SIEMENS

Ausgabe 05/2021

KONFORMITÄTSERKLÄRUNG ERES

SIMATIC

SIMATIC SIPAT V5.1

Elektronische Aufzeichnungen / Elektronische Unterschriften

siemens.com/pharma

SIEMENS

SIMATIC

SIMATIC SIPAT V5.1 Konformitätserklärung ERES

Produktinformation

Elektronische Aufzeichnungen / Elektronische Unterschriften (ERES)

05/2021
A5E50732433-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.

Bestimmungsgemäßer Gebrauch 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 AG. 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 AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
DEUTSCHLAND

A5E50732433-AA
Ⓟ 05/2021 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 SIPAT das System im Hinblick auf diese Anforderungen bewertet und die Ergebnisse in der vorliegenden Konformitätserklärung veröffentlicht. Die vorliegende Konformitätserklärung betrifft die Standardausführung des SIMATIC SIPAT-Systems. Für abweichende Architekturen können andere Konformitätsstufen gelten.

SIMATIC SIPAT V5.1 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 SIPAT (Seite 17)" des vorliegenden Dokuments genannt.

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. In Kapitel "Erfüllung der Anforderungen durch SIMATIC SIPAT (Seite 9)" wird die Funktionalität von SIMATIC SIPAT vorgestellt, mittels derer diese Anforderungen erfüllt werden.
3. Das Kapitel "Bewertungsliste für SIMATIC SIPAT (Seite 17)" enthält eine ausführliche Systembewertung anhand der einzelnen Anforderungen der entsprechenden Vorschriften.

Die Anforderungen im Überblick

2

Annex 11 und Part 11 tragen der Tatsache Rechnung, dass die Gefahr von Manipulationen, Fehlinterpretationen und nicht nachvollziehbaren Änderungen bei elektronischen Aufzeichnungen und elektronischen Unterschriften größer ist als bei herkömmlichen Papieraufzeichnungen und handschriftlichen Unterschriften. Demnach unterscheiden sich die Mittel, die dazu eingesetzt werden, den Zugriff auf elektronische Aufzeichnungen auf berechtigte Personen zu beschränken, erheblich von denen, die für die Beschränkung des Zugriffs auf Papieraufzeichnungen erforderlich sind. Aus diesen Gründen sind zusätzliche Maßnahmen notwendig.

Die Begriffe „elektronische Aufzeichnung" / „elektronisches Dokument" beziehen sich auf jede beliebige Kombination aus Text, Grafik, Daten, auditiven, bildlichen oder sonstigen Informationen in digitaler Form, die mit einem Computersystem erstellt, geändert, gepflegt, archiviert, abgerufen oder verteilt werden.

Unter dem Begriff „elektronische Unterschrift" ist ein computertechnisch zusammengestelltes Symbol oder eine Reihe von Symbolen zu verstehen, das bzw. die von einer Person angefertigt, übernommen oder genehmigt wurde, um ein rechtlich bindendes Äquivalent einer handschriftlichen Unterschrift zu sein. 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 SIPAT 3

Die Empfehlungen von Siemens hinsichtlich Systemarchitektur, Konzeption und Konfiguration unterstützen Systembenutzer bei der Erreichung der Konformität. Zusätzliche Informationen und Hinweise siehe Benutzerhandbuch SIMATIC SIPAT 5.1.

Die im Kapitel "Die Anforderungen im Überblick (Seite 7)" dargelegten Anforderungen können durch Einsatz folgender Kontrollarten in einem computergestützten System erfüllt werden:

- Technologische Kontrollen
  Technologische Kontrollen sind technische oder funktionelle Features der verwendeten Software. Zu den erforderlichen Kontrollen zählen sowohl Funktionen der SIMATIC SIPAT-Standardsoftware als auch Funktionen, die in die zusätzlich zur SIMATIC SIPAT-Standardsoftware entwickelten spezifischen Software integriert sind.
  Die technologischen Standardkontrollen von SIMATIC SIPAT zur Erfüllung rechtlicher Anforderungen werden in diesem Dokument behandelt. Diese Kontrollen können zur Erfüllung weiterer rechtlicher wie nutzerspezifischer Anforderungen konfiguriert werden.
  - Die Implementierung dieser technologischen Kontrollen für Standardfunktionen liegt in der Verantwortung des Lieferanten.
  - Systemintegrator und Kunde tragen gemeinsam dafür Verantwortung, dass bei der Konfigurierung technologischer Standardkontrollen die zutreffenden Konformitätsbestimmungen eingehalten werden.
  - Systemintegrator und Kunde tragen gemeinsam dafür Verantwortung, dass die bezüglich der kundenspezifischen Software geltenden Konformitätsbestimmungen eingehalten werden.
- Verfahrenskontrollen
  Verfahrenskontrollen sind Arbeitsanweisungen (SOP) zur Kontrolle der Nutzung der Applikationssoftware oder der Umgebung, in der sie verwendet wird.
  Der Kunde trägt Verantwortung für die Implementierung der Verfahrenskontrollen zur Einhaltung geltender Konformitätsbestimmungen.
- Administrative Kontrollen
  Administrative Kontrollen sind Verfahren der Systemadministration, etwa zur Regelung des Systemzugriffs, der Benutzerkontensteuerung oder der Passwortverwaltung.
  Der Kunde trägt Verantwortung für die Implementierung der administrativen Kontrollen zur Einhaltung geltender Konformitätsbestimmungen.

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

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 waren jedoch bereits seit Langem Bestandteil anderer Regelwerke als *Part 11* und *Annex 11*. Der Industrieverband ISPE (International Society of Pharmaceutical Engineers, http://www.ispe.org) nahm dies zum Anlass für die Veröffentlichung der Baseline Guides (Baseline® Pharmaceutical Engineering Guides for New and Renovated Facilities, Volume 1-7, ISPE), des GAMP 5-Leitfadens (GAMP 5 – Ein risikobasierter Ansatz für konforme GxP-computergestützte Systeme, ISPE 2008) sowie der GAMP Good Practice Guides.

Folglich sollten der System-Lebenszyklus und der Validierungsansatz unter Berücksichtigung der Richtlinien des GAMP 5-Leitfadens definiert werden. Der Leitfaden umfasst u. a. zahlreiche Anhänge zu den Themen Lifecycle Management, Systementwicklung und Betrieb von computergestützten Systemen.
Da die meisten pharmazeutischen Unternehmen im Rahmen ihrer vorhandenen Prozesse bereits über ein Verfahren zur Validierung von computergestützten Systemen verfügen, ist es von Vorteil, den Lebenszyklus und die Validierung des Systems diesen Prozessen gemäß einzurichten.

3.2 Lieferanten und Dienstleister

Lieferanten von Systemen und Lösungen sowie Dienstleister sind angemessen zu bewerten, 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

Die Datenintegrität wird innerhalb des Systems durch Maßnahmen wie Zugriffsschutz, Audit Trail, Datentypprüfungen, Prüfsummen, Datensicherung/-wiederherstellung und Datenarchivierung/-abruf sichergestellt, ergänzt durch Systemvalidierung, geeignete Arbeitsprozeduren und Personalschulungen.

Archivierung

SIMATIC SIPAT bietet die Möglichkeit, in der zentralen Betriebsdatenbank vorhandene Messdaten in einer Archivdatenbank (Kurzzeitspeicherung) und danach in einem Langzeitarchivmedium wie einem Dateiserver zu archivieren (Standardfunktionalität von SIMATIC SIPAT).

Kurzzeitarchivierung

Die Datensynchronisation zwischen Bedien- und Archivdatenbank erfolgt kontinuierlich und automatisch. In der Archivdatenbank gespeicherte Aufzeichnungen sind über das Modul SIMATIC SIPAT Data Miner und Berichte in SIMATIC SIPAT zugänglich (Berichterstellung wird mit dem System als Option angeboten).

Ist die Kurzzeitarchivierung implementiert, wird SIMATIC SIPAT in der Betriebsart "Replicated" betrieben. Ist die Kurzzeitarchivierung nicht implementiert, wird SIMATIC SIPAT in der Betriebsart "Stand-alone" betrieben.

Langzeitarchivierung

Langzeitarchivierung basiert auf der Verwendung von XML-Dateien. Die Datenintegrität dieser XML-Dateien wird durch eine Prüfsumme sichergestellt. Bei der Überführung von Daten in den Langzeitspeicher werden die Daten zunächst kopiert, anhand der Daten in der Datenbank verifiziert und erst nach erfolgreicher Verifizierung aus der Datenbank gelöscht. Die entsprechenden Abläufe werden erfasst und können in Gänze nachverfolgt werden.

Die Langzeitarchivierung kann auf einem System in der Betriebsart "Stand-alone" (Archivieren von Daten über die zentrale Betriebsdatenbank) oder in der Betriebsart "Replicated" (Archivieren von Daten über die Archivdatenbank) stattfinden. Werden Daten aus der Archivdatenbank verschoben, die noch auf der Betriebsdatenbank gespeichert sind, werden diese zur Vermeidung von Inkonsistenzen zunächst von der Betriebsdatenbank gelöscht.

Die Langzeitarchivierung kann automatisch ablaufen: SIMATIC SIPAT erstellt automatisch Aufgaben, über die die Archivierungsmethoden festgelegt werden.

Archivierungsaufgaben können auch manuell erstellt werden: Der Benutzer legt fest, welche Messdaten archiviert werden sollen, indem er die entsprechenden Methoden in SIMATIC SIPAT auswählt.

Das regulierte Unternehmen ist dafür verantwortlich, die Daten im Langzeitarchiv zu verwalten und die Aufbewahrungsfrist für Daten einzuhalten.

Weitere Informationen über das Verwalten von Archivdaten in SIMATIC SIPAT finden Sie im Benutzerhandbuch zu SIMATIC SIPAT 5.1.

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 (z. B. Zugriffsschutz) zur Verfügung.

Die folgenden Abschnitte beschreiben die Umsetzung von Anforderungen an Audit Trails während des Laufzeitbetriebs und enthalten Hinweise zur Nachverfolgung von Änderungen, die im Konfigurationsmodul von SIMATIC SIPAT vorgenommen werden.

Die Funktionalität "Audit Trail" in SIMATIC SIPAT steht für alle Aufzeichnungen im Laufzeitbetrieb zur Verfügung. Audit Trail-Aufzeichnungen:

- sind sicher, computergeneriert und mit einem Zeitstempel (Datum und Uhrzeit) versehen;
- enthalten die Benutzer-ID und den Benutzernamen der für die Änderung verantwortlichen Person;
- sind für Überprüfungen verfügbar.

Originalaufzeichnungsdaten bleiben auch bei Änderungen oder Löschungen innerhalb einer Aufzeichnung erhalten. Alle Aufzeichnungen sind zudem vor unbefugten Änderungen, Zusätzen oder Löschungen geschützt.

Der Kunde ist dafür verantwortlich, die Uhrzeitsynchronisation zwischen allen verwendeten IT-Geräten sicherzustellen.

Die Unterstützung der Änderungskontrolle ist für alle Konfigurationsaufzeichnungen gegeben. Alle Änderungen an einem Konfigurationsobjekt werden in der Historie dieses Objekts aufgezeichnet. Diese Änderungsaufzeichnungen haben die gleichen Eigenschaften wie der Audit Trail von Laufzeitaufzeichnungen.

Audit Trail

Bei Aktivierung eines Konfigurationsobjekts im Laufzeitmodul wird ein Bedienobjekt erstellt. Ein Bedienobjekt wird auf Grundlage der Informationen einer spezifischen Version des jeweils zugehörigen Konfigurationsobjekts erstellt. Neben den verschiedenen Aktionen, die auf ein Bedienobjekt angewendet werden (wie Start, Stopp usw.), lassen sich nur einzelne Eigenschaften (wie Kontextdaten, Handbuch, Infodaten usw.) an Bedienobjekten ändern. Diese Aktionen und Änderungen werden im Audit Trail protokolliert.

Folgende Informationen werden in der Datenbank gespeichert:

- ID des zugehörigen Konfigurationsobjekts
- Version des entsprechenden Konfigurationsobjekts
- Ortszeit (Datum und Uhrzeit)
- UTC-Zeit (Datum und Uhrzeit)
- Benutzer-ID (Microsoft Windows-Konto)
- Benutzername (Microsoft Windows-Benutzername)
- Kurzbeschreibung der Aktion (z. B. Grund)
- Einzelheiten der Aktion der geänderten Eigenschaft, einschließlich des alten und neuen Werts

Mit einer validierten Methode (GMP) gemessene Daten können bei allen Einstellungen eindeutig mit der Konfiguration verknüpft werden.

Nicht mit GMP-Methoden gemessene Daten können bei den meisten Einstellungen eindeutig mit der Konfiguration verknüpft werden.

Der Audit Trail kann mit den Standardberichten der Software SIMATIC SIPAT exportiert werden.

Audit Trail zu Kurzzeitarchivierungsaktionen

Archivierte Betriebsdaten (siehe Kapitel "Datenintegrität (Seite 10)") können aus der Betriebsdatenbank gelöscht werden, wenn die Archivierung nachgewiesen ist. Folgender Audit Trail des Löschungsvorgangs wird in der Datenbank gespeichert:

- Identifikation der gelöschten Daten. Für Laufzeitmethoden sind dies die Methodenlaufzeit-ID (ME), die Methodeninstanz-ID (MI) und ihr Kontext
- Benutzername und Benutzer-ID der Person, die die Löschung veranlasst hat
- Zeitstempel der Löschung
- Einzelheiten der Löschung

Audit Trail zu Langzeitarchivierungsaktionen

Archivierte Daten können auf ein Langzeitarchivierungsmedium wie einen Dateiserver verschoben oder kopiert werden. Für diese Aktion wird ein vollständiger Audit Trail angelegt. Er enthält folgende Informationen:

- Identifikation der kopierten oder verschobenen Daten, d. h. die Methodenlaufzeit-ID (ME), die Methodeninstanz-ID (MI) und den dazugehörigen Kontext
- Den Speicherort der Original-(XML-)Datei einschließlich des Dateinamens
- Benutzernamen und Benutzer-ID der Person, die die Archivierung veranlasst hat
- Zeitstempel des Archivierungszeitpunkts
- Einzelheiten der Archivierung

Unterstützung der Änderungskontrolle

Die Unterstützung der Änderungskontrolle ist gegeben für:

- Konfigurationsobjekte
  - Stationsdefinitionen
  - Methodendefinitionen
  - Kollektordefinitionen
  - Berechnungsdefinitionen
  - Infodatenblattdefinitionen
  - Arbeitsstationsdefinitionen
- Data-Mining-Objekte
  - Datenblätter

Die Unterstützung der Änderungskontrolle ist durch zwei Funktionen gegeben: Historie und Versionskontrolle eines Objekts.

Objekthistorie

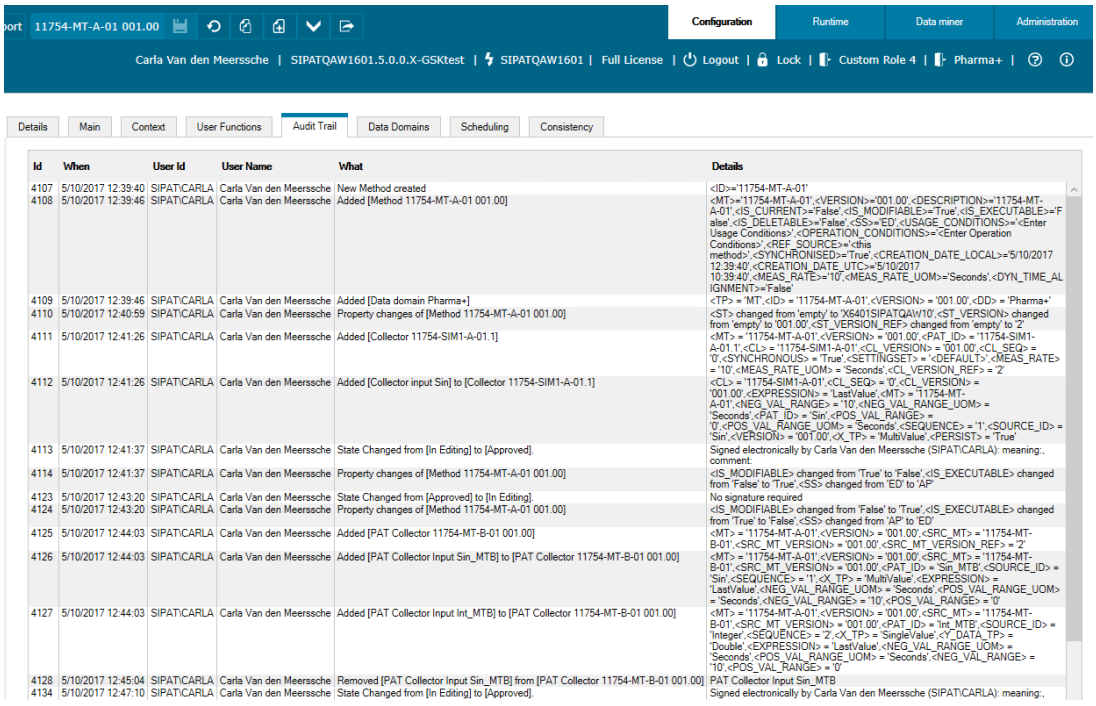
Die Historie eines Konfigurationsobjekts wird im Register "Audit Trail" des Objekts in vier Spalten angezeigt: Was, Wann, Wer und Details:

Was	erläutert die Art der am entsprechenden Objekt vorgenommenen Änderung: z. B. Eigenschafts- oder Zustandsänderungen (Kurzbeschreibung)
Wann	zeigt Datum und Uhrzeit der Änderung an.
Wer	zeigt Namen und Benutzer-ID der für die Änderung verantwortlichen Person an
Details	gibt für Eigenschafts- und Zustandsänderungen jeweils ursprünglichen und neuen Wert an (ausführliche Beschreibung)

Alle mit einer elektronischen Signatur geleisteten Unterschriften, ob erfolgreich oder nicht erfolgreich, werden in der Historie aufgezeichnet.

Der Zeitstempel der Änderung wird mit Datum und Uhrzeit sowohl bezogen auf die Ortszeit als auch auf die UTC gespeichert. Die Informationen über die Änderung sind schreibgeschützt, Benutzer können sie nicht aktualisieren oder löschen.

Benutzer haben die Möglichkeit, gegebenenfalls Kommentare hinzuzufügen, auch das wird in der Historie protokolliert.



Id	When	User Id	User Name	What	Details
4107	5/10/2017 12:39:40	SIPAT\CARLA	Carla Van den Meerssche	New Method created	<ID>='11754-MT-A-01'
4108	5/10/2017 12:39:46	SIPAT\CARLA	Carla Van den Meerssche	Added [Method 11754-MT-A-01 001.00]	<MT>='11754-MT-A-01',<VERSION>='001.00',<DESCRIPTION>='11754-MT-A-01',<IS_CURRENT>='False',<IS_MODIFIABLE>='True',<IS_EXECUTABLE>='False',<IS_DELETABLE>='False',<SS>='ED',<USAGE_CONDITIONS>='<Enter Usage Conditions>',<OPERATION_CONDITIONS>='<Enter Operation Conditions>',<REF_SOURCE>='<this method>',<SYNCHRONISED>='True',<CREATION_DATE_LOCAL>='5/10/2017 12:39:40',<CREATION_DATE_UTC>='5/10/2017 10:39:40',<MEAS_RATE>='10',<MEAS_RATE_UOM>='Seconds',<DYN_TIME_ALIGNMENT>='False'
4109	5/10/2017 12:39:46	SIPAT\CARLA	Carla Van den Meerssche	Added [Data domain Pharma+]	<TP> = 'MT',<ID> = '11754-MT-A-01',<VERSION> = '001.00',<DD> = 'Pharma+'
4110	5/10/2017 12:40:59	SIPAT\CARLA	Carla Van den Meerssche	Property changes of [Method 11754-MT-A-01 001.00]	<ST> changed from 'empty' to 'X6401SIPATQAW10',<ST_VERSION> changed from 'empty' to '001.00',<ST_VERSION_REF> changed from 'empty' to '2'
4111	5/10/2017 12:41:26	SIPAT\CARLA	Carla Van den Meerssche	Added [Collector 11754-SIM1-A-01.1]	<MT> = '11754-MT-A-01',<VERSION> = '001.00',<PAT_ID> = '11754-SIM1-A-01.1',<CL> = '11754-SIM1-A-01',<CL_VERSION> = '001.00',<CL_SEQ> = '0',<SYNCHRONOUS> = 'True',<SETTINGSET> = '<DEFAULT>',<MEAS_RATE> = '10',<MEAS_RATE_UOM> = 'Seconds',<CL_VERSION_REF> = '2'
4112	5/10/2017 12:41:26	SIPAT\CARLA	Carla Van den Meerssche	Added [Collector input Sin] to [Collector 11754-SIM1-A-01.1]	<CL> = '11754-SIM1-A-01',<CL_SEQ> = '0',<CL_VERSION> = '001.00',<EXPRESSION> = 'LastValue',<MT> = '11754-MT-A-01',<NEG_VAL_RANGE> = '10',<NEG_VAL_RANGE_UOM> = 'Seconds',<PAT_ID> = 'Sin',<POS_VAL_RANGE> = '0',<POS_VAL_RANGE_UOM> = 'Seconds',<SEQUENCE> = '1',<SOURCE_ID> = 'Sin',<VERSION> = '001.00',<X_TP> = 'MultiValue',<PERSIST> = 'True'
4113	5/10/2017 12:41:37	SIPAT\CARLA	Carla Van den Meerssche	State Changed from [In Editing] to [Approved].	Signed electronically by Carla Van den Meerssche (SIPAT\CARLA): meaning:, comment:
4114	5/10/2017 12:41:37	SIPAT\CARLA	Carla Van den Meerssche	Property changes of [Method 11754-MT-A-01 001.00]	<IS_MODIFIABLE> changed from 'True' to 'False',<IS_EXECUTABLE> changed from 'False' to 'True',<SS> changed from 'ED' to 'AP'
4123	5/10/2017 12:43:20	SIPAT\CARLA	Carla Van den Meerssche	State Changed from [Approved] to [In Editing].	No signature required
4124	5/10/2017 12:43:20	SIPAT\CARLA	Carla Van den Meerssche	Property changes of [Method 11754-MT-A-01 001.00]	<IS_MODIFIABLE> changed from 'False' to 'True',<IS_EXECUTABLE> changed from 'True' to 'False',<SS> changed from 'AP' to 'ED'
4125	5/10/2017 12:44:03	SIPAT\CARLA	Carla Van den Meerssche	Added [PAT Collector 11754-MT-B-01 001.00]	<MT> = '11754-MT-A-01',<VERSION> = '001.00',<SRC_MT> = '11754-MT-B-01',<SRC_MT_VERSION> = '001.00',<SRC_MT_VERSION_REF> = '2'
4126	5/10/2017 12:44:03	SIPAT\CARLA	Carla Van den Meerssche	Added [PAT Collector Input Sin_MTB] to [PAT Collector 11754-MT-B-01 001.00]	<MT> = '11754-MT-A-01',<VERSION> = '001.00',<SRC_MT> = '11754-MT-B-01',<SRC_MT_VERSION> = '001.00',<PAT_ID> = 'Sin_MTB',<SOURCE_ID> = 'Sin',<SEQUENCE> = '1',<X_TP> = 'MultiValue',<EXPRESSION> = 'LastValue',<NEG_VAL_RANGE_UOM> = 'Seconds',<POS_VAL_RANGE_UOM> = 'Seconds',<NEG_VAL_RANGE> = '10',<POS_VAL_RANGE> = '0'
4127	5/10/2017 12:44:03	SIPAT\CARLA	Carla Van den Meerssche	Added [PAT Collector Input Int_MTB] to [PAT Collector 11754-MT-B-01 001.00]	<MT> = '11754-MT-A-01',<VERSION> = '001.00',<SRC_MT> = '11754-MT-B-01',<SRC_MT_VERSION> = '001.00',<PAT_ID> = 'Int_MTB',<SOURCE_ID> = 'Integer',<SEQUENCE> = '2',<X_TP> = 'SingleValue',<Y_DATA_TP> = 'Double',<EXPRESSION> = 'LastValue',<NEG_VAL_RANGE_UOM> = 'Seconds',<POS_VAL_RANGE_UOM> = 'Seconds',<NEG_VAL_RANGE> = '10',<POS_VAL_RANGE> = '0'
4128	5/10/2017 12:45:04	SIPAT\CARLA	Carla Van den Meerssche	Removed [PAT Collector Input Sin_MTB] from [PAT Collector 11754-MT-B-01 001.00]	PAT Collector Input Sin_MTB
4134	5/10/2017 12:47:10	SIPAT\CARLA	Carla Van den Meerssche	State Changed from [In Editing] to [Approved].	Signed electronically by Carla Van den Meerssche (SIPAT\CARLA): meaning:,

Bild 3-1 Objekthistorie im Register "Audit Trail"

Versionskontrolle

Konfigurationsobjekte können der Änderungskontrolle unterliegen.

Änderungen an einem Konfigurationsobjekt

- müssen in der Objekthistorie protokolliert werden;
- dürfen früher aufgezeichnete Informationen nicht verfälschen oder unlesbar machen.

Ersteres erfolgt wie oben beschrieben. Letzteres wird in SIMATIC SIPAT mittels Versionskontrolle umgesetzt.

Möchte ein Nutzer die Eigenschaften eines Konfigurationsobjekts ändern, welches sich im Status "Freigegeben" befindet, muss er hierzu eine neue Version erstellen. Ältere Versionen, die sich im Status "Freigegeben" befinden, können weder geändert noch gelöscht werden. Im Audit Trail des neu erstellten Objekts wird die Version, die der neuen Version als Grundlage dient, vermerkt.

Die genauen Lebenszykluseigenschaften des Konfigurationsobjekts können für jedes Projekt einzeln angepasst werden. Werden entsprechende Änderungen vorgenommen, sollten deren Auswirkungen auf die im vorliegenden Dokument vorgestellten Antworten ausgewertet werden. Das regulierte Unternehmen trägt hierfür die Verantwortung.

Das Löschen elektronischer Aufzeichnungen auf Konfigurationsebene ist nicht möglich, jedoch können validierte Aufzeichnungen wieder aufgerufen oder obsolet gemacht werden.

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 Zuständigkeit und Zugriffsberechtigung der Systembenutzer", vollständig erfüllt.

Für dieses System bestehen umfangreiche Sicherheits- und Zugriffskontrollen. Sicherheitsmechanismen beschränken den Zugriff auf die verschiedene Teilen der Applikation (Konfigurationszugriff, Bedienzugriff, Administrationszugriff und Zugriff auf Laufzeitdaten sowie jede Teilmenge der genannten Zugriffe auf SIPAT-Module).

Der Zugriff auf das System und auf Funktionen innerhalb des Systems ist abhängig von der Benutzer-ID für Microsoft Windows (Authentifizierung), die bei der Anmeldung verwendet wird, der/den Rolle(n) des Benutzers in SIMATIC SIPAT und den funktionellen, d. h. funktionsbezogenen Zugriffsrechten des Benutzers.

SIMATIC SIPAT wird mit einem Standardset funktioneller Zugriffsrechte für Standardrollen für SIMATIC SIPAT geliefert. Welche funktionellen Zugriffsrechte welchen SIMATIC SIPAT-Rollen zugewiesen werden, kann für jedes Projekt individuell festgelegt werden und liegt in der Verantwortung des regulierten Unternehmens.

Zur Anmeldung bei SIMATIC SIPAT benötigen Nutzer zwei Angaben: ihre Benutzer-ID und ihr Passwort.

Die beiden hierfür bestimmten Felder werden dem Nutzer im Anmeldungsbildschirm leer angezeigt. Benutzer-ID und Passwort werden nie in der Registrierungsdatenbank oder an einem anderen Ort gespeichert.

Alle Versuche, sich bei der Applikation anzumelden, ob gültig oder ungültig, werden registriert. Standardmäßig wird das Benutzerkonto nach dem dritten fehlgeschlagenen Anmeldeversuch gesperrt. Diese Strategie zur Verifizierung der Benutzer und zum Ausschluss unbefugter Benutzer gilt ergänzend zu jeder Richtlinie, die für Windows auf Domainebene festgelegt wird.

Das regulierte Unternehmen ist dafür verantwortlich, den ordnungsgemäßen Systemzugriff zu gewährleisten und die unbefugte Nutzung des Systems SIMATIC SIPAT oder dessen Datenbanken zu verhindern, wobei besonderes Augenmerk zu richten ist auf:

- Der Zugriff für Datenbankinhaber und Datenbankadministrator muss über entsprechende Verfahrensvorschriften geregelt werden.
- Benutzern mit kontrolliertem Zugriff sollte der Zugriff auf SIMATIC SIPAT nur über bestehende Schemata in der SIPAT-Datenbank (z. B. SIPAT_READ, SIPAT_WRITE, SIPAT_DATAMINER) gewährt werden, wie im Installationshandbuch beschrieben.
- Alle anderen Zugriffsberechtigungen für die zentrale Datenbank müssen verifiziert werden.

3.6 Elektronische Unterschrift

SIMATIC SIPAT bietet Funktionen zur Konfiguration einer elektronischen Unterschrift. Für welche Variablen bei der Vornahme von Änderungen eine elektronische Unterschrift benötigt wird, wird in der Phase der Systemkonfiguration spezifiziert.

Geleistet wird die elektronische Unterschrift in einem separaten Dialog, in dem der Benutzer elektronisch unterschreiben muss, indem er die beabsichtigte Aktion durch Eingeben seiner Benutzer-ID und seines Passworts bestätigt.
Je nach Konfiguration der elektronischen Unterschrift muss eine Bedeutung ausgewählt und/oder ein Kommentar hinzugefügt werden.
Der Kommentar kann für jeden Vorgang als optional oder obligatorisch konfiguriert werden. Bei Verwendung der Standardinstallation sind Kommentare optional und die Auswahl einer Bedeutung für eine elektronische Unterschrift ist nicht aktiviert.

Anschließend wird die elektronische Unterschrift im Audit Trail zusammen mit Benutzer-ID, Benutzername, Zeitstempel, Bedeutung, Kommentar und ausgeführter Aktion gespeichert.

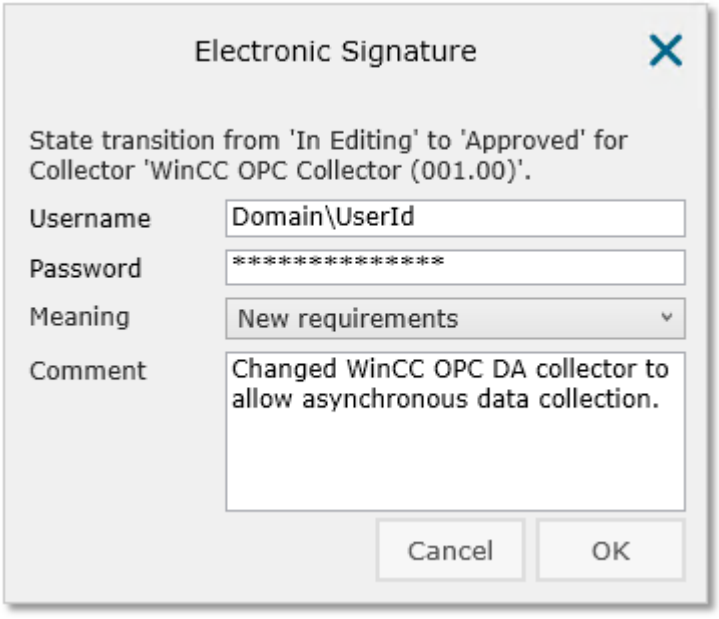


Bild 3-2 Elektronische Unterschrift

Bewertungsliste für SIMATIC SIPAT

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 einer kundenspezifischen Applikation 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 der Kontrolle durch das Siemens QMS und den 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 das Änderungsmanagement und das Abweichungsmanagement Das regulierte Unternehmen muss ein geeignetes Änderungsmanagement und Abweichungsmanagement für kundenspezifische Applikationen sicherstellen (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 kann die Berichte der Standardproduktkonfiguration der Software SIMATIC SIPAT verwenden. Für alle anderen Softwareprodukte, Betriebssysteme, Hosts und Clients muss das regulierte Unternehmen ein geeignetes Berichtswesen, ein Systembestandsverzeichnis sowie Systembeschreibungen pflegen (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 Teil 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	Das Sicherstellen der Tauglichkeit von Testmethoden und Szenarien ist ein integraler Bestandteil des PLM-Prozesses. 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 zur Wartung des Systems.	21 CFR 11.10 (k)	Ja. Während der Produktentwicklung wird die Dokumentation als Teil des Produktes behandelt. In diesem Sinne werden durch den PLM-Prozess geeignete Kontrollmechanismen sichergestellt. Das regulierte Unternehmen muss in der Entwicklung und im Betrieb des Systems 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	Ja. 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)	Ja. 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 Vielzahl von Schulungskursen 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	Um die Bewertung von Vorfällen sowie die Erstellung von Berichten zu ihnen zu unterstützen, werden alle im Zusammenhang mit dem SIMATIC SIPAT-System auftretenden oder von diesem erkannten Vorfälle in Protokolldateien protokolliert. Benutzer mit entsprechenden Zugriffsrechten haben Zugang zu diesen Protokolldateien. Das regulierte Unternehmen muss geeignete Verfahrenskontrollen 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.
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).

	Anforderung	Verweis	Antwort
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 SIPAT folgt dem im Qualitätsmanagementsystem von Siemens festgelegten PLM-Prozess.
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. Für jede Bedienerhandlung wird ein Eintrag im Audit Trail erzeugt. Alle relevanten Änderungen werden einschließlich Zeitstempel und Benutzer-ID sowie des alten und des neuen Werts aufgezeichnet. Je nach Konfiguration wird auch ein Kommentar und eine Bedeutung aufgezeichnet. Unberechtigte Änderungen werden durch den Zugriffsschutz des Systems verhindert. Externe Dokumente, die sich auf die Aufzeichnungen beziehen und ihnen als Anhang hinzugefügt sind, werden einzeln identifiziert. Jede Änderung wird vom System erkannt.
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	Ja. Das Produkt ist so gestaltet, dass Messdaten nicht geändert werden können. Jede betriebsbedingte Änderung von Daten und Metadaten wird im Audit Trail aufgezeichnet und kann in einem Bericht ausgedruckt werden.

	Anforderung	Verweis	Antwort
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. Alle Datenbankaufzeichnungen können über Berichte in SIMATIC SIPAT (Berichterstellung wird als Option mit dem System angeboten) und den SIMATIC SIPAT Data Miner angezeigt werden. Hierfür kann auch jedes andere Programm zur Anzeige von Datenbankeinträgen verwendet werden. Elektronische Aufzeichnungen, einschließlich Audit Trail, können in den Formaten PDF, Microsoft Excel und ASCII erzeugt werden und sind sofort lesbar. Kopien des gesamten Berichts können ebenfalls exportiert werden. Konfigurations- und Laufzeitdaten können im SIMATIC SIPAT Client und im Data Miner eingesehen 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	Ja. Das System besitzt integrierte Plausibilitätskontrollen für die Dateneingabe.
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	SIMATIC SIPAT unterstützt die automatische Erstellung von Sicherungskopien. Das regulierte Unternehmen hat geeignete Prozesse für die Datensicherung und -wiederherstellung einzurichten (siehe GAMP 5, Anhang O9).

	Anforderung	Verweis	Antwort
4.3.8	Elektronische Aufzeichnungen müssen über den gesamten Aufbewahrungszeitraum der Dokumente abrufbar sein.	21 CFR 11.10 (c) Annex 11, 17	Ja. In der SIMATIC SIPAT-Datenbank gespeicherte Aufzeichnungen können abgerufen und über den SIMATIC SIPAT Data Miner und die SIMATIC SIPAT-Berichte exportiert werden. Exportierte Daten und Berichte müssen vom regulierten Unternehmen sicher gespeichert werden, um die Wiederabrufbarkeit während des Aufbewahrungszeitraums zu gewährleisten. Das regulierte Unternehmen ist dafür verantwortlich, für den Bericht ein korrektes Exportformat zu verwenden. Verfügbare Formate sind: XML, CSV und PDF. Die Bereitstellung von Funktionalitäten zur Sicherung aller Aufzeichnungen, die Durchführung von Wiederherstellungstests und die Aufbewahrung der Aufzeichnungen für den dafür vorgesehenen Zeitraum liegen in der Verantwortung des Kunden.
4.3.9	Wenn eine Reihenfolge von Systemschritten oder Ereignissen wichtig ist, so sind geeignete funktionale Systemüberprüfungen umzusetzen.	21 CFR 11.10 (f)	Ja. Standardprozesse und -verfahren zur Sequenzierung von Schritten und Ereignissen liegen im System vor und werden mittels Sicherheitskontrollen durchgesetzt. Dafür sorgen vordefinierte Zustandsmechanismen; sie umfassen darüber hinaus einen Sicherheitsschutz, sodass nur autorisiertes Personal manuell Zustandsübergänge veranlassen kann. Personen ohne diese Berechtigung können diesen Eingriff nicht durchführen. Alle Zustandsübergänge werden im Audit Trail des Objekts protokolliert. Nur Objekte mit dem Status "GMP" sind an einer GMP-Station ausführbar. In der Standardkonfiguration entspricht dies dem Status "Freigegeben". Um den Status "GMP" für eine Objekt zu erhalten, ist eine elektronische Unterschrift erforderlich.

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. Änderungen während des Betriebs können vom System selbst via Audit Trail zurückverfolgt werden und enthalten Informationen mit Zeitstempel, Benutzer-ID, altem Wert, neuem Wert und Kommentar. Der Audit Trail ist innerhalb des Systems sicher und kann nicht durch einen Benutzer geändert werden. Der Audit Trail kann in elektronisch übermittelbaren Dokumentenformaten zur Verfügung gestellt und exportiert 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	Ja. Siehe auch Anforderung 4.4.1.
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. Dies ist technisch umsetzbar und muss im applikationsspezifischen Sicherungs- und Wiederherstellungsprozess des regulierten Unternehmens 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. Siehe auch Anforderung 4.4.1.

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. Der Systemzugriff basiert auf der Benutzerverwaltung von Microsoft Windows. Die Benutzerberechtigungen sind im System festzulegen. Dennoch sind auch 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 allerdings die Systemsicherheit in hohem Maße von der Betriebsumgebung des jeweiligen IT-Systems abhängig ist, sind diese Aspekte im Sicherheitsmanagement des regulierten Unternehmens zu berücksichtigen (siehe GAMP 5, Anhang O11). Empfehlungen und Unterstützung sind über Siemens Industrial Security (http://www.siemens.com/industrialsecurity) erhältlich.
4.5.3	Die Erstellung, Änderung und der Entzug von Zugriffsberechtigungen sind aufzuzeichnen.	Annex 11, 12.3	Ja. Änderungen innerhalb der Benutzerzugriffsverwaltung werden 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. Zur Vermeidung ungültiger Datenquellen wird der Ort bestimmter SIMATIC SIPAT-Komponenten im Allgemeinen und die Quelle der Eingabedaten im Besonderen im System konfiguriert: Alle Komponenten werden auf einer sogenannten SIMATIC SIPAT-Station betrieben. SIMATIC SIPAT-Stationen legen fest, welcher PC tatsächlich verwendet wird, und werden, wie oben beschrieben, mit integrierten Kontrollen konfiguriert. Die Übertragung aller Daten wird auf Fehler geprüft und die erfolgreiche Übermittlung unter Verwendung des TCP/IP-Protokolls bestätigt.
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)	Der Zugriff auf SIMATIC SIPAT basiert auf der Benutzerkontensteuerung von Microsoft Windows. Benutzer-ID und Passwort werden auf Betriebssystemebene verwaltet. Benutzer-ID oder Passwort werden nicht auf dem lokalen PC gespeichert. Die Implementierung und Verwendung der Benutzerverwaltung von Microsoft Windows mit dem Ziel, unberechtigten Zugriff auf Passwörter zu verhindern, liegt im Verantwortungsbereich des regulierten Unternehmens.
4.5.6	Es sind Verfahren vorhanden, die gewährleisten, dass die Gültigkeit von Benutzerkennungen regelmäßig überprüft wird.	21 CFR 11.300 (b)	Das regulierte Unternehmen muss geeignete Verfahrenskontrollen schaffen (siehe "Gute Praxis und Erfüllung der Anforderungen an Elektronische Aufzeichnungen und Unterschriften, Teil 2").

	Anforderung	Verweis	Antwort
4.5.7	Passwörter müssen regelmäßig ablaufen und sind regelmäßig zu ändern.	21 CFR 11.300 (b)	Die Passwortalterung ist eine Standardfunktion der Benutzerverwaltung von Microsoft Windows. Ihre Implementierung liegt in der Verantwortung des regulierten Unternehmens.
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)	Das regulierte Unternehmen muss geeignete Verfahrenskontrollen schaffen (siehe "Gute Praxis und Erfüllung der Anforderungen an Elektronische Aufzeichnungen und Unterschriften, Teil 2"). Die Benutzerverwaltung von Microsoft Windows kann dazu genutzt werden, Benutzerkonten zu deaktivieren.
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 und anderen Geräten, die Benutzerkennungen oder Passwörter enthalten oder erzeugen, aufgehoben werden, sowie Verfahren, mit denen unter Einsatz geeigneter, strenger Kontrollen temporärer oder dauerhafter Einsatz ausgegeben wird.	21 CFR 11.300 (c)	Bei Passwortverlust kann das Microsoft Windows-Konto deaktiviert werden. Eine verlorene Kombination aus Benutzer-ID und Passwort kann durch eine neue Kombination ersetzt werden. Löschungen oder Modifikationen des Benutzernamens werden mithilfe von Verfahrenskontrollen durchgeführt. Das regulierte Unternehmen muss geeignete Verfahrenskontrollen schaffen (siehe "Gute Praxis und Erfüllung der Anforderungen an Elektronische Aufzeichnungen und Unterschriften, Teil 2").
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)	Ja. Fehlerhafte Versuche einer Nutzung des Systems oder der Tätigung von elektronischen Unterschriften werden erkannt und protokolliert: Fehlgeschlagene Versuche werden unmittelbar an die Benutzerschnittstelle gemeldet. Bei Verwendung der Standardinstallation von SIMATIC SIPAT wird das Benutzerkonto nach drei fehlgeschlagenen Versuchen deaktiviert. Das regulierte Unternehmen muss geeignete Verfahrenskontrollen schaffen, um eine regelmäßige Prüfung der Sicherheits- und Zugriffskontrollprotokolle zu gewährleisten (siehe GAMP 5, Anhang O8). Es ist die Aufgabe des Administrators für SIMATIC SIPAT, das Benutzerkonto zu entsperren, wenn das Konto von SIMATIC SIPAT gesperrt wurde.
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 schaffen (siehe "Gute Praxis und Erfüllung der Anforderungen an Elektronische Aufzeichnungen und Unterschriften, Teil 2").

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. Unterschriftsangaben enthalten folgende Informationen: • Benutzer-ID (eindeutig) und vollständigen Benutzernamen • Datum und Uhrzeit (Ortszeit und UTC-Zeit) • Produktfunktionalität erfasst Art der durch den Unterzeichner ausgeführten Aktion • die Bedeutung der elektronischen Unterschrift (siehe Kommentar unten). Kommentar: Die Bedeutung der elektronischen Unterschrift wird aus einer Dropdown-Liste im Fenster für die elektronische Unterschrift gewählt. Die Liste der Bedeutungen für einen betreffenden Zustandsübergang kann vollständig durch das regulierte Unternehmen angepasst werden. In der Standardinstallation von SIMATIC SIPAT sind keine Bedeutungen vordefiniert. Falls Bedeutungen für einen bestimmten Zustandsübergang vorhanden sind, muss ein Wert ausgewählt werden, um die elektronische Unterschrift zu leisten. Die für eine elektronische Unterschrift ausgewählte Bedeutung wird erfasst. In einem zusätzlichen Feld können zusätzlich Kommentare (Notizen) zur ausgeführten Aktion hinterlassen werden. Zum Beispiel: Ein Kommentar kann in einigen Fällen der näheren oder detaillierteren Erläuterung einer Aktion dienen.
4.6.3	Die oben genannten Informationen erscheinen auf den angezeigten und gedruckten Kopien der elektronischen Aufzeichnung.	21 CFR 11.50 (b)	Ja. Die Unterschriftsangaben sind in gleicher Weise geschützt wie die mit ihnen verknüpften elektronischen Aufzeichnungen. Die Unterschriftsangaben können im SIMATIC SIPAT Client angezeigt und mit den SIMATIC SIPAT-Berichten ausgedruckt werden.

	Anforderung	Verweis	Antwort
4.6.4	Elektronische Unterschriften müssen mit den entsprechenden elektronischen Aufzeichnungen so verknüpft sein, dass die Unterschriften nicht entfernt, kopiert oder anderweitig zum Zwecke der Fälschung der elektronischen Aufzeichnung mit üblichen Mitteln übertragen werden können.	21 CFR 11.70 Annex 11, 14.b	Ja. Unterschriftsangaben sind als elektronische Aufzeichnungen geschützt und mit der zugehörigen elektronischen Aufzeichnung verknüpft. Benutzer können die Angaben einer elektronischen Unterschrift nicht entfernen, kopieren oder anderweitig fälschen. Es sind zusätzliche Sicherheitsmaßnahmen zu ergreifen, um die Administratorrechte für SIMATIC SIPAT in der zentralen Datenbank zu schützen. Das regulierte Unternehmen trägt hierfür die Verantwortung.
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 Zugriffssteuerung für SIMATIC SIPAT basiert auf der Benutzerverwaltung von Microsoft Windows. Benutzer-ID und Passwort werden auf Betriebssystemebene verwaltet. Benutzer-ID oder Passwort werden in keiner Weise auf dem lokalen PC gespeichert. Die korrekte Implementierung und Verwendung der Benutzerverwaltung von Microsoft Windows liegt im Verantwortungsbereich des regulierten Unternehmens. Die Wiederverwendung oder Neuzuordnung von elektronischen Unterschriften wird effektiv unterbunden. Durch die Verwendung von Sicherheitsrollen in der Produktfunktionalität wird die Notwendigkeit einer Passwortfreigabe hinfällig. Die Implementierung von Verfahrensanweisungen zur Unterbindung der Passwortfreigabe liegt in der Verantwortung des regulierten Unternehmens.
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. Das regulierte Unternehmen ist dafür verantwortlich, die notwendigen Kontrollmechanismen einzurichten, um sicherzustellen, dass es nur qualifizierten Personen gestattet wird, die Freigabe von Chargen zu bestätigen.
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 ist dafür verantwortlich, geeignete Verfahrenskontrollen für die Verifizierung der Identität einer Person einzurichten, bevor ein Benutzerkonto und/oder elektronische Unterschriften zugewiesen werden.
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. Werden elektronische Unterschriften nicht innerhalb derselben ununterbrochenen Sitzung geleistet, so ist für jede Unterschrift die erneute Eingabe der beiden Komponenten Anmeldeinformationen und Passwort erforderlich.

	Anforderung	Verweis	Antwort
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. Benutzer müssen sich in einem System anmelden, damit der Systemzugriff kontrolliert wird, aber diese Anmeldung dient nicht zum Erstellen einer elektronischen Unterschrift (zunächst muss bei erstmaliger elektronischen Unterschrift die Benutzer-ID neu eingegeben werden, das Passwort muss immer neu eingegeben werden).
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. Darüber hinaus muss das regulierte Unternehmen geeignete Verfahrenskontrollen etablieren, um die Offenlegung von Passwörtern zu verhindern. Der Systemadministrator besitzt die Zugriffsrechte zur Passwortänderung auf Betriebssystemebene. Durch die Einrichtung zusätzlicher Sicherheitsfunktionen können die Rechte des einzelnen Administrators begrenzt werden (dies liegt in der Verantwortung des regulierten Unternehmens).
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)	Die Erstellung elektronischer Unterschriften auf der Grundlage biometrischer Daten zählt nicht zum Standardfunktionsumfang des Produkts.

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	Ja. Die Verschlüsselung der Kommunikation zwischen verschiedenen Diensten sowie zwischen Diensten und Clients wird konsistent implementiert.
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 SIPAT besitzt keine Funktionalität für digitale (verschlüsselte) Unterschriften.

Weitere Informationen

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

PDF (A5E50732433-AA)
Produced in Germany