzrechtsvermerk ® gekennzeichneten Bezeichnungen sind eingetragene Marken der Siemens Aktiengesellschaft. Die übrigen Bezeichnungen in dieser Schrift können Marken sein, deren Benutzung durch Dritte für deren Zwecke die Rechte der Inhaber verletzen kann.

Haftungsausschluss

Wir haben den Inhalt der Druckschrift auf Übereinstimmung mit der beschriebenen Hard- und Software geprüft. Dennoch können Abweichungen nicht ausgeschlossen werden, so dass wir für die vollständige Übereinstimmung keine Gewähr übernehmen. Die Angaben in dieser Druckschrift werden regelmäßig überprüft, notwendige Korrekturen sind in den nachfolgenden Auflagen enthalten.

Siemens Aktiengesellschaft
Digital Industries
Postfach 48 48
90026 NÜRNBERG
DEUTSCHLAND

A5E54273651-AA
Ⓟ 02/2025 Änderungen vorbehalten

Inhaltsverzeichnis

Einleitung

1

In der Life-Science-Industrie werden wichtige Entscheidungen auf Basis von Aufzeichnungen getroffen, die gesetzlichen Vorschriften unterliegen und die zunehmend elektronisch erzeugt, verarbeitet und gespeichert werden. Auch Prüfungen und Freigaben dieser Daten erfolgen auf elektronischem Wege. Aus diesem Grund ist das richtige Management elektronischer Aufzeichnungen und elektronischer Unterschriften für die Life-Science-Industrie zu einem wichtigen Thema geworden.

Dementsprechend haben Aufsichtsbehörden Kriterien festgelegt, bei deren Erfüllung elektronische Aufzeichnungen und elektronische Unterschriften als ebenso zuverlässig und vertrauenswürdig wie Aufzeichnungen in Papierform bzw. handschriftliche Unterschriften auf Papier zu betrachten sind. Diese Anforderungen wurden von der US-Aufsichtsbehörde Food and Drug Administration (FDA) in den Vorschriften von 21 CFR Part 11 (21 CFR Part 11 Electronic Records; Electronic Signatures, US FDA, 1997; kurz: *Part 11*) formuliert und von der Europäischen Kommission im Anhang 11 des EU-GMP-Leitfadens (EU Guidelines to Good Manufacturing Practice, Volume 4, Annex 11: Computerised Systems, European Commission, 2011; kurz: *Annex 11*) verankert.
Da die Anforderungen an elektronische Aufzeichnungen und elektronische Unterschriften immer ein validiertes computergestütztes System voraussetzen, beinhalten beide Regelwerke auch Vorschriften zur Validierung und zum Lebenszyklus des computergestützten Systems.

Die Anwendung von *Part 11* und *Annex 11* (bzw. dessen jeweilige Umsetzung in nationales Recht) ist bei der Verwendung elektronischer Aufzeichnungen und Unterschriften zwingend erforderlich. Diese Vorschriften finden jedoch nur im Rahmen ihres Geltungsbereichs Anwendung.
Der Geltungsbereich beider Regelwerke wird durch den regionalen Markt definiert, auf dem das pharmazeutische Fertigerzeugnis vertrieben wird, und durch die Tatsache, ob computergestützte Systeme und elektronische Aufzeichnungen als Teil GMP-relevanter Aktivitäten eingesetzt werden (siehe Part 11.1 und Annex 11, Grundsätze).

Ergänzend zu den Vorschriften wurden zur Unterstützung bei deren Umsetzung in den vergangenen Jahren diverse Leitfadendokumente, Leitfäden zur guten Praxis und Interpretationshilfen veröffentlicht. Auf einige dieser Veröffentlichungen wird im vorliegenden Dokument Bezug genommen.

Als Hilfe für Kunden hat Siemens als Lieferant von SIMATIC PCS 7 das System im Hinblick auf diese Anforderungen bewertet und die Ergebnisse in der vorliegenden Konformitätserklärung veröffentlicht.

SIMATIC PCS 7 V10.0 erfüllt die funktionalen Anforderungen an elektronische Aufzeichnungen und elektronische Unterschriften in vollem Umfang.

Der vorschriftskonforme Betrieb ist in Verbindung mit Maßnahmen und Verfahrenskontrollen gewährleistet, die durch das regulierte Unternehmen festzulegen sind. Solche Verfahrenskontrollen werden im Kapitel "Bewertungsliste für SIMATIC PCS 7 (Seite 19)" des vorliegenden Dokuments genannt.

Das Dokument berücksichtigt die neuen Funktionen mit der Option SIMATIC PCS 7 Audit in PCS 7 V10.0 Update Collection UC02.

Das vorliegende Dokument gliedert sich in drei Teile:

1. Das Kapitel "Die Anforderungen im Überblick (Seite 7)" enthält eine kurze Beschreibung der verschiedenen Anforderungsthemen.
2. Im Kapitel "Erfüllung der Anforderungen durch SIMATIC PCS 7 (Seite 9)" wird die Funktionalität von SIMATIC PCS 7 vorgestellt, mittels derer diese Anforderungen erfüllt werden.
3. Das Kapitel "Bewertungsliste für SIMATIC PCS 7 (Seite 19)" enthält eine ausführliche Systembewertung anhand der einzelnen Anforderungen der entsprechenden Vorschriften.

Die Anforderungen im Überblick

2

Durch die Anforderungen aus Annex 11 und Part 11 sollen regulierte elektronische Aufzeichnungen und elektronische Unterschriften (kurz: ERES für "Electronic Records / Electronic Signatures") vor Manipulationen, Fehlinterpretationen und nicht nachvollziehbaren Änderungen geschützt werden.

Der Begriff "elektronische Aufzeichnung" bezieht sich auf jede beliebige Kombination aus Text, Grafik, Daten, auditiven, bildlichen oder sonstigen Informationen in digitaler Form, die zur Nutzung in einem regulierten Prozess mit einem Computersystem erstellt, geändert, gepflegt, archiviert, abgerufen oder verteilt werden.

Die "elektronische Unterschrift" stellt ein rechtlich bindendes Äquivalent zur handschriftlichen Unterschrift dar. Die Abgabe der Unterschrift ist hierbei ein technischer Vorgang zur Identifizierung des Unterzeichnenden, wohingegen die Darstellung der Unterschrift in Zusammenhang mit der unterschriebenen Aktion Bestandteil der elektronischen Dokumentation wird. Da elektronische Unterschriften ebenfalls als elektronische Aufzeichnungen gelten, werden sämtliche Anforderungen an elektronische Aufzeichnungen auch an elektronische Unterschriften gestellt.

Die folgende Tabelle gibt einen Überblick über die Anforderungen beider Regelwerke.

Anforderung	Beschreibung
Lebenszyklus und Validierung von computergestützten Systemen	Computergestützte Systeme, die im Rahmen von GMP-bezogenen Aktivitäten eingesetzt werden, müssen validiert werden. Der Validierungsprozess ist mittels eines risikobasierten Ansatzes festzulegen. Er muss sämtliche relevanten Schritte des Lebenszyklus abdecken und eine angemessene Dokumentation beinhalten. Die Funktionalität des Systems muss über den gesamten Lebenszyklus hinweg in Form von Spezifikationen oder einer Systembeschreibung nachvollziehbar dokumentiert werden. Ein formales Verfahren zur Kontrolle von Änderungen und ein Verfahren zum Management von Vorfällen sind einzurichten. Durch regelmäßige Evaluierung ist zu bestätigen, dass der validierte Zustand des Systems aufrechterhalten wird.
Lieferanten und Dienstleister	Da sowohl Kompetenz als auch Zuverlässigkeit der Lieferanten und Dienstleister eine wichtige Rolle spielen, sollte die Lieferantenbeurteilung anhand eines risikobasierten Ansatzes erfolgen. Zwischen dem regulierten Unternehmen und diesen Dritten müssen formale Vereinbarungen bestehen, in denen u. a. die Verantwortlichkeiten und Zuständigkeiten des Dritten klar geregelt sind.

Anforderung	Beschreibung
Datenintegrität	Nach den Anforderungen beider Regelwerke müssen sowohl elektronische Aufzeichnungen als auch elektronische Unterschriften ebenso zuverlässig und vertrauenswürdig sein wie Aufzeichnungen in Papierform. Das System muss über die Möglichkeit verfügen, geänderte Aufzeichnungen zu erkennen. Integrierte Prüfungen auf ordnungsgemäßen und sicheren Umgang mit Daten sind für manuell eingegebene Daten und für mit anderen Systemen elektronisch ausgetauschte Daten vorzusehen. Die Fähigkeit des Systems, korrekte und vollständige Kopien zu erzeugen, ist für die Verwendung von elektronischen Aufzeichnungen im regulierten Umfeld unerlässlich. Gleiches gilt für die Zugänglichkeit, Lesbarkeit und Integrität archivierter Daten während der Aufbewahrungsfrist.
Audit Trail, Unterstützung der Änderungskontrolle	Neben der im Lebenszyklus definierten Kontrolle von Änderungen am System verlangen beide Regelwerke, dass auch Änderungen an GMP-relevanten Daten aufgezeichnet werden. Ein solcher Audit Trail sollte Informationen zur Änderung (vorher/nachher), zur Identität des Bedieners, einen Zeitstempel sowie den Grund für die Änderung umfassen.
Systemzugriff, Benutzerkennungen und Passwörter	Der Zugriff auf das System muss ausschließlich auf berechtigte Personen beschränkt sein. Der Passwortsicherheit ist dabei besondere Aufmerksamkeit zu widmen. Änderungen an der Konfiguration der Benutzerzugriffsverwaltung müssen aufgezeichnet werden. Die Gültigkeit von Benutzerkennungen ist in regelmäßigen Abständen zu prüfen. Es müssen Verfahren zur Aufhebung von Zugriffsrechten beim Ausscheiden einer Person und für das Schadensmanagement bei Verlust existieren. Dem Einsatz von Geräten, die Benutzerkennungen oder Passwortinformationen enthalten oder erzeugen, ist besondere Aufmerksamkeit zu widmen.
Elektronische Unterschrift	Aus der Sicht der Regelwerke sind elektronische Unterschriften rechtlich bindend und in jeder Hinsicht auf Papier geleisteten handschriftlichen Unterschriften gleichwertig. Über die genannten Anforderungen an Benutzerkennungen und Passwörter hinaus müssen elektronische Unterschriften außerdem einer Person eindeutig zugeordnet werden können. Sie müssen mit der zugehörigen elektronischen Aufzeichnung verknüpft sein und dürfen weder kopiert noch anderweitig geändert werden.
Offene Systeme	Bei offenen Systemen können zur Sicherstellung der Datenintegrität und Vertraulichkeit weitere Kontrollen oder Maßnahmen erforderlich sein.

Erfüllung der Anforderungen durch SIMATIC PCS 7 3

Die Empfehlungen von Siemens hinsichtlich Systemarchitektur, Konzeption und Konfiguration unterstützen Systembenutzer bei der Erreichung der Konformität. Weitere Informationen und Hilfen enthält das „GMP Engineering Handbuch SIMATIC PCS 7" von Siemens.

Die im Kapitel "Die Anforderungen im Überblick (Seite 7)" dargestellten Anforderungen können, wie im Folgenden gezeigt, durch das System unterstützt werden.

Die Datensteuerungs-Grundsätze eines regulierten Unternehmens beziehen sich auf Personen, Prozesse und Techniken.

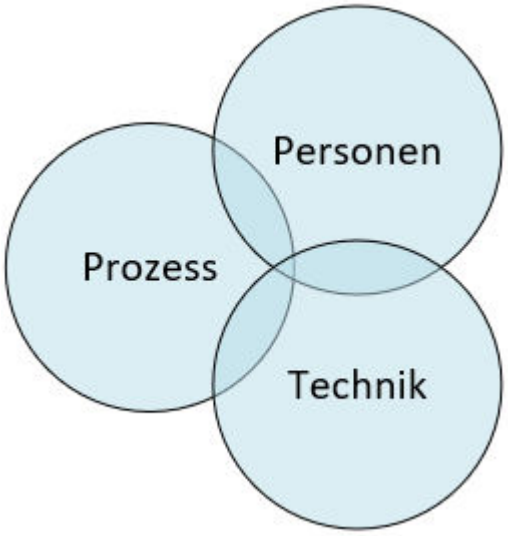


Bild 3-1 Elemente der Datensteuerung

Nur die Summe aller Maßnahmen kann erreichen, dass das System konform mit den gesetzlichen Vorgaben betrieben wird.

- Prozess: Prozeduren z. B. für Betrieb, Änderungsmanagement, Validierung und Archivierung
- Personen: geeignete Qualifikation und Schulung der Mitarbeiter sowie Befolgen der etablierten Prozesse
- Technik: Auswahl und Funktionalität der Basis-Komponenten als auch spezifische Konfiguration für den Anwendungsfall

3.1 Lebenszyklus und Validierung von computergestützten Systemen

Bereits im Annex 11 von 1992 bzw. im Part 11 von 1997 verlangte der Gesetzgeber, dass computergestützte Systeme zu validieren seien. Kriterien für die Validierung des Systems und dessen Lebenszyklus wurden in der überarbeiteten Revision des Annex 11 von 2011 ergänzt.

Anforderungen an die Validierung von computergestützten Systemen und an die Aufrechterhaltung des validierten Zustands sind auch Bestandteil anderer Publikationen, so zum Beispiel den Baseline Guides (Leitfäden), den GAMP Guides und den GAMP Good Practice Guides des Industrieverbands ISPE (International Society of Pharmaceutical Engineers (https://www.ispe.org)).

Folglich sollten der System-Lebenszyklus und der Validierungsansatz unter Berücksichtigung der Empfehlungen des GAMP 5-Leitfadens (GAMP 5 - Ein risikobasierter Ansatz für konforme GxP-computergestützte Systeme) definiert werden. Auch Themen wie Lifecycle Management, Systementwicklung und Betrieb von computergestützten Systemen werden in den GAMP Guides ausführlich behandelt.

3.2 Lieferanten und Dienstleister

Lieferanten von Systemen und Lösungen sowie Dienstleister sollten angemessen bewertet werden, siehe GAMP 5, Anhang M2. Als Hersteller von Hardware- und Softwarekomponenten befolgt Siemens interne Verfahren zum Product Lifecycle Management und arbeitet entsprechend einem Qualitätsmanagementsystem, das von einem externen Zertifizierungsunternehmen regelmäßig überprüft und zertifiziert wird.

3.3 Datenintegrität

Regulierte Unternehmen sollten ganzheitliche Strategien zur Datenintegrität implementieren. Von besonderem Interesse sind hierbei jene Daten, die für Entscheidungen verwendet werden, die Auswirkungen auf die Produktqualität und auf die Sicherheit der Patienten haben.

Die Verlässlichkeit der Daten setzt ein hohes Maß an Datenintegrität über den gesamten Aufbewahrungszeitraum voraus und erstreckt sich auch auf das Archivieren und Abrufen von Daten.

Darüber hinaus muss das System über die Möglichkeit verfügen, ungültige oder geänderte Aufzeichnungen zu erkennen. Auf Seiten des Computersystems tragen Funktionalitäten wie z. B. Zugriffsschutz, Audit Trail, Datentypprüfungen, Prüfsummen, Datensicherung/-wiederherstellung und Datenarchivierung/-abruf zum Erhalt der Datenintegrität bei. Diese Maßnahmen und technischen Eigenschaften werden ergänzt durch die Systemvalidierung, geeignete Arbeitsprozeduren und Personalschulungen.

IT Security

Auch IT Security ist eine unabdingbare Voraussetzung, um Datenintegrität zu erreichen und zu bewahren. Support durch Siemens finden Sie unter Industrial Cybersecurity Services. (https://new.siemens.com/de/de/produkte/services/digital-enterprise-services/industrial-security-services.html)

Kontinuierliche Archivierung

SIMATIC PCS 7 bietet ein konfigurierbares und skalierbares Archivierungskonzept. Meldungen und Messwerte werden kontinuierlich in systemeigenen Archiven abgelegt. Diese lokal archivierten Daten können automatisch in ein Langzeitarchiv wie z. B. Process Historian übertragen werden. Durch die Generierung von Prüfsummen werden Manipulationen an den Archivdaten erkannt. Die Archivdaten können während des gesamten Aufbewahrungszeitraums abgerufen werden. Die Daten können in SIMATIC PCS 7 entweder mithilfe von Standardfunktionen oder über zusätzliche Standardschnittstellen bzw. mit Optionspaketen abgerufen werden. Weitere Hinweise enthält das PCS 7 OS Projektierungshandbuch.

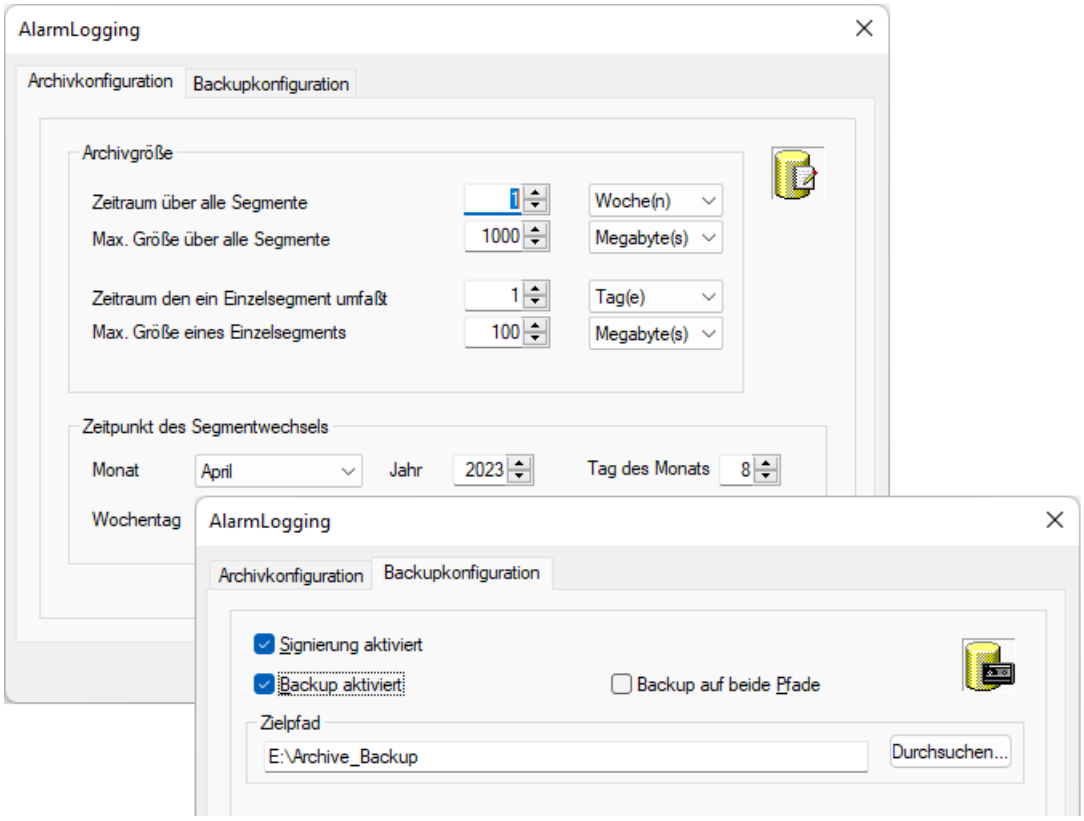


Bild 3-2 Konfiguration der Archivierungsstrategie

Chargenorientierte Archivierung

Mit SIMATIC BATCH kann eine chargenorientierte Datenarchivierung durchgeführt werden. Die Daten können zur Langzeitarchivierung mittels der hier genannten Hilfsmittel verwaltet werden.

SIMATIC PCS 7 und SIMATIC BATCH bieten Standard-Schnittstellen zu verschiedenen Archivierungslösungen an, u.a. Process Historian. Weitere Hinweise enthält das SIMATIC BATCH Projektierungshandbuch.

3.4 Audit Trail, Unterstützung der Änderungskontrolle

„Audit Trails sind besonders dort wichtig, wo der Benutzer regulierte Aufzeichnungen während des normalen Betriebes erstellen, ändern oder löschen darf." (Guidance for Industry Part 11 – Scope and Application, FDA, 2003)

Audit Trails sind nicht erforderlich für automatisch erzeugte elektronische Aufzeichnungen, die vom Bediener weder geändert noch gelöscht werden können. Das System stellt für solche elektronischen Aufzeichnungen ausreichende Systemsicherheitsmechanismen zur Verfügung.

Änderungen an der Konfiguration eines validierten Systems unterliegen einem Änderungsverfahren und müssen entsprechend kontrolliert werden. Dies kann durch Versionierung, Systemlogs und ähnliche Mittel unterstützt werden. Die nachfolgenden Abschnitte unterscheiden daher zwischen den Anforderungen an Audit Trails im laufenden Betrieb und der Kontrolle von Konfigurationsänderungen im Engineering.

Aufzeichnungen im laufenden Betrieb

Aufzeichnung von Batchdaten

Alle chargenrelevanten Aufzeichnungen werden in einem Chargenprotokoll dokumentiert, inklusive Bedieneingriffen und elektronische Unterschriften.

Die Chargenprotokolle können im XML- und PDF-Dateiformat abgespeichert werden. SIMATIC PCS 7 und SIMATIC BATCH bieten keine Bedienmöglichkeiten, um diese Daten zu ändern. Manipulationen direkt an diesen Dateien sind über die Sicherheitseinstellungen des Betriebssystems zu unterbinden.

Mit SIMATIC PCS 7 Audit können zusätzlich Bedienereignisse aus SIMATIC BATCH in der Audit-Datenbank des SIMATIC Process Historian aufgezeichnet werden. Sie stehen somit der Berichterstellung im SIMATIC Information Server zur Verfügung.

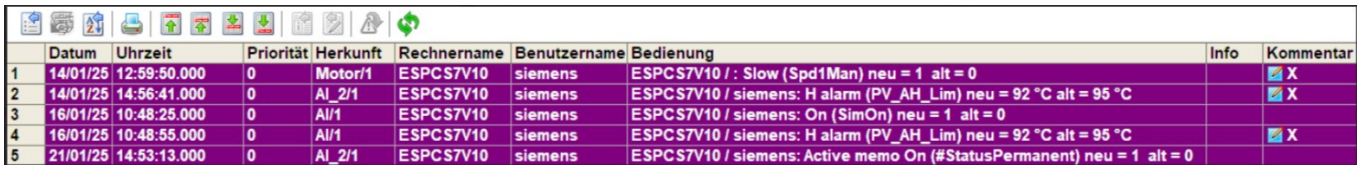
Aufzeichnung von Prozessdaten

Prozessdaten (im Wesentlichen also Prozesswerte, Alarme und Meldungen) werden gespeichert, ohne dass der Bediener die Möglichkeit hat, Änderungen vorzunehmen.

Bedienereingaben im laufenden Betrieb

Alle Änderungen und Eingaben relevanter Daten, die der Bediener im laufenden Betrieb vornimmt, werden in einem Audit Trail protokolliert.

Im Meldearchiv von SIMATIC PCS 7 werden daher die erforderlichen Ereignisse und Informationen (Alter Wert, Neuer Wert, Benutzer-ID, Datums- und Zeitstempel, bei Bedarf Begründung) aufgezeichnet. Ein Bericht hierzu kann gemäß vorher definierter Filterkriterien ausgedruckt werden.



	Datum	Uhrzeit	Priorität	Herkunft	Rechnername	Benutzername	Bedienung	Info	Kommentar
1	14/01/25	12:59:50.000	0	Motor/1	ESPCS7V10	siemens	ESPCS7V10 / : Slow (Spd1Man) neu = 1 alt = 0		X
2	14/01/25	14:56:41.000	0	AI_2/1	ESPCS7V10	siemens	ESPCS7V10 / siemens: H alarm (PV_AH_Lim) neu = 92 °C alt = 95 °C		X
3	16/01/25	10:48:25.000	0	AI/1	ESPCS7V10	siemens	ESPCS7V10 / siemens: On (SimOn) neu = 1 alt = 0		
4	16/01/25	10:48:55.000	0	AI/1	ESPCS7V10	siemens	ESPCS7V10 / siemens: H alarm (PV_AH_Lim) neu = 92 °C alt = 95 °C		X
5	21/01/25	14:53:13.000	0	AI_2/1	ESPCS7V10	siemens	ESPCS7V10 / siemens: Active memo On (#StatusPermanent) neu = 1 alt = 0		

Bild 3-3 Anzeige der Bedienmeldungen im Alarm Logging

GMP-relevanter Audit Trail

Es können GMP-relevante Parameter im Engineering angewählt werden, die bei Bedienung zur Laufzeit einen verpflichtenden Kommentar (Begründung) erhalten sollen. Mit SIMATIC PCS 7 Audit werden diese Ereignisse dann in die Audit-Datenbank des SIMATIC Process Historian geschrieben. Über den SIMATIC Information Server kann ein Audit Trail Report erstellt werden.

Konfigurationskontrolle

Im Gegensatz zum Audit Trail unterliegen Änderungen an der Systemkonfiguration dem Verfahren der Änderungskontrolle.

Solche Änderungen werden vor ihrer Ausführung geplant, ihre potenzielle Auswirkung bewertet, während der Ausführung dokumentiert und anschließend auf korrekte Umsetzung getestet.

Die Dokumentation der durchgeführten Änderung kann durch verschiedene Werkzeuge unterstützt werden.

Änderungen im Batchsystem

SIMATIC BATCH unterstützt die Versionierung von Rezepten, Formulas und ROP-Library Objekten. Weiterhin wird jeweils mit Zeit/Datumsstempel der Ersteller dokumentiert, wer das Rezept editiert und wer es freigegeben hat. Außerdem können mit dem Rezeptvergleicher Unterschiede zwischen den Rezeptversionen dargestellt werden.

Mit SIMATIC PCS 7 Audit können zusätzlich Ereignisse aus SIMATIC BATCH in die Audit-Datenbank des SIMATIC Process Historian übertragen werden.

Änderungen im Engineeringsystem

Mit Hilfe des SIMATIC Version Cross Manager (VXM) können Vergleiche zweier Projekte oder Projektversionen (nicht Multiprojekte) durchgeführt werden.

Die Vergleichsergebnisse können als Datei exportiert werden.

Mit SIMATIC PCS 7 Audit können ausgewählte Ereignisse im Engineeringsystem in die Audit-Datenbank des SIMATIC Process Historian übertragen werden. Dies beinhaltet zum Beispiel das Laden von Änderungen in das Automatisierungssystem.

Änderungen im Automatisierungssystem

Bei aktiviertem Änderungsprotokoll werden Zugriffe vom Engineering System auf das Automatisierungssystem (AS) dokumentiert.

Zusätzlich können mit SIMATIC PCS 7 Audit Eingriffe mit direktem Einfluss zur Laufzeit ausgewählt und in die Audit-Datenbank des SIMATIC Process Historian geschrieben werden. Dort stehen sie zur Auswertung und Protokollierung zur Verfügung.

Änderungen der installierten SIMATIC PCS 7 Systemsoftware

Es stehen verschiedene Bordmittel und Optionen zur Verfügung, um die installierte Software auszulesen und zu dokumentieren, siehe hierzu GMP Engineering Handbuch für PCS 7.

Projektarchivierung

Die Option SIMATIC Version Trail unterstützt eine Archivierung der PCS 7 Projekte mit Vergabe einer Versionskennung. Es kann zwischen Haupt- und Nebenversion unterschieden

werden, auch eine zyklische Archivierung ist möglich. Ältere Projektierungsstände können wieder zurückgelesen werden; der Vergleich zwischen zwei Versionen über den Version Cross Manager zeigt die Unterschiede auf.

In einer Versionshistorie werden die Aktionen wie Anlegen, Ändern, alte Projektierungsstände löschen usw. mit Archivnamen, Datum und Kommentar aufgezeichnet. Damit wird eine lückenlose Dokumentation der verschiedenen Ausgabestände systemseitig erstellt.

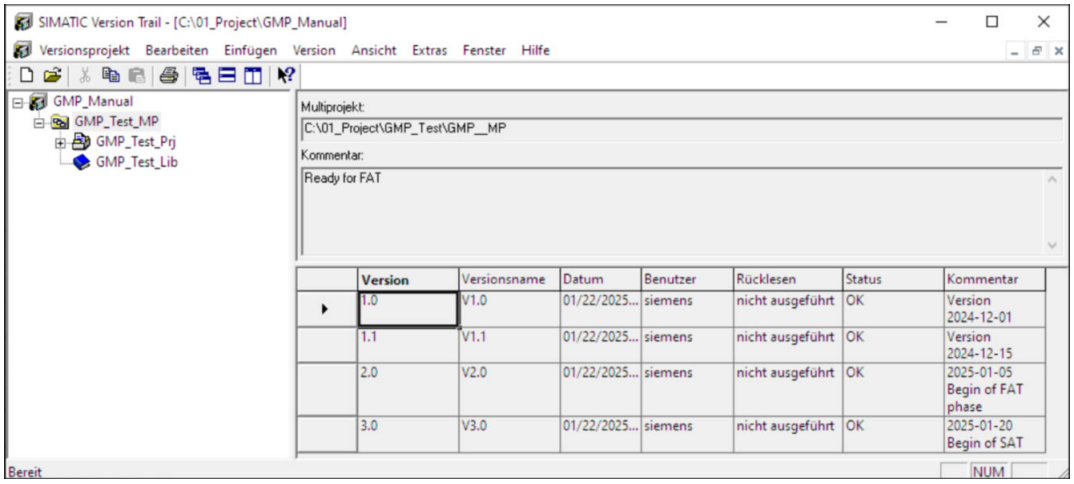


Bild 3-4 Projekt-Versionierung - Archivierung mit SIMATIC Version Trail

Änderungen in der Benutzerverwaltung

Die Änderungen im Rahmen der Benutzerverwaltung (wie z. B. das Einrichten neuer Benutzer, das Sperren von Benutzern, etc.) werden im Ereignisprotokoll von Windows aufgezeichnet. Zu diesem Zweck muss das Ereignisprotokoll entsprechend konfiguriert werden, wie in der Microsoft-Dokumentation beschrieben.

3.5 Systemzugriff, Benutzerkennungen und Passwörter

Benutzer dürfen ausschließlich die erforderlichen Zugriffsrechte erhalten. Hierdurch wird ein unbefugter Zugriff auf das Dateisystem, Verzeichnisstrukturen, Systemdaten und deren unerwünschte Manipulation verhindert.

Die Anforderungen hinsichtlich des Zugriffsschutzes werden in Verbindung mit Verfahrenskontrollen, wie z. B. zur "Festlegung der Rechte und Rollen", vollständig erfüllt.

Adäquate Sicherheitsmechanismen sind eine unabdingbare Voraussetzung für den sicheren Betrieb eines Systems. Dies gilt insbesondere für „offene Pfade“, die durch zusätzliche Maßnahmen abgesichert werden müssen. Grundprinzipien des Sicherheitskonzepts sowie Konfigurationsempfehlungen enthalten das Handbuch „Sicherheitskonzept PCS 7 und WinCC“ sowie das PCS 7 Engineering Kompendium Teil F.

SIMATIC Logon, eine der Grundfunktionen von SIMATIC PCS 7, dient zur Einrichtung einer Benutzerverwaltung auf Basis der Sicherheitsmechanismen von Microsoft Windows:

- Die einzelnen Nutzer und ihre Zuordnung zu Windows-Benutzergruppen werden in der Benutzerverwaltung von Microsoft Windows definiert.
- SIMATIC Logon stellt die Verbindung zwischen den Windows-Benutzergruppen und den Benutzergruppen der SIMATIC-Komponenten wie PCS 7 OS, SIMATIC BATCH, etc. her.
- Basierend auf den Benutzergruppen werden Berechtigungen mit verschiedenen Berechtigungsstufen in der jeweiligen SIMATIC-Komponente (z. B. PCS 7 OS) definiert.
- Projekte eines Multiprojekts können mittels SIMATIC Logon vor nicht autorisiertem Zugriff geschützt werden. Der Zugriff kann dann so konfiguriert werden, dass ein Zugriff nur mit persönlicher Kombination aus Benutzerkennung und Passwort möglich ist.

Damit werden die folgenden Anforderungen an die Zugriffssicherheit erfüllt:

- Zentrale Benutzerverwaltung (Einrichtung, Deaktivierung, Blockierung, Entsperrung, Zuordnung zu Benutzergruppen) durch den Administrator
- Verwendung einer eindeutigen Benutzerkennung
- Definition von Zugriffsberechtigungen für Benutzergruppen/Rollen
- Zugriff und Berechtigungsstufe je nach konkretem Anlagenbereich
- Passworteinstellungen und Passwortalterung
- Erzwingen eines neuen Passworts bei der ersten Anmeldung (Initialpasswort).
- Sperren eines Benutzers nach einer einstellbaren Anzahl von fehlerhaften Anmeldeversuchen
- Automatisches Abmelden (Auto-Logout) nach einer konfigurierbaren Zeit, in der weder Tastatur noch Maus benutzt wurden.
- Log-Funktionen für Aktionen hinsichtlich des Zugriffsschutzes

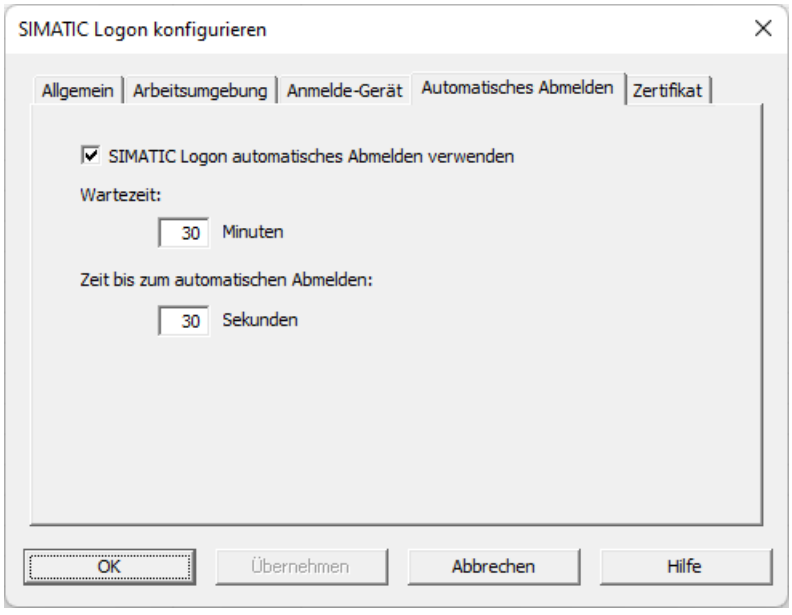


Bild 3-5 Konfiguration von SIMATIC Logon

Zusätzlich müssen den Benutzern bestimmte Zugriffsrechte auf Betriebssystemebene zugewiesen bzw. entzogen werden, um unbefugte Zugriffe auf die Verzeichnisstruktur der verschiedenen Systemprogramme sowie unbeabsichtigte Manipulationen zu verhindern.

3.6 Elektronische Unterschrift

Elektronische Unterschrift in SIMATIC BATCH

SIMATIC Electronic Signature ist ein integraler Bestandteil von SIMATIC Logon.

Der Aufruf des Unterschriften-Dialogs ist standardmäßig in SIMATIC BATCH integriert (z. B. Rezeptfreigabe, Betriebsartwechsel für Chargen, Eingabe im Operatordialog) und wird über die Anlagen- bzw. Objekteigenschaften projektiert. Die Abfrage und Überprüfung der einzugebenden Informationen (Benutzerkennung, Passwort) nimmt SIMATIC Logon vor.

Innerhalb von SIMATIC BATCH werden die technischen Eigenschaften der Unterschrift konfiguriert:

- Was unterschrieben werden soll
- Personen / Gruppen, die signieren müssen
- Abfolge der Unterschriften, falls erforderlich
- Signierung innerhalb der gleichen Sitzung erforderlich oder nicht

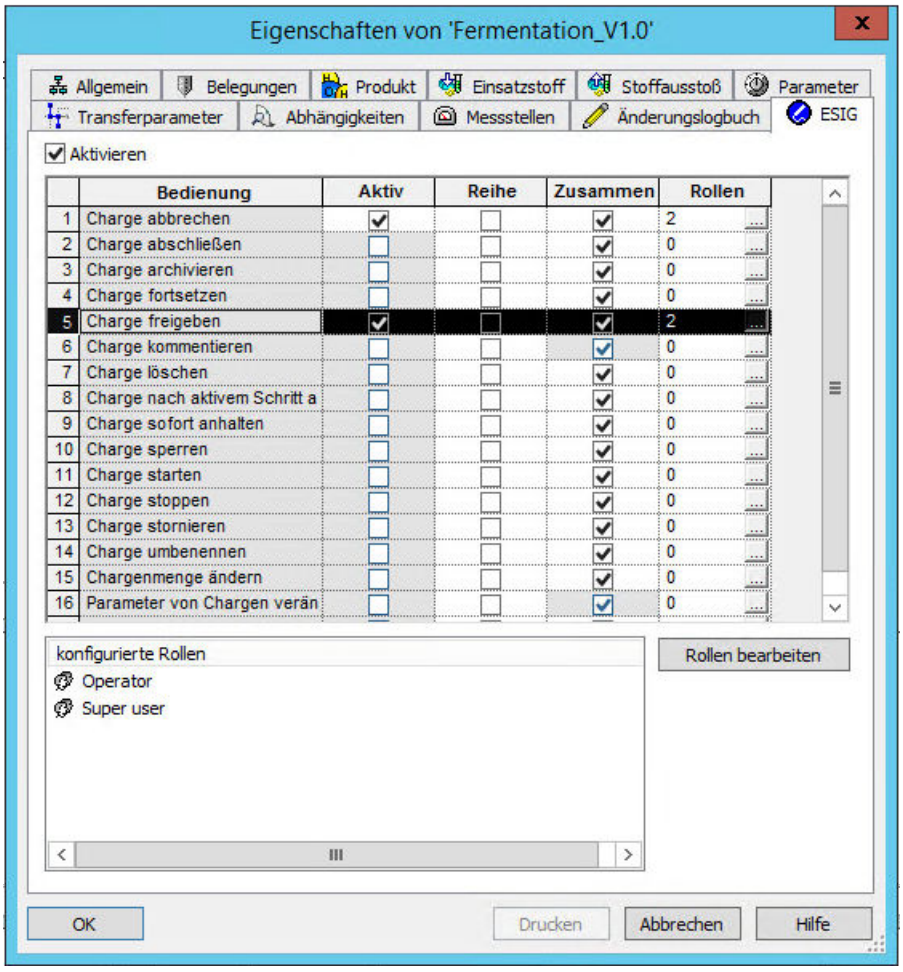


Bild 3-6 Konfiguration der elektronischen Unterschrift für Chargenfreigabe und Parameteränderung

Die Nachvollziehbarkeit der geleisteten Aktionsfreigaben wird durch den Eintrag der elektronischen Unterschrift in das Chargenprotokoll gewährleistet.

Aktion:

ID	Aktion	Login	Bearbeiter	Erzeugt	Ausgeführt	Zustand
1	Charge freigeben	WIN-PINR0BNLR85\Julia Boss	Julia Boss	WIN-PINR0BNLR85 9/2/2021 3:00:25 PM -07:00	WIN-PINR0BNLR85 9/2/2021 3:00:26 PM -07:00	Abgeschlossen

Signaturen

Login	Benutzername	Rechner	Zeit	Zustand
Julia Boss	Julia Boss	WIN-PINR0BNLR85	9/2/2021 2:59:58 PM -07:00	SIGNIERT
	Kommentar	Released!		

Signaturen

Login	Benutzername	Rechner	Zeit	Zustand
Susan Op	Susan Miller	WIN-PINR0BNLR85	9/2/2021 2:58:40 PM -07:00	SIGNIERT
	Kommentar	Everything fine!		

Bild 3-7 Darstellung einer elektronischen Unterschrift im Chargenprotokoll

Elektronische Unterschrift in SIMATIC PCS 7 OS

Mit der Bibliothek PCS 7 Advanced Process Library (APL) kann für bedienbare Parameter ein sogenanntes Audit-Level konfiguriert werden. Hierbei sind die folgenden Levels verfügbar:

- 0 = keine zusätzliche Eingabe erforderlich
- 1 = verpflichtender Kommentar (Begründung für GMP-relevanten Audit Trail)
- 2 = elektronische Unterschrift des eingeloggten Benutzers mit optionalem Kommentar
- 3 = elektronische Unterschrift des eingeloggten Benutzers mit verpflichtendem Kommentar

In der nachfolgenden Abbildung wurde für die obere Alarmgrenze eine elektronische Unterschrift mit verpflichtendem Kommentar konfiguriert. Erst nach Eingabe eines Kommentars und des korrekten Benutzerpasswortes kann die Eingabe mit "OK" abgeschlossen werden. Die Änderung des Grenzwertes von 95 (Altwert) auf 92 (Neuwert) wird wirksam. Für weitere Details siehe das Funktionshandbuch "SIMATIC PCS 7 Advanced Process Library" unter der Beitrags-ID 109973505 im SiePortal (https://support.industry.siemens.com).

Bild 3-8 Elektronische Unterschrift bei einer Parameteränderung über ein Faceplate

Bewertungsliste für SIMATIC PCS 7

4

Die folgende Anforderungsliste beinhaltet sämtliche Anforderungen aus 21 CFR Part 11 und EU-GMP-Leitfaden Annex 11. Alle Anforderungen wurden in diejenigen Themengebiete unterteilt, wie sie bereits in Kapitel "Die Anforderungen im Überblick (Seite 7)" dieser Konformitätserklärung aufgeführt wurden.

Die aufgeführten *Anforderungen* berücksichtigen beide Regelwerke vollständig, und zwar unabhängig davon, ob technische Maßnahmen oder Verfahrensanweisungen oder eine Kombination aus beiden für die vollständige Einhaltung von Part 11 und Annex 11 erforderlich sind.

Die *Antworten* geben u. a. Aufschluss darüber (sofern zutreffend), wie eine Anforderung während der Produktentwicklung gehandhabt wird und welche Maßnahmen während der Konfiguration und des Systembetriebs realisiert werden sollten. Ferner enthalten die Antworten Verweise auf die Produktdokumentation zu technischen Themen und auf den GAMP 5-Leitfaden bei den Verfahrenskontrollen, die dort bereits berücksichtigt wurden.

4.1 Lebenszyklus und Validierung von computergestützten Systemen

Die grundlegende Anforderung, dass ein für GMP-relevante Aktivitäten eingesetztes computergestütztes System zu validieren ist, wird in der Revision des Annex 11 von 2011 durch Anforderungen ergänzt, die Details zu Erwartungen an den Lebenszyklus des Systems enthalten.

	Anforderung	Verweis	Antwort
4.1.1	Ein Risikomanagement ist während der gesamten Lebensdauer des computergestützten Systems durchzuführen.	Annex 11, 1	Ja. Der PLM-Prozess (Product Lifecycle Management) ist der Entwicklungsprozess für Siemens-Softwareprodukte. Dieser Prozess umfasst ein entsprechendes Risikomanagement. Während der Validierung und im Betrieb des Systems ist das Risikomanagement durch das regulierte Unternehmen sicherzustellen.
4.1.2	Durch die Validierung eines Systems werden dessen fehlerfreie Funktion, Zuverlässigkeit, gleichbleibende bestimmungsgemäße Leistung und die Fähigkeit, ungültige oder geänderte Aufzeichnungen zu erkennen, sichergestellt.	21 CFR 11.10 (a)	Ja. Die Entwicklung des Softwareprodukts (COTS, siehe Annex 11, Glossar) unterliegt dem Siemens QMS und dem PLM-Prozess. Das regulierte Unternehmen muss geeignete Maßnahmen zur Validierung der Applikation (siehe Annex 11, Glossar) und zur Aufrechterhaltung des validierten Zustands ergreifen.
4.1.3	Die Validierungsdokumentation erstreckt sich auf alle relevanten Schritte des Lebenszyklus.	Annex 11, 4.1	Ja. Der PLM-Prozess beinhaltet alle relevanten Dokumente. Die Verantwortung für die Validierung der Applikation (siehe Annex 11, Glossar) liegt beim regulierten Unternehmen.

	Anforderung	Verweis	Antwort
4.1.4	Für die Validierung von maßgeschneiderten oder kundenspezifisch angepassten Systemen muss ein Prozess vorhanden sein.	Annex 11, 4.6	Kundenspezifische Applikationen werden im Zuge der Realisierung entsprechend den im Projekt vereinbarten Zuständigkeiten verifiziert. Der Validierungsprozess fällt in den Verantwortungsbereich des regulierten Unternehmens.
4.1.5	Im Rahmen des Validierungsprozesses werden Verfahren zum Management von Änderungen und Abweichungen angewandt.	Annex 11, 4.2	Ja. Der PLM-Prozess beinhaltet Verfahren zum Management von Änderungen und Abweichungen sowie Fehlerkorrekturen. Das regulierte Unternehmen muss geeignete Verfahren zum Management von Änderungen und Abweichungen schaffen (siehe GAMP 5, Anhänge M8 und D5).
4.1.6	Eine aktuelle Bestandsübersicht über alle relevanten Systeme und deren GMP-Funktionalität ist verfügbar. Für kritische Systeme muss eine aktuelle Systembeschreibung [...] verfügbar sein.	Annex 11, 4.3	Das regulierte Unternehmen muss ein geeignetes Berichtswesen, eine Bestandsübersicht über die Systeme sowie Systembeschreibungen realisieren (siehe GAMP 5, Anhang D6).
4.1.7	Die Benutzeranforderungen haben die erforderlichen Funktionen zu beschreiben. Außerdem müssen sie einem risikobasierten Ansatz folgen und über den gesamten Lebenszyklus hinweg verfolgbar sein.	Annex 11, 4.4	Ja. Die Anforderungsspezifikation ist Bestandteil des PLM-Prozesses. Für die projektspezifische Konfiguration muss das regulierte Unternehmen die Benutzeranforderungen im Lebenszyklus des Systems beschreiben (siehe GAMP 5, Anhang D1).
4.1.8	Es ist ein Nachweis über geeignete Testmethoden und Testszenarien zu erbringen.	Annex 11, 4.7	Die Sicherstellung der Eignung von Testmethoden und -szenarien ist ein wesentlicher Bestandteil des PLM-Prozesses sowie der Testplanung. In Bezug auf die Applikation muss das regulierte Unternehmen an der Planung der Teststrategie (siehe GAMP 5, Anhang D5) beteiligt sein bzw. ihr zustimmen.
4.1.9	In Bezug auf die Systemdokumentation sind geeignete Kontrollen durchzuführen. Diese umfassen die Verteilung von, den Zugriff auf und die Verwendung der Dokumentation zur Bedienung und Wartung des Systems.	21 CFR 11.10 (k)	Während der Produktentwicklung wird die Dokumentation als Teil des Produktes behandelt. Somit unterliegt die Dokumentation selbst ebenfalls den Anforderungen an den PLM-Prozess. Während der Entwicklung und des Betriebs eines Produktivsystems muss das regulierte Unternehmen geeignete Verfahrenskontrollen etablieren (siehe GAMP 5, Anhänge M9 und D6).
4.1.10	Im Rahmen eines formalen Änderungskontrollverfahrens für die Systemdokumentation werden Änderungen in chronologischer Reihenfolge aufgezeichnet.	21 CFR 11.10 (k) Annex 11, 10	Während der Produktentwicklung werden Änderungen gemäß dem PLM-Prozess bearbeitet. Während der Entwicklung und des Betriebs des Systems muss das regulierte Unternehmen geeignete Verfahrenskontrollen etablieren (siehe GAMP 5, Anhänge M8 und O6).

	Anforderung	Verweis	Antwort
4.1.11	Personen, die elektronische Aufzeichnungs-/ Unterschriftssysteme entwickeln, pflegen oder nutzen, müssen über die erforderliche Qualifikation, Ausbildung und Erfahrung zur Ausübung der ihnen zugewiesenen Tätigkeit verfügen.	21 CFR 11.10 (i)	Anhand der Prozesse von Siemens wird sichergestellt, dass die Mitarbeiter eine ihren Aufgaben entsprechende Schulung absolviert haben und dass diese Schulung ordnungsgemäß dokumentiert wird. Darüber hinaus bietet Siemens eine Vielfalt an Kursen für Benutzer, Administratoren und Supportpersonal an.
4.1.12	Computergestützte Systeme müssen regelmäßig evaluiert werden, um zu bestätigen, dass sie sich noch im validen Zustand befinden und GMP-konform sind.	Annex 11, 11	Das regulierte Unternehmen muss geeignete Verfahrenskontrollen etablieren (siehe GAMP 5, Anhänge O3 und O8).
4.1.13	Alle Vorfälle sind zu berichten und zu bewerten.	Annex 11, 13	Das SIMATIC-Portfolio beinhaltet Funktionen, die eine Berichterstattung auf verschiedenen Systemebenen unterstützen. Das regulierte Unternehmen hat geeignete Verfahrenskontrollen zu etablieren (siehe GAMP 5, Anhang O5).
4.1.14	Wenn computergestützte Systeme kritische Prozesse unterstützen, sind Vorkehrungen zu treffen, um die kontinuierliche Unterstützung dieser Prozesse bei einem Systemausfall zu gewährleisten.	Annex 11, 16	Das regulierte Unternehmen muss das System in seinem Business-Continuity-Plan angemessen berücksichtigen (siehe GAMP 5, Anhang O10).

4.2 Lieferanten und Dienstleister

Unterhält das regulierte Unternehmen Geschäftsbeziehungen mit Dritten, die sich auf die Planung, Entwicklung, Validierung, den Betrieb und die Wartung eines computergestützten Systems erstrecken, so sind Kompetenz und Zuverlässigkeit dieses Geschäftspartners mithilfe eines risikobasierten Ansatzes zu betrachten.

	Anforderung	Verweis	Antwort
4.2.1	Bei Inanspruchnahme von Dritten müssen zwischen dem Hersteller und dem Dritten formale Vereinbarungen bestehen.	Annex 11, 3.1	Das regulierte Unternehmen ist dafür verantwortlich, dass mit Lieferanten und Dritten formale Vereinbarungen getroffen werden (siehe GAMP 5, Anhang O2).
4.2.2	Kompetenz und Zuverlässigkeit eines Lieferanten spielen bei der Auswahl eines Produkts oder Dienstleisters eine zentrale Rolle. Die Notwendigkeit eines Audits sollte auf einer Risikobewertung basieren.	Annex 11, 3.2 Annex 11, 4.5	Das regulierte Unternehmen muss seine Lieferanten entsprechend bewerten (siehe GAMP 5, Anhang M2).
4.2.3	Das regulierte Unternehmen muss sicherstellen, dass das System gemäß einem geeigneten Qualitätsmanagementsystem entwickelt wurde.	Annex 11, 4.5	Die Entwicklung von SIMATIC-Produkten erfolgt gemäß dem im Siemens Qualitätsmanagementsystem festgelegten PLM-Prozess.

	Anforderung	Verweis	Antwort
4.2.4	Die Dokumentation von kommerziell erhältlichen Standardprodukten ist vom regulierten Unternehmen darauf zu prüfen, ob sie die Benutzeranforderungen erfüllt.	Annex 11, 3.3	Das regulierte Unternehmen ist für die Durchführung solcher Prüfungen verantwortlich.
4.2.5	Den Inspektoren sind Informationen zum Qualitätssystem und zum Audit im Zusammenhang mit Lieferanten oder Entwicklern von Software und implementierten Systemen auf Nachfrage zur Verfügung zu stellen.	Annex 11, 3.4	Inhalt und Umfang der von dieser Anforderung betroffenen Dokumentation sind zwischen dem regulierten Unternehmen und Siemens zu vereinbaren. Diese Anforderung ist in der gemeinsamen Geheimhaltungsvereinbarung entsprechend festzuhalten.

4.3 Datenintegrität

Das Hauptziel beider Regelwerke besteht in der Festlegung von Kriterien, nach denen elektronische Aufzeichnungen und elektronische Unterschriften ebenso zuverlässig und vertrauenswürdig sind wie Aufzeichnungen in Papierform. Dieses Ziel setzt ein hohes Maß an Datenintegrität über den gesamten Datenaufbewahrungszeitraum hinweg voraus und erstreckt sich auch auf das Archivieren und Abrufen relevanter Daten.

	Anforderung	Verweis	Antwort
4.3.1	Das System muss über die Möglichkeit verfügen, ungültige oder geänderte Aufzeichnungen zu erkennen.	21 CFR 11.10 (a)	Ja, die Lösungen für die einzelnen PCS 7 Komponenten sind: **SIMATIC BATCH** Das Batchprotokoll selbst ist nicht mehr änderbar und benötigt deswegen keinen Audit Trail. Unberechtigte Änderungen werden durch den Zugriffsschutz des Systems verhindert.
			SIMATIC PCS 7 OS (Bedienebene) Für jeden Bedieneingriff kann ein Eintrag erzeugt werden (wenn beispielsweise der Bediener Sollwerte / Alarmgrenzwerte / den Überwachungsmodus, etc. verändert oder Alarme quittiert). Aufgezeichnete Daten sind vor unbefugten Änderungen geschützt. Zusätzlich sind entsprechende Zugriffsrechte und Prozeduren zu etablieren.
			SIMATIC PCS 7 ES (Konfigurationsebene) Neben dem lokalen Änderungsprotokoll einer AS können verschiedene Eingriffe auch mittels SIMATIC PCS 7 Audit in die Audit-Datenbank des Process Historian geschrieben werden. Desweiteren gibt es verschiedene Möglichkeiten zur Erkennung von Änderungen an der Konfiguration (siehe Kapitel "Audit Trail, Unterstützung der Änderungskontrolle (Seite 12)").

	Anforderung	Verweis	Antwort
4.3.2	Von Protokollen, die zur Chargenfreigabe herangezogen werden, müssen Ausdrucke generiert werden können, die eine Veränderung der Daten nach der Ersteingabe erkennen lassen.	Annex 11, 8.2	Änderungen von Daten durch den Bediener werden im allgemeinen Audit Trail aufgezeichnet und können mit internen oder externen Mitteln in Form eines Berichts ausgedruckt werden. Mit SIMATIC PCS 7 Audit steht im SIMATIC Information Server ein Template für einen Audit Trail Report zur Verfügung, der insbesondere die als GMP-relevant markierten Eingriffe filtert.
4.3.3	Das System muss über die Möglichkeit verfügen, korrekte und vollständige Kopien der Dokumente sowohl in für Menschen lesbarer als auch in elektronischer Form zu erzeugen.	21 CFR 11.10 (b) Annex 11, 8.1	Ja. Exakte und komplette Kopien können im elektronischen Format oder auf Papier erzeugt werden.
4.3.4	Computergestützte Systeme, die Daten mit anderen Systemen elektronisch austauschen, müssen über geeignete Prüfmechanismen für die korrekte und sichere Eingabe und Verarbeitung der Daten verfügen.	Annex 11, 5	Ja. Je nach Datentyp umfassen diese integrierten Prüffunktionen u. a. Wertbereiche, Datentypprüfungen, Zugriffsberechtigungen, Prüfsummen usw. sowie den Validierungsprozess einschließlich Schnittstellentests.
4.3.5	Werden kritische Daten manuell eingegeben, muss die Richtigkeit dieser Dateneingabe durch eine zusätzliche Prüfung abgesichert werden.	Annex 11, 6	Das System besitzt integrierte Plausibilitätsprüfungen für die Dateneingabe. Außerdem kann als zusätzlicher Prüfmechanismus ein Dialog zur Eingabe mehrerer Unterschriften oder ein Bedienerdialog realisiert werden.
4.3.6	Daten sollten durch physische und elektronische Maßnahmen vor Beschädigung geschützt werden.	Annex 11, 7.1	Zusätzlich zu den Zugriffsschutzmechanismen des Systems hat das regulierte Unternehmen geeignete Schutzmaßnahmen (physische Zugriffskontrolle, Datensicherungsstrategie, eingeschränkte Zugriffsberechtigungen für Benutzer, regelmäßige Tests der Datenlesbarkeit usw.) zu ergreifen. Darüber hinaus muss das regulierte Unternehmen den Datenaufbewahrungszeitraum festlegen und in seinen Prozessen entsprechend berücksichtigen (siehe GAMP 5, Anhänge O3, O4, O8, O9, O11 und O13).
4.3.7	Es müssen regelmäßig Sicherungskopien aller relevanten Daten erstellt werden.	Annex 11, 7.2	Das regulierte Unternehmen hat geeignete Prozesse für die Datensicherung und -wiedereinspielung einzurichten (siehe GAMP 5, Anhang O9).
4.3.8	Elektronische Aufzeichnungen müssen über den gesamten Aufbewahrungszeitraum der Dokumente abrufbar sein.	21 CFR 11.10 (c) Annex 11, 17	Ja. Bei Auslagerung von Archiven muss das regulierte Unternehmen Verfahrenskontrollen für die Archivierung und die Rückspielung der Daten etablieren (siehe GAMP 5, Anhang O13).
4.3.9	Wenn eine Reihenfolge von Systemschritten oder Ereignissen wichtig ist, so sind geeignete funktionale Systemprüfungen umzusetzen.	21 CFR 11.10 (f)	Ja. Beispielsweise kann die Möglichkeit zu einer bestimmten Reihenfolge von Bedieneraktionen vorgesehen werden, indem die Applikation entsprechend konfiguriert wird.

4.4 Audit Trail, Unterstützung der Änderungskontrolle

Im laufenden Betrieb müssen laut den Vorschriften solche Bedienaktionen aufgezeichnet werden, die zur Erzeugung neuer relevanter Daten bzw. zur Änderung oder Löschung vorhandener Daten führen können.

	Anforderung	Verweis	Antwort
4.4.1	Das System muss eine Aufzeichnung aller GMP-relevanten Änderungen und Löschungen (einen systemgenerierten „Audit Trail") erzeugen. Bei Änderung oder Löschung GMP-relevanter Daten sollte der Grund dokumentiert werden.	21 CFR 11.10 (e) Annex 11, 9	Ja. Im laufenden Betrieb vorgenommene Änderungen können vom System mithilfe eines Audit Trails zurückverfolgt werden und enthalten Informationen mit Zeitstempel, Benutzerkennung, den alten und den neuen Wert sowie einen optionalen Kommentar. Der Audit Trail ist innerhalb des Systems sicher und kann nicht durch einen Benutzer geändert werden.
4.4.2	Systeme zur Verwaltung von Daten und Dokumenten müssen in der Lage sein, die Identität des Bedieners, der Daten eingibt, ändert, bestätigt oder löscht, mit Datum und Uhrzeit aufzuzeichnen.	Annex 11, 12.4	Soweit sich dies auf Daten in SIMATIC PCS 7 bezieht, so sind die geforderten Informationen in den entsprechenden Protokollen bzw. Systemlogs enthalten. Die Bedieneingriffe werden mit Benutzerkennung und Zeitstempel aufgezeichnet.
4.4.3	Änderungen an elektronischen Aufzeichnungen dürfen nicht dazu führen, dass zuvor aufgezeichnete Daten unkenntlich werden.	21 CFR 11.10 (e)	Ja. Einmal aufgezeichnete Informationen werden nicht überschrieben und sind jederzeit in der Datenbank verfügbar.
4.4.4	Der Audit Trail muss über einen Zeitraum aufbewahrt werden, der mindestens dem für die entsprechenden elektronischen Dokumente geforderten Zeitraum entspricht.	21 CFR 11.10 (e) Annex 11, 9	Ja. Diese Vorgabe ist technisch umsetzbar und muss in den Verfahrenskontrollen des regulierten Unternehmens zur Datensicherung und Archivierung berücksichtigt werden (siehe GAMP 5, Anhänge O9 und O13).
4.4.5	Der Audit Trail muss den zuständigen Aufsichtsbehörden zu Überprüfungszwecken und zum Kopieren zugänglich gemacht werden.	21 CFR 11.10 (e)	Ja. Der Audit Trail kann verfügbar gemacht und auch in elektronische Formate exportiert werden.

4.5 Systemzugriff, Benutzerkennungen und Passwörter

Da der Systemzugriff auf berechtigte Personen zu beschränken ist und auch die Eindeutigkeit von elektronischen Unterschriften von der Echtheit der Anmeldedaten der Benutzer abhängt, umfasst die Benutzerzugriffsverwaltung eine Reihe von Anforderungen, die für die Akzeptanz von elektronischen Aufzeichnungen und elektronischen Unterschriften unerlässlich sind.

	Anforderung	Verweis	Antwort
4.5.1	Der Zugriff auf das System ist auf berechtigte Personen zu beschränken.	21 CFR 11.10 (d) 21 CFR 11.10 (g) Annex 11, 12.1	Ja. Über die Benutzerkontensteuerung kann der Systemzugriff reguliert werden. Die einzelnen Berechtigungen müssen durch das regulierte Unternehmen spezifiziert werden. Es sind Verfahrenskontrollen durch das regulierte Unternehmen festzulegen wie in GAMP 5, Anhang O11 beschrieben.
4.5.2	Der Umfang der Sicherheitsmaßnahmen ist von der Kritikalität des computergestützten Systems abhängig.	Annex 11, 12.2	Während der Planungs- und Entwicklungsphase von SIMATIC-Produkten spielt die Systemsicherheit eine zentrale Rolle. Da die Systemsicherheit in hohem Maße von der Betriebsumgebung des konkreten IT-Systems abhängt, sind diese Aspekte im Rahmen des Sicherheitsmanagements zu berücksichtigen (siehe GAMP 5, Anhang O11). Empfehlungen und Unterstützung sind über Siemens Industrial Security erhältlich.
4.5.3	Die Erstellung, Änderung und der Entzug von Zugriffsberechtigungen sind aufzuzeichnen.	Annex 11, 12.3	Änderungen innerhalb der Benutzerzugriffsverwaltung werden im Systemlog des Betriebssystems aufgezeichnet und unterliegen dem Änderungskontrollverfahren des regulierten Unternehmens.
4.5.4	Sofern es ein Erfordernis des Systems ist, dass Eingabedaten oder Befehle nur von bestimmten Eingabegeräten (z. B. Terminals) stammen dürfen, prüft das System die Gültigkeit der Quelle aller eingehenden Daten und Befehle? (Hinweis: Dies gilt für Fälle, in denen die Daten oder Befehle von mehreren Geräten stammen können und das System daher die Integrität der Quelle, z. B. ein Netzwerk aus Waagen oder über Funk angebundene entfernte Terminals, verifizieren muss.)	21 CFR 11.10 (h)	Ja. Die SIMATIC PCS 7 OS und die SIMATIC BATCH Arbeitsstationen sind so projektierbar, dass spezielle Eingabedaten / Befehle nur von einer einzelnen dedizierten Arbeitsstation oder einer Gruppe von dedizierten Arbeitsstationen ausgeführt werden können. Alle anderen Arbeitsstationen verfügen höchstens über Lesezugriffsrechte. Das System führt Gültigkeitsprüfungen durch, da die Anbindung der Stationen innerhalb des Systems erfolgen muss.
4.5.5	Es müssen Kontrollen vorhanden sein, die gewährleisten, dass die Eindeutigkeit der einzelnen Kombinationen aus Benutzerkennung und Passwort aufrechterhalten bleibt, sodass jede Kombination nur jeweils einmal vergeben wird.	21 CFR 11.300 (a)	Ja. Es ist sichergestellt, dass jede Benutzerkennung innerhalb des Systems eindeutig ist. Somit ist auch jede Kombination aus Benutzerkennung und Passwort eindeutig.
4.5.6	Es sind Verfahren vorhanden, die gewährleisten, dass die Gültigkeit von Benutzerkennungen regelmäßig überprüft wird.	21 CFR 11.300 (b) Annex 11, 11	Das regulierte Unternehmen muss geeignete Verfahrenskontrollen etablieren.
4.5.7	Passwörter müssen regelmäßig ablaufen und sind regelmäßig zu ändern.	21 CFR 11.300 (b)	Ja. Die Passwortalterung lässt sich in der Benutzerverwaltung konfigurieren.

	Anforderung	Verweis	Antwort
4.5.8	Ein Verfahren zur Aufhebung von Benutzerkennungen und Passwörtern muss für den Fall vorhanden sein, dass eine Person ausscheidet oder innerhalb des Unternehmens wechselt.	21 CFR 11.300 (b) Annex 11, 12.1	Ja. Ein Benutzerkonto kann deaktiviert werden. Alternativ können dem Benutzer die zugeordneten Berechtigungen entzogen werden. Das regulierte Unternehmen muss geeignete Verfahrenskontrollen etablieren.
4.5.9	Es sind Verfahren zum Schadensmanagement bei Verlusten zu befolgen, mit denen die Berechtigungen von verlorenen, gestohlenen, fehlenden oder anderweitig in ihrer Sicherheit beeinträchtigten Tokens, Karten oder anderen Geräten, die Benutzerkennungen oder Passwörter enthalten oder erzeugen, aufgehoben werden, sowie Verfahren, mit denen unter Einsatz geeigneter, strenger Kontrollen temporärer oder dauerhafter Ersatz ausgegeben wird.	21 CFR 11.300 (c)	Das regulierte Unternehmen muss geeignete Verfahrenskontrollen etablieren.
4.5.10	Maßnahmen zur Erkennung von Versuchen einer unbefugten Nutzung sowie zur Benachrichtigung der Sicherheitseinheit und der Unternehmensführung müssen eingerichtet sein.	21 CFR 11.300 (d) Annex 11, 12.1	Ja. Fehlerhafte Versuche einer Nutzung des Systems oder der Tätigung von elektronischen Unterschriften werden erkannt und können protokolliert werden. Das regulierte Unternehmen muss geeignete Verfahrenskontrollen etablieren, um eine regelmäßige Prüfung der Sicherheits- und Zugriffskontrollprotokolle zu gewährleisten (siehe GAMP 5, Anhang O8).
4.5.11	Anfängliches und im Anschluss daran regelmäßiges Testen der Geräte (z. B. Tokens, Karten), die Benutzerkennungs- oder Passwortinformationen enthalten oder erzeugen, um zu gewährleisten, dass sie ordnungsgemäß funktionieren und nicht unbefugt verändert wurden.	21 CFR 11.300 (e)	Das regulierte Unternehmen muss geeignete Verfahrenskontrollen etablieren.

4.6 Elektronische Unterschrift

Um zu erreichen, dass elektronische Unterschriften den handschriftlichen Unterschriften in allen Belangen als gleichwertig anerkannt werden, erstrecken sich die Anforderungen an sie nicht allein auf den Akt der elektronischen Unterzeichnung von Aufzeichnungen. Sie beinhalten darüber hinaus auch Vorschriften zur Aufbewahrung von Aufzeichnungen und zur Erscheinungsform der elektronischen Unterschrift.

	Anforderung	Verweis	Antwort
4.6.1	Es müssen schriftliche Verfahrensanweisungen geschaffen werden, nach denen Personen für unter ihrer elektronischen Unterschrift vorgenommene Handlungen verantwortlich gemacht werden, sodass Abschreckungsmechanismen gegen das Fälschen von Dokumenten und Unterschriften vorhanden sind.	21 CFR 11.10 (j) Annex 11, 14.a	Das regulierte Unternehmen muss geeignete Verfahrenskontrollen schaffen.
4.6.2	Unterschriebene elektronische Dokumente müssen die folgenden zugehörigen Informationen enthalten: • Name des Unterzeichnenden in Druckbuchstaben • Datum und Zeitpunkt der Unterschrift • Bedeutung der Unterschrift (wie z. B. Freigabe, Überprüfung, Verantwortlichkeit)	21 CFR 11.50 (a) Annex 11, 14.c	Ja. Die genannten Informationen sind verfügbar.
4.6.3	Die oben genannten Informationen erscheinen auf den angezeigten und gedruckten Kopien der elektronischen Aufzeichnung.	21 CFR 11.50 (b)	Ja. Die genannten Informationen sind verfügbar.
4.6.4	Elektronische Unterschriften müssen mit den entsprechenden elektronischen Aufzeichnungen so verknüpft sein, dass die Unterschriften nicht entfernt, kopiert oder anderweitig zum Zweck der Fälschung der elektronischen Aufzeichnung mit üblichen Mitteln übertragen werden können.	21 CFR 11.70 Annex 11, 14.b	Ja. Die elektronischen Unterschriften können nicht entfernt oder anderweitig verwendet werden.
4.6.5	Jede elektronische Unterschrift muss in Bezug auf eine Person eindeutig sein und darf von keiner anderen Person wiederverwendet oder keiner anderen Person neu zugeordnet werden.	21 CFR 11.100 (a) 21 CFR 11.200 (a) (2)	Ja. Die elektronische Unterschrift nutzt die eindeutigen Kennungen für Benutzerkonten in der Benutzerkontensteuerung von Microsoft Windows. Die Wiederverwendung oder Neuzuordnung von elektronischen Unterschriften wird effektiv unterbunden.
4.6.6	Wird ein System zur Aufzeichnung der Zertifizierung und Chargenfreigabe eingesetzt, muss durch das System sichergestellt werden, dass nur sachkundige Personen die Chargenfreigabe zertifizieren können.	Annex 11, 15	Elektronische Unterschriften sind jeweils mit einer einzelnen Person verknüpft. Das System ermöglicht strikte Festlegungen, welche Rolle bzw. welche Person eine Unterschrift leisten darf.
4.6.7	Die Identität einer Person ist zu prüfen, bevor dieser Person Komponenten einer elektronischen Unterschrift zugewiesen werden.	21 CFR 11.100 (b)	Das regulierte Unternehmen muss geeignete Verfahrenskontrollen zur Prüfung der Identität einer Person einrichten, bevor ein Benutzerkonto und/oder elektronische Unterschriften zugewiesen werden.

	Anforderung	Verweis	Antwort
4.6.8	Unterschreibt eine Person mehrfach, allerdings nicht innerhalb einer ununterbrochenen Sitzung, so ist jede Unterschrift unter Verwendung aller Komponenten der elektronischen Unterschrift zu leisten.	21 CFR 11.200 (a) (1) (ii)	Ja. Um eine elektronische Unterschrift zu leisten, sind Benutzerkennung und Benutzerpasswort erforderlich.
4.6.9	Unterschreibt eine Person während einer ununterbrochenen Sitzung mehrfach, so ist die erste Unterschrift unter Verwendung aller Komponenten der elektronischen Unterschrift zu leisten. Nachfolgende Unterschriften sind unter Verwendung mindestens einer persönlichen Komponente der elektronischen Unterschrift zu leisten.	21 CFR 11.200 (a) (1) (i)	Ja. Jede Unterschrift besteht aus zwei Komponenten (Benutzerkennung und Passwort).
4.6.10	Der Versuch einer Person, eine ihr nicht eigene elektronische Unterschrift zu verwenden, würde die Zusammenarbeit von mindestens zwei Personen erfordern.	21 CFR 11.200 (a) (3)	Ja. Es ist nicht möglich, eine elektronische Unterschrift bei der Unterzeichnung oder nach Aufzeichnung der Unterschrift zu fälschen. Zusätzlich benötigt das regulierte Unternehmen Verfahrensanweisungen, die eine Offenlegung von Passwörtern verbieten.
4.6.11	Elektronische Unterschriften auf der Grundlage biometrischer Daten müssen so konzipiert sein, dass sie ausschließlich durch ihren authentischen Eigentümer verwendet werden können.	21 CFR 11.200 (b)	Standardtools von Fremdherstellern können für die Erzeugung von biometrischen elektronischen Unterschriften verwendet werden. Die Integrität einer solchen Lösung ist individuell zu bewerten.

4.7 Offene Systeme

Der Betrieb eines offenen Systems kann zusätzliche Kontrollen zur Gewährleistung der Datenintegrität und einer eventuellen Vertraulichkeit elektronischer Aufzeichnungen erfordern.

	Anforderung	Verweis	Antwort
4.7.1	Zur Sicherstellung der Echtheit, Integrität und ggf. Vertraulichkeit elektronischer Aufzeichnungen werden zusätzliche Maßnahmen wie z. B. Datenverschlüsselung ergriffen.	21 CFR 11.30	Bei offenen Systemen sind zusätzliche Sicherheitsmaßnahmen zu ergreifen. Unterstützung hierbei wird beispielsweise anhand der Konfigurationsinformationen im Handbuch "Sicherheitskonzept PCS 7 und WinCC" sowie durch marktübliche Standardtools z. B. zur Verschlüsselung geleistet. Die SSL-Verschlüsselung für die Datenkommunikation des Terminalbusses ist eine dieser möglichen Maßnahmen.
4.7.2	Zur Sicherstellung der Echtheit und Integrität von elektronischen Unterschriften werden zusätzliche Maßnahmen, z. B. die Nutzung von Standards für digitale Unterschriften, ergriffen.	21 CFR 11.30	SIMATIC PCS 7 besitzt keine Funktionalität für digitale (verschlüsselte) Unterschriften.

Weitere Informationen

Siemens AG
Digital Industries
Pharmaceutical and Life Science Industry
Siemensallee 84
76187 Karlsruhe, Deutschland

PDF (A5E54273651-AA)
Produced in Germany