

The image shows a Siemens SIMATIC WinCC control panel in an industrial environment. The panel features a large touchscreen displaying a technical diagram of a process, with the word "TOUCH" printed vertically on the right side of the screen. Below the screen are several physical buttons: a black rotary knob, a green button, a white button, a red button, and a prominent red emergency stop button. The panel is mounted on a stainless steel stand. In the background, there is a complex industrial machine with multiple vertical stainless steel columns, each equipped with a blue motor at the top. The machine is connected to a network of pipes and valves. The overall scene is brightly lit, highlighting the metallic surfaces of the equipment.

**SIEMENS**

**SIMATIC**

**SIMATIC WinCC (TIA Portal) V14**

Elektronische Aufzeichnungen / Elektronische Unterschriften (ERES)

Konformitätserklärung

Ausgabe

03/2017

Answers for industry.



# SIEMENS

## SIMATIC

### SIMATIC WinCC (TIA Portal) V14 Konformitätserklärung ERES

Produktinformation


<u>Einleitung</u>	<b>1</b>
<u>Die Anforderungen im Überblick</u>	<b>2</b>
<u>Erfüllung der Anforderungen durch SIMATIC WinCC (TIA Portal)</u>	<b>3</b>
<u>Bewertungsliste für SIMATIC WinCC (TIA Portal)</u>	<b>4</b>


Elektronische Aufzeichnungen /  
Elektronische Unterschriften (ERES)


## 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.

 <b>GEFAHR</b>
bedeutet, dass Tod oder schwere Körperverletzung eintreten <b>wird</b> , wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

 <b>WARNUNG</b>
bedeutet, dass Tod oder schwere Körperverletzung eintreten <b>kann</b> , wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

 <b>VORSICHT</b>
bedeutet, dass eine leichte Körperverletzung eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

<b>ACHTUNG</b>
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:

 <b>WARNUNG</b>
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.

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung.....</b>	<b>7</b>
<b>2</b>	<b>Die Anforderungen im Überblick.....</b>	<b>9</b>
<b>3</b>	<b>Erfüllung der Anforderungen durch SIMATIC WinCC (TIA Portal).....</b>	<b>11</b>
3.1	Lebenszyklus und Validierung von computergestützten Systemen.....	11
3.2	Lieferanten und Dienstleister.....	11
3.3	Datenintegrität.....	12
3.4	Audit Trail, Unterstützung der Änderungskontrolle.....	13
3.5	Systemzugriff, Benutzerkennungen und Passwörter.....	15
3.6	Elektronische Unterschrift.....	17
<b>4</b>	<b>Bewertungsliste für SIMATIC WinCC (TIA Portal).....</b>	<b>19</b>
4.1	Lebenszyklus und Validierung von computergestützten Systemen.....	19
4.2	Lieferanten und Dienstleister.....	21
4.3	Datenintegrität.....	22
4.4	Audit Trail, Unterstützung der Änderungskontrolle.....	23
4.5	Systemzugriff, Benutzerkennungen und Passwörter.....	24
4.6	Elektronische Unterschrift.....	26
4.7	Offene Systeme.....	28



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 WinCC (TIA Portal) das System in der Version 14 im Hinblick auf diese Anforderungen bewertet und die Ergebnisse in der vorliegenden Konformitätserklärung veröffentlicht. Aufgrund des Detaillierungsgrades wurde diese Analyse anhand der oben erwähnten Regulierungen und Richtlinien durchgeführt.

## **SIMATIC WinCC (TIA Portal) V14 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 den Kunden (das regulierte Unternehmen) festzulegen sind. Solche Verfahrenskontrollen werden in Kapitel "Bewertungsliste für SIMATIC WinCC (TIA Portal) (Seite 19)" des vorliegenden Dokuments genannt.

Das vorliegende Dokument gliedert sich in drei Teile:

1. Kapitel "Die Anforderungen im Überblick (Seite 9)" enthält eine kurze Beschreibung der verschiedenen Anforderungsthemen.
2. In Kapitel "Erfüllung der Anforderungen durch SIMATIC WinCC (TIA Portal) (Seite 11)" wird die Funktionalität von SIMATIC WinCC (TIA Portal) V14 vorgestellt, mittels derer diese Anforderungen erfüllt werden.
3. Kapitel "Bewertungsliste für SIMATIC WinCC (TIA Portal) (Seite 19)" enthält eine ausführliche Systembewertung anhand der einzelnen Anforderungen der entsprechenden Vorschriften.



## Die Anforderungen im Überblick

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 berechnigte 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	<p>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.</p> <p>Die Funktionalität des Systems muss über den gesamten Lebenszyklus hinweg in Form von Spezifikationen oder einer Systembeschreibung nachvollziehbar dokumentiert werden.</p> <p>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.</p>
Lieferanten und Dienstleister	<p>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.</p>

Anforderung	Beschreibung
Datenintegrität	<p>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.</p> <p>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.</p>
Audit Trail, Unterstützung der Änderungskontrolle	<p>Neben der im Lebenszyklus definierten Kontrolle von Änderungen am System verlangen beide Regelwerke, dass auch Änderungen an GMP-relevanten Daten aufgezeichnet werden.</p> <p>Ein solcher Audit Trail sollte Informationen zur Änderung (vorher/nachher), zur Identität des Bedieners, einen Zeitstempel sowie den Grund für die Änderung umfassen.</p>
Systemzugriff, Benutzerkennungen und Passwörter	<p>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.</p> <p>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.</p> <p>Dem Einsatz von Geräten, die Benutzerkennungen oder Passwortinformationen enthalten oder erzeugen, ist besondere Aufmerksamkeit zu widmen.</p>
Elektronische Unterschrift	<p>Aus der Sicht der Regelwerke sind elektronische Unterschriften rechtlich bindend und in jeder Hinsicht auf Papier geleisteten handschriftlichen Unterschriften gleichwertig.</p> <p>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.</p>
Offene Systeme	<p>Bei offenen Systemen können zur Sicherstellung der Datenintegrität und Vertraulichkeit weitere Kontrollen oder Maßnahmen erforderlich sein.</p>

# Erfüllung der Anforderungen durch SIMATIC WinCC (TIA Portal)

# 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 WinCC (TIA Portal)" von Siemens.

Die in Kapitel "Die Anforderungen im Überblick (Seite 9)" dargestellten Anforderungen können, wie im Folgenden gezeigt, durch das System unterstützt werden.

## 3.1 Lebenszyklus und Validierung von computergestützten Systemen

Obwohl bereits 1992 im Annex 11 bzw. 1997 im Part 11 betont wurde, dass computergestützte Systeme zu validieren seien, wurden umfassende Kriterien für die Validierung des Systems und dessen Lebenszyklus erst im Jahr 2011 mit der überarbeiteten Version von Annex 11 eingeführt.

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 SIMATIC-Hardware- und SIMATIC-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.

#### Kontinuierliche Archivierung

Prozessdaten (Meldungen, Prozesswerte) und Audit Trails können aufgezeichnet und gespeichert werden. Außerdem können sie in Langzeitarchive ausgelagert werden, wobei durch das Prüfsummenverfahren die Datenintegrität abgesichert wird.

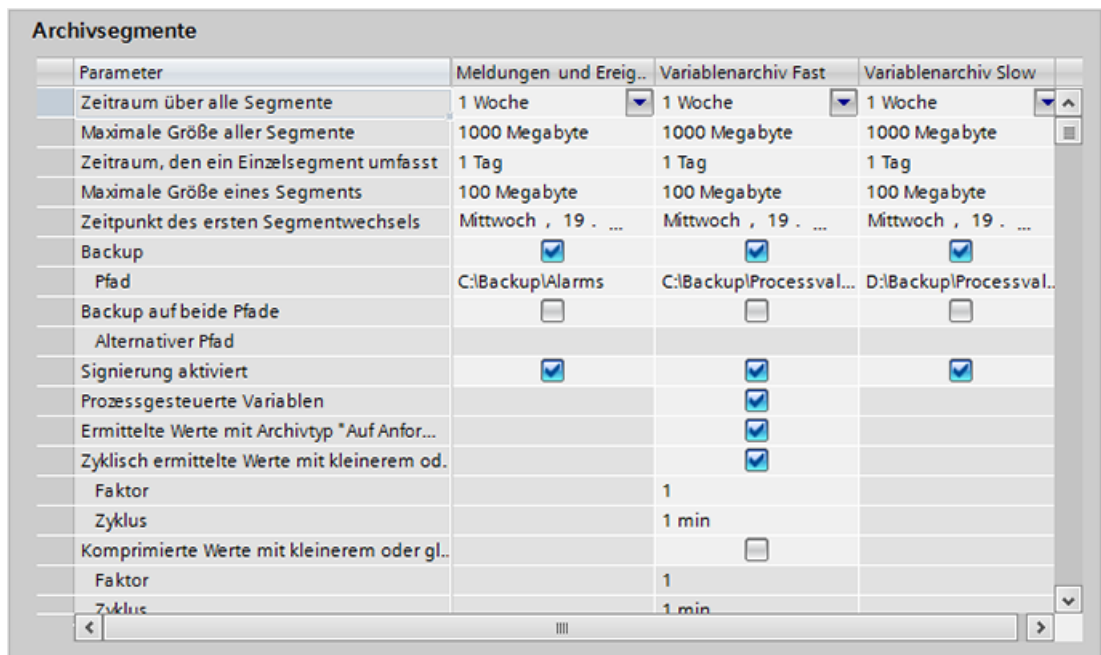


Bild 3-1 Konfiguration der Archivierungsstrategie für WinCC Runtime Professional

Bei Verwendung lokaler HMI-Geräte werden die Daten auf einem lokalen Speichergerät (z. B. CF-Karte) zwischengespeichert und anschließend über das Netzwerk oder USB-Gerät übertragen.

#### Chargenorientierte Archivierung

Das WinCC Premium-Add-on PM-QUALITY wird zur chargenorientierten Datenarchivierung eingesetzt. PM-QUALITY übernimmt die automatische Verwaltung der lokalen Archive und Langzeitarchive. Für den Zugriff auf die WinCC-Daten nutzt PM-QUALITY die Standardschnittstellen von SIMATIC WinCC. Diese Schnittstellen sind für andere Archivierungstools (von Siemens und Drittherstellern) ebenfalls verfügbar.

## 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 nachfolgenden Abschnitte beschreiben die Umsetzung von Anforderungen im Hinblick auf Audit Trails im laufenden Betrieb und geben darüber hinaus Hinweise für die Verfolgung von im Engineering System vorgenommenen Änderungen.

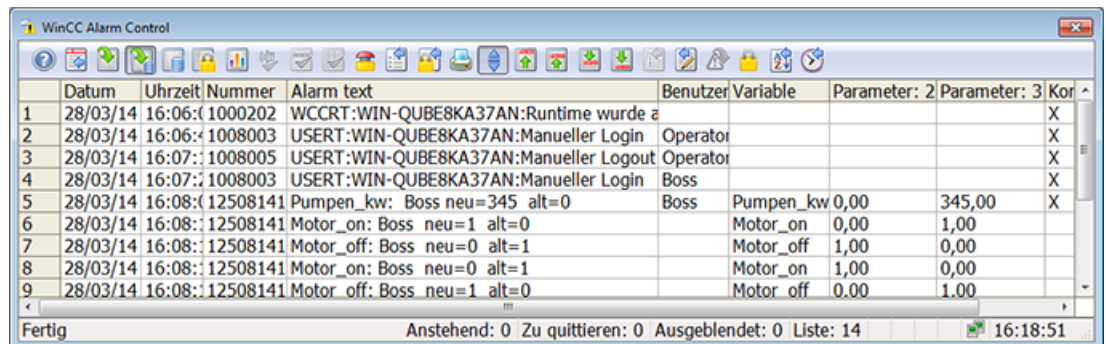
### Audit Trail im laufenden Betrieb

SIMATIC WinCC (TIA Portal) unterstützt die Anforderung eines Audit Trails bei GMP-relevanten Bedienaktionen durch entsprechende Aufzeichnung dieser Aktionen (wer, was, wann und optional, warum). Solche elektronischen Aufzeichnungen werden durch systemseitige Sicherheitsmechanismen (z. B. Zugriffsschutz) gesichert. Die GMP-relevanten Daten werden durch das regulierte Unternehmen gemäß der für ihn geltenden gesetzlichen Vorschriften definiert.

Prozessdaten (z. B. Prozesswerte, Prozess- oder Bedienmeldungen) werden im System gespeichert, ohne dass der Bediener die Möglichkeit hat, Änderungen vorzunehmen. Für diese Daten ist kein Audit Trail erforderlich.

### WinCC Runtime Professional

In WinCC vorgenommene Bedieneingriffe können in einem Audit Trail aufgezeichnet werden. Der Audit Trail kann gedruckt, exportiert und archiviert werden.



	Datum	Uhrzeit	Nummer	Alarm text	Benutzer	Variable	Parameter: 2	Parameter: 3	Kor.
1	28/03/14	16:06:	1000202	WCCRT:WIN-QUBE8KA37AN:Runtime wurde a					X
2	28/03/14	16:06:	1008003	USERT:WIN-QUBE8KA37AN:Manueller Login	Operator				X
3	28/03/14	16:07:	1008005	USERT:WIN-QUBE8KA37AN:Manueller Logout	Operator				X
4	28/03/14	16:07:	1008003	USERT:WIN-QUBE8KA37AN:Manueller Login	Boss				X
5	28/03/14	16:08:	12508141	Pumpen_kw: Boss neu=345 alt=0	Boss	Pumpen_kw	0,00	345,00	X
6	28/03/14	16:08:	12508141	Motor_on: Boss neu=1 alt=0		Motor_on	0,00	1,00	
7	28/03/14	16:08:	12508141	Motor_off: Boss neu=0 alt=1		Motor_off	1,00	0,00	
8	28/03/14	16:08:	12508141	Motor_on: Boss neu=0 alt=1		Motor_on	1,00	0,00	
9	28/03/14	16:08:	12508141	Motor_off: Boss neu=1 alt=0		Motor_off	0,00	1,00	

Fertig Anstehend: 0 Zu quittieren: 0 Ausgeblendet: 0 Liste: 14 16:18:51

Bild 3-2 Anzeige des Audit Trails über Alarm Logging

### Comfort Panels / WinCC Runtime Advanced

Welche Daten im Audit Trail zu verfolgen sind, kann im Engineering-System konfiguriert werden, siehe Abbildung unten. Hierbei kann als Bestätigungstyp "ohne Bestätigung", "mit Bestätigung" oder "mit elektronischer Unterschrift" angewählt werden. Ein Kommentar kann optional oder verpflichtend sein.

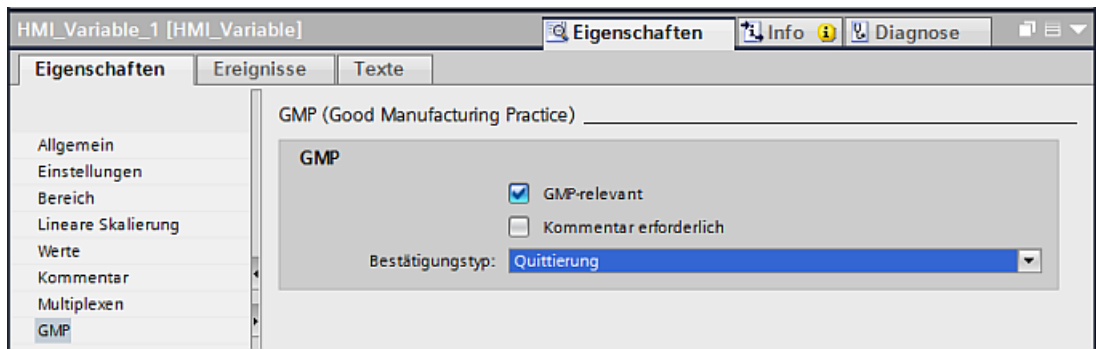


Bild 3-3 Eine Variable wird als GMP-relevant klassifiziert, sodass ein Audit-Trail-Eintrag immer dann erstellt wird, wenn diese vom Benutzer geändert wird.

Der Audit Trail wird als RDB-Datei (Binärdatei) gespeichert. Außerdem ist eine Archivierung als CSV- oder Unicode-fähige TXT-Datei möglich. Ein integrierter Algorithmus bildet automatisch eine Prüfsumme für jeden Datensatz. Anhand der Prüfsumme kann der Benutzer manuelle Veränderungen der Datensätze erkennen.

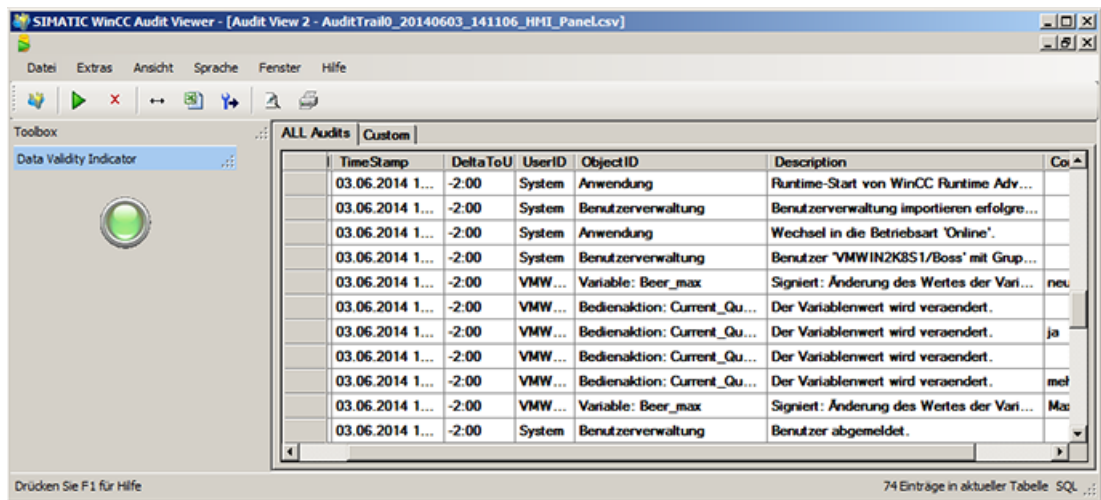


Bild 3-4 Im Audit Viewer wird die Audit-Trail-Datei der Comfort Panels und von WinCC Runtime Advanced angezeigt; die grüne Signallampe bestätigt, dass der Audit Trail nicht manipuliert wurde.

### Konfigurationskontrolle

SIMATIC WinCC (TIA Portal) verfügt über bestimmte Systemfunktionen, Optionen und Add-ons zur Unterstützung der Kontrolle der Systemkonfiguration. Enthalten sind u. a. die Versionierung von Softwareelementen und -projekten sowie Funktionen zur Datensicherung/-wiederherstellung, mit denen die entsprechenden Verfahren unterstützt werden. Nähere Informationen enthält das "GMP Engineering Handbuch SIMATIC WinCC (TIA Portal)" von Siemens.

## 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.

Falls es "offene Pfade" gibt, müssen diese durch zusätzliche Sicherheitsmechanismen abgesichert werden. Grundprinzipien des Sicherheitskonzepts sowie Konfigurationsempfehlungen enthält das Handbuch "Sicherheitskonzept PCS 7 und WinCC".

Die Konfiguration der Benutzerverwaltung erfolgt für die einzelnen Applikationen zentral über ein Engineering-System. Nach Prüfung der Anmeldedaten auf Richtigkeit werden die entsprechenden Benutzergruppeninformationen, die die Benutzerzugriffsrechte festlegen, auf die jeweiligen HMI-Geräte übertragen.

SIMATIC WinCC (TIA Portal) unterstützt den Schutz elektronischer Aufzeichnungen durch:

- Verwendung einer eindeutigen Benutzerkennung (Benutzer-ID) in Verbindung mit einem Passwort.
- Definition von Zugriffsberechtigungen für Benutzergruppen.
- Passworteinstellungen und Passwortalterung: Der Benutzer muss sein Passwort nach einer einstellbaren Zeit ändern; das Passwort kann erst nach "n" Generationen wieder verwendet werden.
- Erzwingen eines neuen Passworts bei der ersten Anmeldung (Initialpasswort).
- Der Benutzer wird automatisch nach einer einstellbaren Anzahl von fehlerhaften Anmeldeversuchen gesperrt und kann nur durch den Administrator wieder entsperrt werden.
- Automatisches Abmelden (Auto-Logout) nach einer konfigurierbaren Zeit, in der weder Tastatur noch Maus benutzt wurden.
- Log-Funktionen für Aktionen hinsichtlich des Zugriffsschutzes, z. B. Anmeldung, manuelles und automatisches Abmelden, fehlgeschlagene Anmeldeversuche, Sperrung des Benutzers nach mehrfacher Falscheingabe des Passwortes, Passwortänderung durch den Benutzer.

### Zentrale Benutzerverwaltung

Wir empfehlen die Implementierung einer zentralen Benutzerverwaltung basierend auf Microsoft Windows und SIMATIC Logon, wenn anwendbar in einer Domänenstruktur.

- Die einzelnen Nutzer und deren Zuordnung zu Windows-Benutzergruppen werden in der Benutzerkontensteuerung von MS Windows definiert.
- SIMATIC Logon stellt die Verbindung zwischen den Windows-Benutzergruppen und den Benutzergruppen des WinCC Runtime-Systems her.

- Benutzerberechtigungen mit unterschiedlichen Berechtigungsstufen werden in Abhängigkeit von Benutzergruppen in der Benutzerverwaltung für ein konkretes HMI-Gerät oder für das WinCC Runtime-System definiert.
- Kann keine Netzwerkverbindung hergestellt werden, wird die Benutzerverwaltung von der lokalen Benutzerverwaltung übernommen. So kann ein für den Notfall festgelegter Benutzer für einen festgelegten Notbetrieb eingesetzt werden. SIMATIC Logon-Nutzer (zentrale Nutzer), die bereits angemeldet sind, bleiben bis zur Abmeldung aktiv.

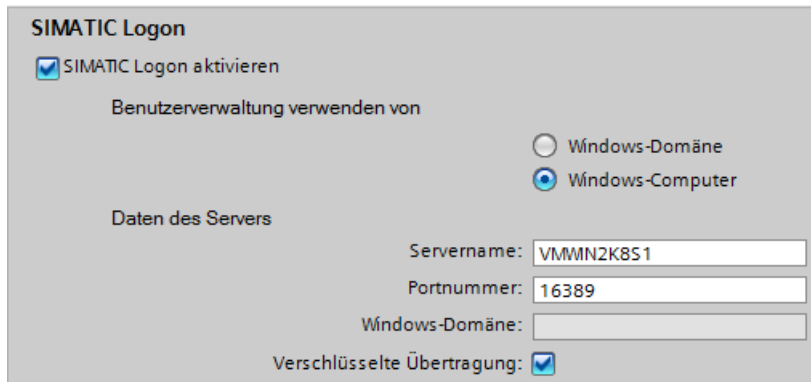


Bild 3-5 Aktivierung der Benutzerverwaltung auf Basis von Microsoft Windows und SIMATIC Logon

### Benutzerverwaltung auf lokalen HMI-Geräten

Lokale HMI-Geräte werden oftmals ohne Netzwerkverbindung installiert. Daher kann auf diesen HMI-Geräten die lokale Benutzerverwaltung in SIMATIC WinCC (TIA Portal) implementiert werden. In diesem Fall sind einzelne Nutzer und deren Zuordnung zu Benutzergruppen nur lokal bekannt.

- Die einzelnen Benutzer und deren Zuordnung zu Benutzergruppen werden in der WinCC-Projektierung definiert.
- Benutzerberechtigungen mit unterschiedlichen Berechtigungsstufen werden in Abhängigkeit von Benutzergruppen in der Benutzerverwaltung für ein konkretes HMI-Gerät oder das WinCC Runtime Advanced-System definiert.



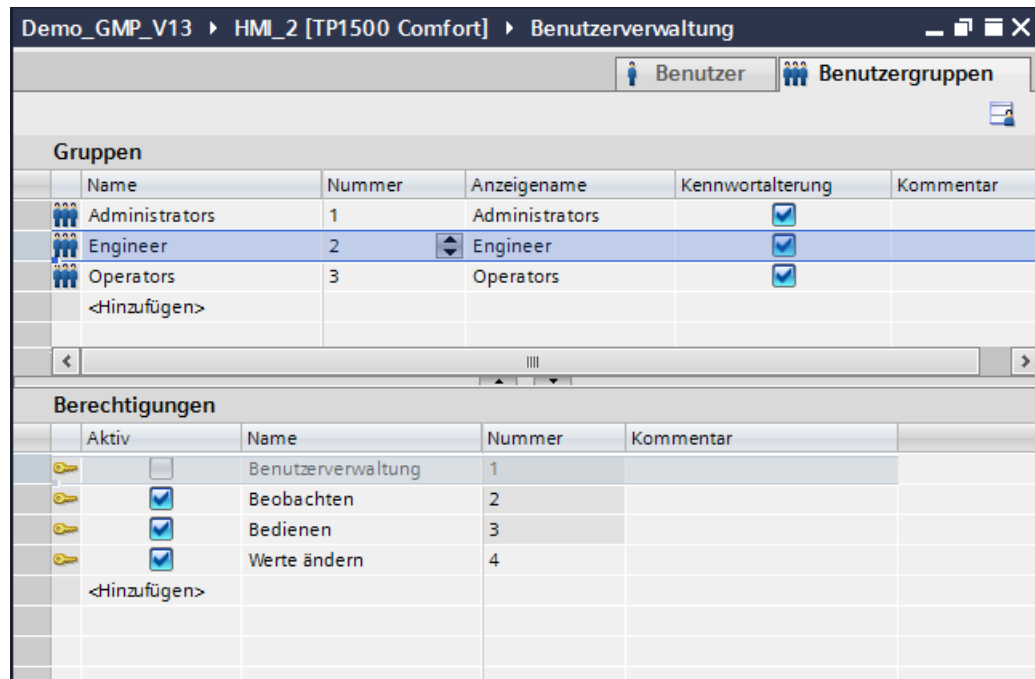


Bild 3-6 Zuordnung von Benutzerberechtigungen zu Benutzergruppen

### 3.6 Elektronische Unterschrift

SIMATIC WinCC (TIA Portal) bietet Funktionen zur Konfiguration einer elektronischen Unterschrift. Die elektronische Unterschrift wird in einem Dialog ausgeführt. In der Projektierungsphase wird angegeben, für welche Variablen bei einer Veränderung eine elektronische Unterschrift erforderlich ist. Der Benutzer kann elektronisch unterschreiben, indem er die beabsichtigte Handlung durch Eingabe seines Passworts bestätigt. Dadurch wird die elektronische Unterschrift im Audit Trail zusammen mit dem Benutzernamen, Zeitstempel und der ausgeführten Aktion hinterlegt.

Bei den SIMATIC Comfort Panels und bei WinCC Runtime Advanced ist ein separater Unterschriftsdialog mit der Option "SIMATIC WinCC Audit für SIMATIC Panels" oder "SIMATIC WinCC Audit für Runtime Advanced" verfügbar. Der Kommentar kann für jedes Objekt als optional oder zwingend zur Eingabe konfiguriert werden.

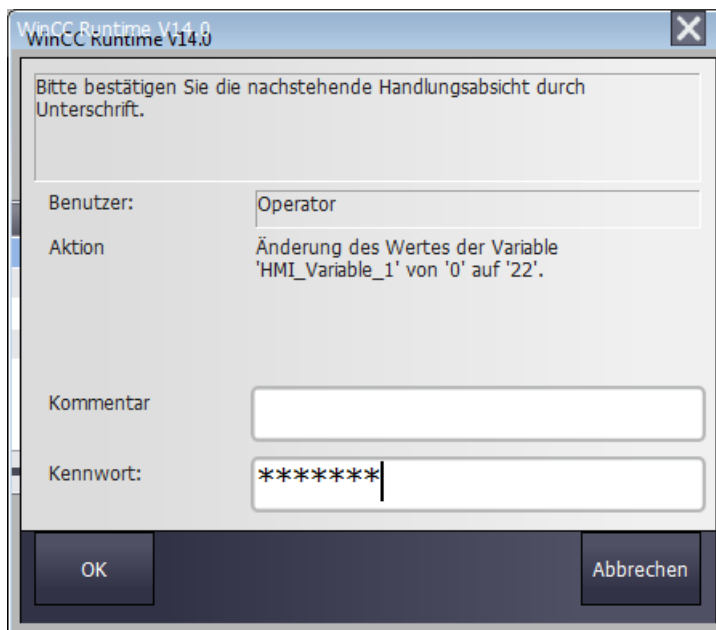


Bild 3-7 Elektronische Unterschrift zur Änderung eines Variablenwerts über ein Comfort Panel oder in WinCC Runtime Advanced, hier mit optionalem Kommentar

## Bewertungsliste für SIMATIC WinCC (TIA Portal)

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 9)" 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 im Annex 11 durch mehrere neuere Anforderungen ergänzt, die weitere 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 hinweg durchzuführen.	Annex 11, 1	Der Entwicklungsprozess für Siemens-Softwareprodukte 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 dem Siemens QMS und dem PLM-Prozess (Product Lifecycle Management). 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 Entwicklungsprozess für das Softwareprodukt erstreckt sich auf alle entsprechenden Schritte des Software Development Life Cycle (SDLC). Die Verantwortung für die Validierung der Applikation (siehe Annex 11, Glossar) liegt beim regulierten Unternehmen.

4.1 Lebenszyklus und Validierung von computergestützten Systemen

	Anforderung	Verweis	Antwort
4.1.4	Für die Validierung von maßgeschneiderten oder kundenspezifisch angepassten Systemen muss ein Prozess vorhanden sein.	Annex 11, 4.6	Der Validierungsprozess für kundenspezifische Applikationen liegt in der Verantwortung des regulierten Unternehmens. Siemens bietet jedoch an, den Kunden bei dessen Validierungsaktivitäten zu unterstützen.
4.1.5	Im Rahmen des Validierungsprozesses werden Verfahren zum Management von Änderungen und Abweichungen angewandt.	Annex 11, 4.2	Ja. Der Entwicklungsprozess für das Softwareprodukt 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	In der Produktentwicklung ist die Anforderungsspezifikation Bestandteil des zugehörigen Entwicklungsprozesses. Für die projektspezifische Konfiguration muss das regulierte Unternehmen die Benutzeranforderungen im Lebenszyklus des Systems entsprechend berücksichtigen (siehe GAMP 5, Anhang D1).
4.1.8	Es ist ein Nachweis über geeignete Testmethoden und Testscenarien zu erbringen.	Annex 11, 4.7	Die Sicherstellung der Eignung von Testmethoden und -scenarien ist ein wesentlicher Bestandteil des Entwicklungsprozesses für SIMATIC-Produkte 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 zur 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 Entwicklungsprozess. Während der Entwicklung und des Betriebs eines Produktsystems 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 entsprechend dem Entwicklungsprozess gehandhabt. Während der Entwicklung und dem Betrieb des Systems muss das regulierte Unternehmen geeignete Verfahren etablieren (siehe GAMP 5, Anhänge M8 und O6).
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.

	Anforderung	Verweis	Antwort
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.
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 Entwicklungsprozess.

4.3 Datenintegrität

	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)	Dies ist mithilfe der folgenden Funktionen realisierbar: Zeitstempel, Revisionen, Versionierung für Konfiguration und Dokumente sowie Audit Trail für Bedieneingaben.
4.3.2	Von Protokollen, die zur Chargenfreigabe herangezogen werden, müssen Ausdrücke 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 Add-on-Funktionen in Form eines Berichts ausgedruckt werden.
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 PDF-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. 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 Bedienerdialog realisiert werden.

	Anforderung	Verweis	Antwort
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 Sicherung und Wiederherstellung von Daten eingerichtet (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. Wie oben angegeben, müssen Verfahrenskontrollen für die Sicherung/Wiederherstellung und die Archivierung/ den Abruf von Daten etabliert sein.
4.3.9	Wenn eine Reihenfolge von Systemschritten oder Ereignissen wichtig ist, so sind geeignete funktionale Systemüberprüfungen 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. Der Audit Trail kann zur Verfügung gestellt und darüber hinaus in das elektronische PDF-Format 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	Sofern Daten im SIMATIC WinCC HMI-Gerät betroffen sind, sind die angeforderten Informationen Teil der Revisionsinformationen, Versionsinformationen und Audit Trails.
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 bleiben in der Datenbank verfügbar.

4.5 Systemzugriff, Benutzerkennungen und Passwörter

	Anforderung	Verweis	Antwort
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 im applikationsspezifischen Prozess zur Datensicherung und -wiederherstellung berücksichtigt werden (vgl. 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 berechnigte 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 berechnigte Personen zu beschränken.	21 CFR 11.10 (d) 21 CFR 11.10 (g) Annex 11, 12.1	Ja. Der Systemzugriff über SIMATIC Logon basiert auf der Benutzerkontensteuerung des Betriebssystems. Die Benutzerberechtigungen müssen im System definiert werden. 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 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 aufgezeichnet und unterliegen dem Änderungskontrollverfahren des regulierten Unternehmens.



	Anforderung	Verweis	Antwort
4.5.4	<p>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?</p> <p>(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.)</p>	21 CFR 11.10 (h)	<p>Ja.</p> <p>Die WinCC HMI-Geräte können so konfiguriert werden, dass spezielle Eingaben/Befehle nur von einem einzelnen dafür vorgesehenen Gerät oder einer Gruppe solcher Geräte geleistet werden können. Alle anderen Geräte verfügen in diesem Fall höchstens über Lesezugriffsrechte.</p>
4.5.5	<p>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.</p>	21 CFR 11.300 (a)	<p>Ja.</p> <p>Die Eindeutigkeit der Benutzerkennung wird entweder durch das Sicherheitssystem von Microsoft Windows (mit SIMATIC Logon) oder durch die lokale Benutzerverwaltung des WinCC HMI-Geräts sichergestellt. Es ist nicht möglich, mehrere Benutzer mit der gleichen Benutzerkennung innerhalb einer Arbeitsgruppe/Domäne zu definieren. Somit ist jede Kombination aus Benutzer-ID und Passwort eindeutig.</p>
4.5.6	<p>Es sind Verfahren vorhanden, die gewährleisten, dass die Gültigkeit von Benutzerkennungen regelmäßig überprüft wird.</p>	21 CFR 11.300 (b)	<p>Das regulierte Unternehmen muss geeignete Verfahrenskontrollen etablieren (siehe "Gute Praxis und Erfüllung der Anforderungen an Elektronische Aufzeichnungen und Unterschriften, Teil 2").</p>
4.5.7	<p>Passwörter müssen regelmäßig ablaufen und sind regelmäßig zu ändern.</p>	21 CFR 11.300 (b)	<p>Ja.</p> <p>Die Passwortalterung lässt sich in der Benutzerverwaltung konfigurieren.</p>
4.5.8	<p>Ein Verfahren zur Aufhebung von Benutzerkennungen und Passwörtern muss für den Fall vorhanden sein, dass eine Person ausscheidet oder innerhalb des Unternehmens wechselt.</p>	21 CFR 11.300 (b)	<p>Das regulierte Unternehmen muss geeignete Verfahrenskontrollen etablieren (siehe "Gute Praxis und Erfüllung der Anforderungen an Elektronische Aufzeichnungen und Unterschriften, Teil 2").</p> <p>Bei Verwendung der zentralen Benutzerverwaltung kann ein Benutzerkonto mit dem Microsoft Windows-Sicherheitssystem deaktiviert werden. In der lokalen Benutzerverwaltung hingegen kann ein Benutzer, statt deaktiviert zu werden, einer Benutzergruppe ohne aktive Berechtigungen zugewiesen werden.</p>

4.6 Elektronische Unterschrift

	Anforderung	Verweis	Antwort
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 Ersatz ausgegeben wird.	21 CFR 11.300 (c)	Das regulierte Unternehmen muss geeignete Verfahrenskontrollen etablieren (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 Tätigkeit 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)	Solche Geräte sind nicht Bestandteil des SIMATIC HMI-Portfolios, können aber möglicherweise über SIMATIC Logon in das System integriert werden. 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 einrichten.
4.6.2	Unterschriebene elektronische Dokumente müssen die folgenden zugehörigen Informationen enthalten: <ul style="list-style-type: none"> <li>• Name des Unterzeichnenden in Druckbuchstaben</li> <li>• Datum und Zeitpunkt der Unterschrift</li> <li>• Bedeutung der Unterschrift (wie z. B. Freigabe, Überprüfung, Verantwortlichkeit)</li> </ul>	21 CFR 11.50 (a) Annex 11, 14.c	Ja.
4.6.3	Die oben genannten Informationen erscheinen auf den angezeigten und gedruckten Kopien der elektronischen Aufzeichnung.	21 CFR 11.50 (b)	Ja.
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 Methoden übertragen werden können.	21 CFR 11.70 Annex 11, 14.b	Ja.
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. Die Wiederverwendung bzw. Neuuzuordnung 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 strenge 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.

4.7 Offene Systeme

	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 Benutzererkennung 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 (Benutzererkennung 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. Dies wird beispielsweise unterstützt durch Konfigurationshinweise im Handbuch "Sicherheitskonzept PCS 7 und WinCC" sowie durch marktübliche Standard-Verschlüsselungstools.
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 WinCC (TIA Portal) besitzt keine Funktionalität für digitale (verschlüsselte) Unterschriften.



## Weitere Informationen

E-Mail:  
[pharma@siemens.com](mailto:pharma@siemens.com)

Internet:  
[www.siemens.com/pharma](http://www.siemens.com/pharma)

Siemens AG  
Process Industries and Drives  
Pharmaceutical and Life  
Science Industry  
76181 Karlsruhe  
GERMANY

Änderungen vorbehalten  
A5E41088906-AA  
© Siemens AG 2017



[www.siemens.com/automation](http://www.siemens.com/automation)