SIEMENS

Ausgabe 05/2022

GMP ENGINEERING HANDBUCH

SIMATIC

SIMATIC PCS 7 V9.1

Leitfaden zur Durchführung von Automatisierungsprojekten im GMP Umfeld

siemens.com/pharma

SIEMENS

SIMATIC

SIMATIC PCS 7 V9.1
GMP Engineering Handbuch

Projektierungshandbuch

Leitfaden zur Durchführung von Automatisierungsprojekten im GMP Umfeld

05/2022
A5E42888172-AB

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

A5E42888172-AB
Ⓟ 05/2022 Änderungen vorbehalten

Einleitung

Zielsetzung des Handbuchs

Das vorliegende Handbuch ist eine Anleitung für Systembetreiber und Programmierer zur Integration von SIMATIC-Systemen in das GMP-Umfeld (GMP = Good Manufacturing Practice) in Bezug auf die Validierung, auch unter Berücksichtigung der besonderen Anforderungen internationaler Behörden und Organisationen, wie z. B. 21 CFR Part 11 der FDA oder EU GMP-Leitfaden Annex 11.

Zunächst beschreibt das Handbuch die Anforderungen aus pharmazeutisch regulatorischer Sicht (kurz: GMP-Sicht) an ein Computersystem, dessen Software sowie die Vorgehensweise für die Projektierung eines solchen Systems. In den weiteren Kapiteln wird der Zusammenhang zwischen den Anforderungen und der Umsetzung anhand von praktischen Beispielen erläutert.

Für Verbesserungsvorschläge nutzen Sie bitte die Kontaktdaten auf der Rückseite dieses Handbuchs.

Zielgruppen

Das Handbuch richtet sich an Anlagenbetreiber, Verantwortliche für branchenspezifische Systemkonzepte, Projektleiter und Programmierer sowie Wartungs- und Instandsetzungspersonal, die Automatisierungs- und Prozessleittechnik im GMP-Umfeld einsetzen.

Erforderliche Grundkenntnisse

Zum Verständnis dieses Handbuches sind Grundkenntnisse von SIMATIC PCS 7 erforderlich. Ebenfalls von Vorteil sind GMP-Kenntnisse aus dem Bereich der pharmazeutischen Industrie.

Gültigkeitsbereich des Handbuchs

Die in diesem Handbuch beschriebenen Informationen sind für SIMATIC PCS 7 V9.1 evaluiert. Die untersuchten Komponenten sind PCS 7 ES, PCS 7 OS und SIMATIC BATCH. Informationen bzgl. der genauen Kompatibilität zwischen den einzelnen Komponenten sind dem Produktkatalog bzw. dem Kompatibilitätstool zu entnehmen.

- Produktkatalog SIMATIC PCS 7 (https://support.industry.siemens.com/cs/de/de/view/109745632)
- Kompatibilitätstool (www.siemens.de/kompatool)

Die Kompatibilität der Add-on-Produkte zu SIMATIC PCS 7 ist direkt beim verantwortlichen Lieferanten zu erfragen.

Industry Mall Katalog- und Bestellsystem- Add-ons für SIMATIC PCS 7 (https://mall.industry.siemens.com/mall/de/de/Catalog/Products/10008888?tree=CatalogTree)

Einordnung in die Informationslandschaft

Die Systemdokumentation des Prozessleitsystems SIMATIC PCS 7 ist integraler Bestandteil der SIMATIC PCS 7 Systemsoftware. Sie steht jedem Benutzer im Plant and User Documentation Manager (PUD Manager) bzw. online als PDF zur Verfügung.

Das vorliegende Handbuch ist eine Ergänzung zu den bestehenden SIMATIC PCS 7 Handbüchern. Es dient nicht nur als Leitfaden bei der Projektierung, vielmehr gibt es einen Überblick über Voraussetzungen für die Projektierung sowie die Anforderungen an Computersysteme im GMP-Umfeld.

Aufbau des Leitfadens

Es werden Verordnungen und Richtlinien, Empfehlungen sowie notwendige Spezifikationen erläutert, die die Grundlagen für die Projektierung von Computersystemen darstellen.

Zusätzlich werden alle notwendigen Funktionen und Anforderungen an Hardware- und Softwarekomponenten beschrieben, wodurch die Auswahl an einzusetzenden Komponenten erleichtert werden soll.

Beispielhaft wird erläutert, wie Hardware und Software in Bezug auf die Anforderungen angewandt und konfiguriert bzw. programmiert werden. Darüber hinausgehende Erläuterungen können der Standarddokumentation entnommen werden.

Trainingscenter

Um Ihnen den Einstieg in SIMATIC PCS 7 zu erleichtern, bieten wir entsprechende Kurse an. Wenden Sie sich bitte an Ihr regionales Trainingscenter oder an das zentrale Trainingscenter in D 90327 Nürnberg.

Internet (http://www.sitrain.com)

Siemens im Internet

Den Wegweiser zum Angebot an technischen Dokumentationen für die einzelnen SIMATIC Produkte und Systeme finden Sie unter:

Technische Dokumentation SIMATIC PCS 7 (https://support.industry.siemens.com/cs/ww/de/view/109794065)

Den Online-Katalog und das Online-Bestellsystem finden Sie unter: (http://mall.industry.siemens.com/)

Weitere Informationen über das Angebot von Siemens für die Pharmaindustrie finden Sie hier: (http://www.siemens.com/pharma)

Technischer Support im Internet

Umfangreiche Informationen zu unserem Service und Support finden Sie hier: (http://support.industry.siemens.com/)

Der Industry Online Support bietet dort zum Beispiel:

- Handbücher und Produktinformationen
- FAQs und Anwendungsbeispiele

Des Weiteren finden Sie auf dieser Seite:

- Services in einer umfassenden Übersicht, z. B. Informationen über Vor-Ort Service, Reparaturen, Ersatzteile und vieles mehr
- ein Forum, in welchem Anwender und Spezialisten weltweit Erfahrungen austauschen
- mySupport für persönliche Filter, Benachrichtigungen, Support-Anfragen, u. a. auch den Newsletter, der Sie ständig mit den aktuellsten Informationen zu Ihren Produkten versorgt

Weitere Unterstützung

Bei Fragen zur Nutzung der im Handbuch beschriebenen Produkte, die Sie hier nicht beantwortet finden, wenden Sie sich bitte an Ihren Siemens-Ansprechpartner in den für Sie zuständigen Vertretungen und Geschäftsstellen.

Ihren persönlichen Siemens Ansprechpartner finden Sie hier: (http://www.siemens.com/automation/partner)

Bei Fragen zum Handbuch wenden Sie sich bitte an:

E-Mail: pharma@siemens.com

Inhaltsverzeichnis

Projektierung im GMP-Umfeld 1

Als Voraussetzung für die Projektierung von Computersystemen im GMP-Umfeld müssen genehmigte Spezifikationen vorliegen. Bei der Erstellung dieser Spezifikationen sowie bei der Realisierung und beim Betreiben von Computersystemen sollten Vorgaben aus Normen, Empfehlungen und Richtlinien beachtet werden. In diesem Kapitel werden die wichtigsten dieser Regelwerke sowie einige Grundgedanken daraus aufgeführt.

1.1 Verordnungen und Richtlinien

Zur Projektierung von validierungspflichtigen Computersystemen im GMP-Umfeld sollten die Verordnungen, Richtlinien und Empfehlungen verschiedener nationaler und internationaler Behörden und Organisationen beachtet werden. In Bezug auf Computersysteme sind hier insbesondere die folgenden zu nennen:

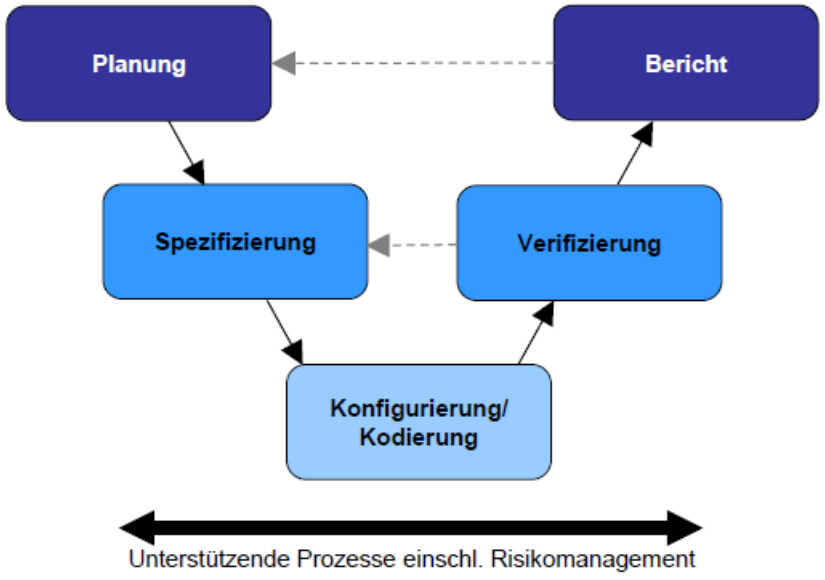
Bezeichnung (Ersteller)	Titel	Geltungsbereich
21 CFR Part 11 (US Food and Drug Administration, FDA)	Electronic Records, Electronic Signatures	Gesetz/Verordnung für Hersteller und Importeure von Arzneimitteln für den US-amerikanischen Markt
Annex 11 zum EU GMP-Leitfaden (European Commission)	Computerised Systems	Verbindliche Richtlinie innerhalb der Europäischen Union zur Umsetzung in das jeweilige nationale Recht
GAMP 5 (ISPE)	A Risk-Based Approach to Compliant GxP Computerized Systems	Leitfaden mit weltweiter Gültigkeit als Empfehlung

1.2 Lebenszyklusmodell

Zentraler Bestandteil der Good Engineering Practice (GEP) ist die Anwendung einer anerkannten Projektmethodik basierend auf einem definierten Lebenszyklus. Das Ziel liegt in der Bereitstellung einer den Anforderungen angemessenen Lösung, dem sogenannten risikobasierten Ansatz.

GAMP 5-Ansatz

Die folgende Abbildung zeigt den allgemeinen Ansatz gemäß GAMP 5 zur Entwicklung computergestützter Systeme. Es beginnt mit der Planungsphase eines Projektes und endet mit der Aufnahme der pharmazeutischen Produktion nach Abschluss der Tests und der Berichterstattung.



Quelle: Abbildung 3.3, GAMP 5 – Ein risikobasierter Ansatz für konforme GxP-computergestützte Systeme

Der hier abgebildete Lebenszyklusansatz wird in GAMP 5 als generisches Modell bezeichnet. Auf dessen Basis werden mehrere Lebenszyklusmodelle für verschieden "kritische" Systeme mit unterschiedlichen Stufen an Spezifikation und Verifizierungsphasen beispielhaft vorgestellt.

Nach Aufnahme der Produktion geht der vollständige Systemlebenszyklus bis zur Außerbetriebnahme weiter.

Siemens Validation Manual

In Anlehnung an und in Ergänzung zu den Empfehlungen des GAMP-Leitfadens hat Siemens ein "Validation Manual" erarbeitet. Dieses dient den internen Projektteams mit allgemeinen Hinweisen und konkreten Templates (Dokumenten-Vorlagen) als Hilfe bei der Festlegung der Validierungsstrategie für ein Projekt. Sowohl für die Projektplanung als auch für die Systemspezifikation und die Testdokumentation existieren Vorlagen für die entsprechenden Dokumente. Im Gegensatz zu dem hier vorliegenden GMP-Handbuch ist das Siemens Validation Manual nur für Siemens-internen Gebrauch verfügbar.

1.3 Verantwortlichkeiten

Beim Projektieren von Computersystemen im GMP-Umfeld und der Erstellung der entsprechenden Spezifikationen sind die Verantwortlichkeiten für die Aktivitäten der einzelnen Lebenszyklusphasen festzulegen. Da diese Festlegung meist kunden- und projektspezifisch erfolgt und der vertraglichen Vereinbarung bedarf, wird deren Festlegung im Qualitäts- und Projektplan empfohlen.

Siehe auch

- GAMP 5-Leitfaden, Anhang M6 "Lieferanten-Qualitäts- und Projektplanung"

1.4 Genehmigung und Änderungsverfahren

Bei der Errichtung neuer validierungspflichtiger Systeme oder der Änderung von in Betrieb befindlichen validierungspflichtigen Systemen gilt die oberste Priorität der Erreichung bzw. dem Erhalt des validierten Zustands, das heißt der Sicherstellung der Nachvollziehbarkeit der durchgeführten Schritte.

Vor der Errichtung oder Änderung eines Systems ist es daher erforderlich, die anstehenden Schritte funktional und zeitlich zu planen, zu dokumentieren und vom Kunden bzw. Anlagenbetreiber genehmigen zu lassen.

1.5 Risikobasierte Vorgehensweise

Sowohl die US-amerikanische Behörde FDA ("Pharmaceutical cGMPs for the 21st Century Initiative", 2004) als auch der Industrieverband ISPE/GAMP (Leitfaden "GAMP 5", 2008) empfehlen einen risikobasierten Ansatz bei der Validierung von Systemen. Das bedeutet, ob und mit welchem Aufwand ein System validiert wird, sollte abhängig von seiner Komplexität und seinem Einfluss auf die Produktqualität festgelegt werden.

Anforderungen an Computersysteme im GMP-Umfeld

2

In Bezug auf den Einsatz von Computersystemen sind in diesem Kapitel die wesentlichen Anforderungen aufgeführt, die ein automatisiertes System im GMP-Umfeld erfüllen muss. Diese Anforderungen sind in der Spezifikation festzuhalten und während der Projektierung umzusetzen. Bei späteren Änderungen oder Eingriffen ins System muss zu jeder Zeit der sichere Nachweis erbracht werden, wer, zu welchem Zeitpunkt, was geändert bzw. durchgeführt hat. Die Anforderungen an diese Aufgabe werden in verschiedenen Funktionen umgesetzt und sind in den nachfolgenden Kapiteln beschrieben.

Hinweis

In diesem Kapitel sind die Anforderungen an Computersysteme allgemein beschrieben. Die systemspezifische Erfüllung folgt ab dem Kapitel "Systemspezifikation (Seite 25)".

2.1 Kategorisierung von Hardware und Software

Hardware(HW)-Kategorisierung

Nach dem GAMP 5-Leitfaden werden Hardwarekomponenten eines Systems in zwei Kategorien unterschieden, in sog. "Standard-Hardwarekomponenten" (Kategorie 1) und "kundenspezifisch erstellte Hardwarekomponenten" (Kategorie 2).

Software(SW)-Kategorisierung

Nach dem GAMP 5-Leitfaden werden die Softwarekomponenten eines Systems in verschiedene Software-Kategorien eingestuft. Dies reicht von kommerziell verfügbaren und vorkonfigurierten "Standard"-Softwareprodukten, die lediglich installiert werden, über konfigurierte Softwareprodukte bis hin zu kundenspezifischen Applikationen ("programmierte Software").

2.2 Testaufwand abhängig von der Kategorisierung

Der Aufwand für die Validierung (Spezifizieren und Testen) ist beim Einsatz von konfigurierten und insbesondere bei kundenspezifisch zugeschnittenen Produkten wesentlich höher als bei Standard-Produkten (HW und/oder SW). Der Gesamtaufwand der Validierung kann somit durch möglichst umfangreichen Einsatz von Standardprodukten deutlich reduziert werden.

2.3 Änderungs- und Konfigurationsmanagement

Alle kontrollierten Elemente eines Systems sollten durch Name und Version gekennzeichnet und Änderungen daran kontrolliert werden. Der Übergang von der Projektphase in das entsprechende betriebliche Verfahren sollte frühzeitig festgelegt werden.

Das Verfahren beinhaltet z. B.

- Identifikation der betroffenen Elemente
- Kennzeichnung der Elemente durch Namen und Versionsnummer
- Änderungslenkung
- Kontrolle der Konfiguration (Speicherung, Freigabe, etc.)
- Periodische Prüfungen der Konfiguration

Siehe auch

- GAMP 5-Leitfaden,
  Anhang M8 "Projekt-Änderungs- und Konfigurationsmanagement"

2.4 Software-Erstellung

Im Rahmen der Software-Erstellung sollten Richtlinien eingehalten werden, die im Qualitäts- und Projektplan zu dokumentieren sind (im Sinne der Good Engineering Practice, kurz GEP). Richtlinien zur Software-Erstellung können den GAMP-Leitfäden und einschlägigen Normen und Empfehlungen entnommen werden.

Verwendung von Typ-Instanz-Konzepten und Kopiervorlagen

Während sich der Validierungsaufwand bei "Standard"-Softwareprodukten auf die Überprüfung von Software-Namen und Version beschränkt, beläuft sich der Aufwand für die Validierung von kundenspezifischer Software auf die Überprüfung des kompletten Funktionsumfanges sowie ein mögliches Lieferantenaudit.

Um den Validierungsaufwand so gering wie möglich zu halten, sind aus diesem Grund bei der Projektierung standardisierte Bausteine zu bevorzugen (Produkte, Hausstandards, Projektstandards). Daraus werden kundenspezifische Typen und Vorlagen nach den Designvorgaben erstellt und getestet.

Kennung von Software-Modulen / Typen / Kopiervorlagen

Bei der Software-Erstellung sollten die einzelnen Software-Module eindeutig mit Name, Version und einer Kurzbeschreibung des entsprechenden Bausteins versehen werden.

Änderung von Software-Modulen / Typen / Kopiervorlagen

Änderungen an Software-Modulen sollten entsprechend dokumentiert werden. Neben der Erhöhung der Versionskennung sollten auch das Datum und der Name des Ändernden aufgenommen werden, ggf. mit Verweis auf den zugehörigen Änderungsantrag / -auftrag.

2.5 Zugriffskontrolle und Benutzerverwaltung

Um die Sicherheit von Computersystemen im GMP-Umfeld gewährleisten zu können, sollten diese Systeme mit einem Zugriffskontrollsystem ausgestattet sein. Zugriffskontrollsysteme bieten zusätzlich zur räumlichen Zugangskontrolle die Möglichkeit, Computersysteme vor unberechtigtem Zugriff zu schützen. Die Benutzer sollten hierbei in Benutzergruppen zusammengefasst werden, über die die Verwaltung der Benutzerrechte erfolgt. Die Zugriffsberechtigung der einzelnen Benutzer kann über verschiedene Möglichkeiten realisiert werden:

- Kombination aus eindeutiger Benutzerkennung und Passwort, siehe auch Kapitel "Anforderungen an Benutzerkennung und Passwort (Seite 19)"
- RFID-/Chipkarte gemeinsam mit Passwort
- Auswertung biometrischer Merkmale, z. B. Fingerabdruckscanner

2.5.1 Anwendung der Zugriffskontrolle auf ein System

Generell sollten Aktionen, die an einem Computersystem ausgeführt werden können, vor unberechtigtem Zugriff geschützt werden. Je nach Aufgabenbereich können dem Benutzer verschiedene Rechte zugewiesen werden. Der Zugriff auf die Benutzeradministration sollte nur dem Systemeigner bzw. einem von ihm bestimmten, eng begrenzten Mitarbeiterkreis gewährt werden. Weiterhin ist der Zugriff Unberechtigter auf die elektronisch aufgezeichneten Daten unbedingt zu verhindern.

Die Verwendung einer automatischen Logout-Funktion ist empfehlenswert und stellt eine zusätzliche Zugriffssicherheit dar. Sie ersetzt jedoch nicht die allgemeine Verpflichtung des Benutzers zur Abmeldung beim Verlassen des Systems. Die automatische Logout-Zeit sollte in Abstimmung mit dem Betreiber in der Spezifikation definiert werden.

Hinweis

Sowohl der Zugang zu PCs als auch der Zugriff auf das System insgesamt darf nur für berechtigte Personen möglich sein. Dies kann durch geeignete Mechanismen wie mechanisches Abschließen sowie durch die Nutzung von Hard- und Software für den Fernzugriff unterstützt werden.

2.5.2 Anforderungen an Benutzerkennung und Passwort

Benutzerkennung:

Die Benutzerkennung eines Systems sollte eine durch den Kunden festgelegte Mindestlänge besitzen und innerhalb des Systems eindeutig sein.

Passwort:

Beim Anlegen von Passwörtern sollte eine Mindestanzahl von Zeichen sowie ein Zeitraum bis zum Ablaufen eines Passwortes festgelegt werden. Ein Passwort sollte generell aus einer

Kombination von Zeichen bestehen, die neben der Mindestlänge mindestens drei der nachfolgend aufgeführten Kriterien erfüllt.

- Verwendung von Großbuchstaben
- Verwendung von Kleinbuchstaben
- Verwendung von Ziffern (0-9)
- Verwendung von Sonderzeichen

Siehe auch

- Kapitel "Einrichten der Benutzerverwaltung (Seite 43)"

2.6 Anforderungen an elektronische Aufzeichnungen

Bei der Nutzung von elektronischen Aufzeichnungen für relevante Daten gelten außerdem die folgenden Anforderungen:

- Das System muss validiert sein.
- Die Eingabe oder Änderung von Daten darf nur autorisierten Personen möglich sein (Zugriffskontrolle).
- Die Änderung oder Löschung von Daten ist aufzuzeichnen (Audit Trail).
- Aufzubewahrende elektronische Aufzeichnungen sind durch geeignete Maßnahmen langfristig zu sichern und verfügbar zu halten.
- Durch Regulationen geforderte Namenszeichen und Unterschriften sind als elektronische Unterschriften zu implementieren.
- "Relevante" Verarbeitungsschritte/-vorgänge, "wichtige" Zwischenstufen sowie "wichtige" Ausrüstung sind vorher durch den pharmazeutisch Verantwortlichen zu definieren. Diese Definition ist häufig prozessspezifisch.
- Im Falle eines elektronischen Herstellprotokolls müssen dessen Aufbau und Inhalt zusätzlich mit Aufbau und Inhalt der Herstellanweisung übereinstimmen. Alternativ können Herstellanweisung und -protokoll auch in einem Dokument zusammengefasst werden.

Siehe auch

- EU GMP-Leitfaden Kapitel 4.9 sowie Annex 11
- 21 CFR Part 11 "Electronic Records, Electronic Signatures", US FDA

2.7 Elektronische Unterschriften

Elektronische Unterschriften sind computergenerierte Zeichenfolgen, die als rechtlich verbindliches Äquivalent zur handschriftlichen Unterschrift gelten.

Die Vorschriften zum Einsatz von elektronischen Unterschriften sind z. B. in 21 CFR Part 11 der US FDA bzw. im EU GMP-Leitfaden Annex 11 festgehalten.

Praxisrelevant sind elektronische Unterschriften z. B. für manuelle Dateneingaben und Bedieneingriffe zur Laufzeit, Freigabe von Verfahrensschritten und Datenreports sowie bei der Änderung von Rezepten.

Jede elektronische Unterschrift muss einer Person eindeutig zugeordnet sein und darf von keiner anderen Person verwendet werden.

Hinweis

Bei der Herstellung von Arzneimitteln und Medizingeräten, die auf den US-amerikanischen Markt gelangen, müssen die Vorschriften der FDA erfüllt werden. Bezüglich elektronischer Unterschriften ist dies der 21 CFR Part 11.

Konventionelle elektronische Unterschriften

Werden elektronische Unterschriften eingesetzt, die nicht auf Biometrie basieren, so sind diese so anzulegen, dass sich der Unterschreibende über mindestens zwei Identifikationskomponenten identifizieren muss. Dies gilt ebenfalls in all den Fällen, in denen eine Chipkarte eine der beiden Identifikationskomponenten ersetzt.

Diese Identifikationskomponenten können z. B. aus einer Benutzerkennung und einem Passwort bestehen. Die Identifikationskomponenten sind eindeutig zu vergeben und dürfen nur vom eigentlichen Benutzer verwendet werden.

Elektronische Unterschriften auf biometrischer Basis

Eine auf Biometrie basierende elektronische Unterschrift muss so angelegt sein, dass sie nur von einem Benutzer verwendet werden kann. Wendet der Unterschreibende die elektronische Unterschrift auf biometrischer Basis an, so reicht eine Identifikationskomponente aus.

Biometrische Erkennungsmerkmale sind z. B. Fingerabdrücke, Iris-Struktur, etc.

2.8 Audit Trail

Der Audit Trail ist ein systemseitiger Kontrollmechanismus, der die Nachvollziehbarkeit von Dateneingaben bzw. Datenänderungen durch den Bediener sicherstellt. Ein sicherer Audit Trail ist besonders in Zusammenhang mit der Erstellung, Änderung oder Löschung von GMP-relevanten Datenaufzeichnungen (Electronic Records) erforderlich.

Ein solcher Audit Trail muss die im "normalen Betrieb" vorgenommenen Änderungen an GMP-relevanten Werten mit Datum und Uhrzeit dokumentieren. Der Audit Trail beinhaltet Wer, hat Wann, Was geändert (Altwert / Neuwert), optional auch das "Warum".

2.9 Protokollierung von Chargendaten

Bei der Herstellung von Arzneimitteln und Medizingeräten kommt der Chargendokumentation besondere Bedeutung zu. Für den pharmazeutischen Hersteller stellt die ordnungsgemäß erstellte Chargendokumentation im Rahmen der Produkthaftung oftmals die einzige dokumentierte Basis für eine Beweisführung dar.

Bestandteile der Chargendokumentation sind:

- Herstellanweisung und Herstellprotokoll
- Verpackungsanweisung und Verpackungsprotokoll (die Verpackung des fertigen Arzneimittels ist aus pharmazeutischer Sicht Teil des Herstellprozesses)
- Prüfanweisung und Prüfprotokoll (hinsichtlich aller Qualitätsprüfungen, z. B. in der Analytik)

Zentrale Bedeutung kommt hierbei dem Begriff des Herstell- bzw. Verpackungsprotokolls zu, welcher wie folgt definiert ist:

- Das Herstellprotokoll ist immer produkt- und chargenbezogen,
- basiert immer auf den entsprechenden Teilen der gültigen Herstellanweisung,
- beinhaltet alle prozessrelevanten Mess-, Regel- und Steuervorgänge als Ist-Werte
- sowie Abweichungen von den festgelegten Soll-Werten.

2.10 Archivierung von Daten

Unter (elektronischer) Archivierung versteht man die dauerhafte Aufbewahrung elektronischer Daten und Aufzeichnungen in einem Langzeitspeicher.

Der Kunde ist verantwortlich für die Definition von Verfahren und Kontrollen zur Aufbewahrung elektronischer Daten.

Basierend auf gesetzlichen Bestimmungen (EU-GMP-Leitfaden, 21 CFR Part 210/211, etc.) muss entschieden werden, wie elektronische Daten aufbewahrt werden und vor allem welche Daten hiervon betroffen sind. Dieser Entscheidung sollte eine begründete und dokumentierte Risikobetrachtung zugrunde liegen, die auch die Aussagekraft der elektronischen Daten über den zu archivierenden Zeitraum berücksichtigt.

Für den Fall einer Migration oder Konvertierung der archivierten Daten muss die Integrität der Daten über den gesamten Konvertierungsprozess gewährleistet sein.

Siehe auch

- GAMP 5-Leitfaden, Anhang O9 "Sicherung und Wiedereinspielung"

2.11 Datensicherung (Backup)

Im Unterschied zur Archivierung elektronischer Daten dienen Datensicherungen der Erstellung von Sicherungskopien, welche die Wiederherstellung des Systems im Falle eines Verlusts der Originaldaten oder eines Systemausfalls sicherstellen.

Das Sicherungsverfahren muss die periodische Sicherung von nicht beständiger Information abdecken, um den Totalverlust der Daten durch Defekt von Systemkomponenten oder versehentliches Löschen der Daten zu vermeiden. Sicherungsverfahren müssen geprüft werden, um die ordnungsgemäße Speicherung der Daten sicherzustellen. Sicherungskopien sollten klar und verständlich bezeichnet und mit Datum versehen werden.

Datensicherungen werden auf externen Datenträgern erstellt. Hierbei sollten Datenträger verwendet werden, die den Empfehlungen der Gerätehersteller entsprechen.

Bei der Sicherung von elektronischen Daten wird unterschieden in

- Sicherung der Installation, z. B. Partitionsimage
- Sicherung der Applikation
- Sicherung von Archivdaten wie z. B. Prozessdaten

Ein besonderes Augenmerk liegt hierbei auch auf der Aufbewahrung von Datensicherungsmedien (räumliche Trennung der Kopie vom Original, Schutz vor Magnetfeldern und Elementarschäden).

Siehe auch

- GAMP 5-Leitfaden, Anhang O9 "Sicherung und Wiedereinspielung"

2.12 Rücklesen von ausgelagerten Daten

Es muss gewährleistet werden, dass die archivierten/gesicherten Daten zu jedem Zeitpunkt rücklesbar sind. Für den Fall einer Systemaktualisierung/Migration ist auf eine Kompatibilität der vor der Aktualisierung ausgelagerten Daten zu achten. Falls erforderlich müssen die ausgelagerten Daten ebenfalls migriert werden.

Siehe auch

- GAMP 5-Leitfaden, Anhang O13 "Archivierung und Rückspielung"
- GAMP 5-Leitfaden, Anhang D7 "Datenmigration"

2.13 Uhrzeitsynchronisation

Innerhalb eines Systems muss eine einheitliche Zeitreferenz (inklusive einer Zeitzonenreferenz) gewährleistet sein, um die Archivierung von Meldungen, Alarmen etc. mit eindeutigen Zeitstempeln versehen zu können.

Besonders wichtig ist die Zeitsynchronisierung bei der Archivierung von Daten und der Analyse von Störungen einer Anlage. Als Zeitbasis für die Speicherung von Daten wird UTC (Universal Time Coordinated, siehe auch ISO 8601) empfohlen. Der Zeitstempel von Meldungen und Werten kann in lokaler Zeit mit dem Hinweis auf Sommer- / Winterzeit dargestellt werden.

2.14 Einsatz von Fremdkomponenten

Bei dem Einsatz von Fremdkomponenten (Hardware und Software) muss die Kompatibilität mit den eingesetzten Komponenten bestätigt werden. Im Falle von projektspezifisch "zugeschnittenen" (customized) Komponenten sollte ein Lieferantenaudit erwogen werden, um den Lieferanten und dessen Qualitätsmanagementsystem zu überprüfen.

Siehe auch

- GAMP 5-Leitfaden, Anhang M2 "Lieferantenbewertung"

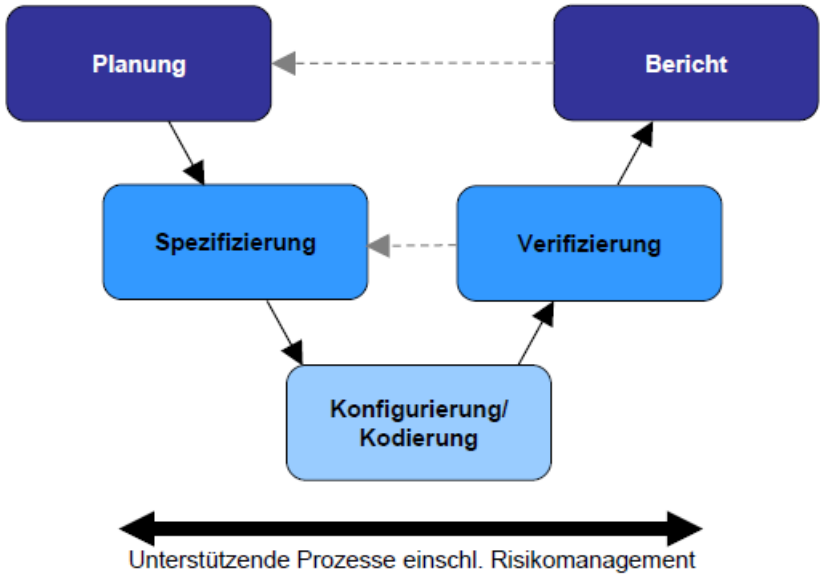
Systemspezifikation

3

In der Spezifikationsphase eines Computersystems werden das zu errichtende System und dessen Funktionalität definiert, und zwar so detailliert wie es zur Umsetzung erforderlich ist.

Spezifikationen stellen nicht nur die Basis zu einer strukturierten und nachvollziehbaren Projektierung dar, sondern sind gerade im GMP-Umfeld eine unabdingbare Voraussetzung als Referenz für die abschließende Verifizierung des Systems.

Zur Spezifikation gehören sowohl die Auswahl der Produkte, Produktvarianten, Optionen und Systemkonstellationen als auch die Applikationssoftware.



Quelle: Abbildung 3.3, GAMP 5 – Ein risikobasierter Ansatz für konforme GxP-computergestützte Systeme

Die Spezifikation insgesamt kann z. B. aufgeteilt werden in:

- Funktionsspezifikation (FS) als Antwort auf Kundenanforderungen (URS)
- Konfiguration und Design allgemein (Systementwurf, allgemeine Themen)
- Hardware (und Netzwerk) Design Spezifikation (HDS)
- Software Design Spezifikation (SDS)
- HMI Spezifikation

Eine sehr gute Übersicht über das PCS 7 Portfolio sowie zur optimierten Abwicklung von Projekten von der Planung über die Umsetzung und den Test bis hin zur Übergabe an den Kunden bietet auch der folgende Artikel. Dieser ist allerdings nur Siemens-intern verfügbar.

- Multimediales Vorführsystem "Fast Track Engineering", Online-Support unter Beitrags-ID 60242433 (https://support.industry.siemens.com/cs/ww/de/view/60242433)

3.1 Auswahl und Spezifikation der Hardware

Sowohl für die Automatisierung als auch für die Bedienung und Beobachtung einfacher sowie komplexerer Produktionsprozesse und Fertigungsabläufe kommen verschiedene Systemausprägungen zum Einsatz.

Die Auswahl von Hardwarekomponenten sollte an den Anforderungen gemessen werden. Diese Anforderungen können funktionaler Art sein, aber auch Aspekte wie örtliche Gegebenheiten, kompatible Software oder Datensicherheit beinhalten.

3.1.1 Hardware-Spezifikation

Die Hardware Design Spezifikation (kurz: HDS) beschreibt die Architektur und Konfiguration der Hardware inkl. der Netzwerke. Hierbei sollten z. B. die nachfolgenden Punkte definiert werden. Dies dient später als Prüfgrundlage für die Verifizierung.

- Hardware-Übersichtsplan, Systemaufbau und -organisation
- Schaltschränke (Schaltschranknamen, UPS Konfiguration, Standort), PC-Stationen Schaltschränke, Automatisierungssystem mit CPUs, E/A-Karten, etc.
- PC-Komponenten für Server und Client
- Installationsprozeduren und Anleitungen für Server, Clients, ES
- Sinnvolle Aufteilung der Anlagen- und Teilanlagenbereiche zu den AS
- Netzwerkstruktur Industrial Ethernet, z. B. Switches, Übertragungstechnik (elektrisch, optisch, drahtlos), Namen und Ethernet Konfiguration der Teilnehmer (AS, PC-Stationen etc.), allgemeine Netzwerkeinstellungen
- Profibus-/Profinet-Installation, Aufteilung der Netzwerke zu den ASen und spezifische Profibus-/Profinet-Einstellungen
- Zeitsynchronisation, sofern Hardware-Komponenten beteiligt
- Barcodescanner Konfiguration
- Feldgeräte

Die HDS kann Bestandteil einer Gesamtspezifikation sein oder aber in einem separaten Dokument erfolgen.

Hinweis

Die Vorgaben im Hardware-Übersichtsplan sowie die Benennung von Hardwarekomponenten müssen eineindeutig sein.

Siehe auch

- GAMP 5-Leitfaden, Anhang D3 "Konfigurierung und Entwurf"

3.1.2 Auswahl der Hardware-Komponenten

Durch den Einsatz von Hardwarekomponenten aus dem PCS 7 Katalog wird die Verfügbarkeit von Hardware und Ersatzteilen auf lange Zeit sichergestellt.

Aus Gründen der Systemverfügbarkeit und der Datensicherheit sollten bei der Systemauslegung RAID-Systeme einer geeigneten Klasse für PC-Komponenten wie ES, OS-Einzelplatzstation, OS-Server und BATCH-Server eingesetzt werden.

Mit der Auslieferung eines **SIMATIC PCS 7 Bundles** erhält man einen PC mit vollständig installierter Software für die jeweiligen Anwendungen. Die darin enthaltenen Komponenten sind nicht immer identisch mit der auf dem Markt erhältlichen gleichnamigen Ware. Demzufolge unterscheidet sich auch die Lieferbarkeit von kompatiblen Ersatzteilen.

Auch bei virtuellen Systemen sollte auf entsprechend bewährte Komponenten zurückgegriffen werden, wie z. B. ESXi Server.

Hinweis

Es sollte nur Hardware aus dem aktuellen PCS 7 Katalog verwendet werden. Bei nicht freigegebenen Konstellationen ist erhöhter Aufwand für Spezifikation und Testphase erforderlich, siehe Produktkatalog (https://support.industry.siemens.com/cs/de/de/view/109745632).

Bei der Auslagerung von PCs in Schaltschränke ist darauf zu achten, dass entsprechende Hardwarekomponenten wie z. B. Bedienkanalverlängerungen eingeplant werden.

Bei den Automatisierungssystemen unterscheidet man die Ausführungen

- **Standard Automatisierungssystem**
- **Hochverfügbares Automatisierungssystem**
  Das geladene Anwenderprogramm ist in beiden CPUs vollkommen identisch und wird von beiden CPUs synchron abgearbeitet. Die Umschaltung hat keine Rückwirkung auf den laufenden Prozess, da sie stoßfrei verläuft.
- **Fehlersicheres Automatisierungssystem**
  Die Anlage wird im Fehlerfall automatisch in einen sicheren Zustand gebracht. Bei Projektierung, Inbetriebnahme und Betrieb fehlersicherer Anlagen sind entsprechende nationale Vorschriften zu beachten. S7 F-Systeme stellen eine Referenzsumme über den fehlersicheren Programmteil zur Verfügung; diese Summe wird aufgenommen und ermöglicht die Erkennung von Änderungen im fehlersicheren Programm.

Siehe auch

- Handbuch "PCS 7 PC-Konfiguration", Online-Support unter Beitrags-ID 109794377 (https://support.industry.siemens.com/cs/ww/de/view/109794377)

3.1.3 CPU 410 für Prozessautomatisierung

Die "CPU 410-5H Process Automation" ist speziell für das SIMATIC PCS 7 Leitsystem konzipiert. Wie auch die bisherigen Controller des SIMATIC PCS 7 Systems ist die CPU 410-5H Process Automation in allen Branchen der Prozessautomatisierung einsetzbar. Die besonders flexible Skalierbarkeit, basierend auf den PCS 7 Prozessobjekten, ermöglicht es, den gesamten Leistungsbereich, vom kleinsten bis zum größten Controller, in Standard, hochverfügbaren oder fehlersicheren Anwendungen mit nur einer Hardware abzudecken.

Dies bedeutet die folgenden Vorteile:

- Reduzierte Anzahl von CPU-Varianten, keine Speicherkarten
- dadurch weniger Ersatzteile
- Einfache System- und Funktionalitätserweiterung
- Flexibler Einsatzbereich, erhöhte Robustheit

Siehe auch

- Handbuch „PCS 7 CPU 410 Process Automation“, Online-Support unter Beitrags-ID 109801828 (https://support.industry.siemens.com/cs/ww/de/view/109801828)

3.1.4 Hardwarelösungen für spezielle Automatisierungsaufgaben

Zur Anbindung von Hardwarekomponenten, die nicht im SIMATIC Hardwaremanager vorhanden sind, werden zusätzlich gerätespezifische Lösungen benötigt. Diese Komponenten sind über eigene Geräte-Stammdaten (GSD) anzubinden. Beispiele für die Anbindung solcher Hardwarekomponenten sind:

- Anbindung von Wägebaugruppen (SIWAREX)
- Anbindung von Frequenzumrichtern für Antriebe (Masterdrives, Micromaster)
- Anbindung von betreiberspezifischen Feldgeräten

Durch die Verwendung von Hardwarekomponenten aus dem PCS 7 Add-on-Katalog (ST PCS 7 AO) kann der Validierungsaufwand reduziert werden.

3.2 Sicherheit des Anlagennetzwerks

Bei modernen Prozessleitsystemen verschwinden mehr und mehr die Grenzen zwischen der Office- und der Automatisierungswelt. Automatisierungslösungen mit angebundenen Web Clients, MES-Applikationen und kundenspezifischen Büronetzwerken und Applikationen gewinnen mehr und mehr an Bedeutung. Um diesen Anforderungen gerecht zu werden und stets eine möglichst hohe Datensicherheit zu gewährleisten, sind die Planung und der Aufbau von vernetzten PCS 7-Automatisierungslösungen von großer Bedeutung.

Maßnahmen zur Erhöhung der Daten- und Anlagensicherheit

SIMATIC bietet mehrere Möglichkeiten, die Daten- und Informationssicherheit und damit die Sicherheit einer Produktionsanlage zu erhöhen. Dazu gehören:

- Gestaffeltes User-, Gruppen- und Rollenkonzept
- Sicherheitskonzepte bezüglich Netzwerksicherheit sowie beschränkter Zugriff auf Netzlaufwerke
- SIMATIC Security Control (SSC)
- SCALANCE-S Firewall- und VPN-Module

Weitere Hinweise siehe auch

- Kapitel "Informationssicherheit und Datenintegrität (Seite 55)"
- "Industrial Security", Online-Support unter Beitrags-ID 50203404 (https://support.industry.siemens.com/cs/ww/de/view/50203404)
- Handbuch "Sicherheitskonzept PCS 7 und WinCC", Online-Support unter Beitrags-ID 109780811 (https://support.industry.siemens.com/cs/ww/de/view/109780811)
- Handbuch "PCS 7 Kompendium Teil F – Industrial Security", Online-Support unter Beitrags-ID 109804118 (https://support.industry.siemens.com/cs/ww/de/view/109804118)

3.3 Spezifikation der Basissoftware

Die Software Design Spezifikation (SDS) beschreibt die Architektur und Konfiguration der Software. Hierzu gehört neben der Applikationssoftware auch die Definition der im System eingesetzten "Standard"-Softwarekomponenten, z. B. durch Angabe von Bezeichnung, Versionsnummer, etc. Diese Beschreibung dient als Referenz bei den späteren Tests (FAT, SAT, etc.).

Zu den Komponenten an kommerziell erhältlicher Standardsoftware gehören die Komponenten der Automatisierungssoftware und auch Software von Drittanbietern, siehe auch Kapitel "Verifizierung von Software (Seite 144)".

Hardware- und Software-Voraussetzungen sowie Betriebssystemauswahl

- Kompatibilitätstool (www.siemens.de/kompatool)
- PCS 7 Toolset-DVD, Liesmich-Datei
- Handbuch "PCS 7 PC-Konfiguration", Online-Support unter Beitrags-ID 109794377 (https://support.industry.siemens.com/cs/ww/de/view/109794377)
- Verträglichkeit von Microsoft Updates, Online-Support unter Beitrags-ID 18490004 (https://support.industry.siemens.com/cs/ww/de/view/18490004)

3.3.1 Betriebssystem

Informationen zur Freigabe der SIMATIC Produkte mit verschiedenen Betriebssystemen (32-bit und 64-bit) sind enthalten in:

- Produktkatalog SIMATIC PCS 7 (https://support.industry.siemens.com/cs/de/de/view/109745632)
- Kompatibilitätstool (www.siemens.de/kompatool)
- Online-Hilfe, Liesmich-Datei

Die von Microsoft bereitgestellten Sicherheitsupdates und "Wichtige Updates" für das Windows-Betriebssystem werden von Siemens auf Kompatibilität zur SIMATIC Software geprüft und freigegeben, siehe Hinweis unter Kapitel "Aktualisierung der Systemsoftware (Seite 176)".

3.3.2 Basissoftware Benutzerverwaltung

Eine wesentliche Anforderung insbesondere im GMP-Umfeld ist die Zugriffskontrolle auf das System; nur so kann ein sicherer und vorschriftskonformer Betrieb gewährleistet werden (21 CFR Part 11 und EU GMP-Leitfaden Annex 11). Der unerlaubte Zugriff sowohl auf das Bedien- und Beobachtungssystem als auch auf das Dateisystem und die Verzeichnisstrukturen im Betriebssystem muss vermieden werden. Dazu bedarf es einer entsprechenden Planung:

- Definition der Benutzergruppen mit unterschiedlichen Berechtigungsstufen für Bedienung und Wartung
- Definition der Benutzer und Zuordnung zu den Benutzergruppen
- Festlegen einer angepassten Anlagenstruktur und Laufwerksablage inklusive Berechtigungen

Die Zugriffskontrolle zu den SIMATIC PCS 7 Systemkomponenten wird mittels SIMATIC Logon realisiert. Weitere Informationen zu Installation und Konfiguration der verschiedenen Komponenten von SIMATIC Logon enthält das Kapitel "Einrichten der Benutzerverwaltung (Seite 43)" sowie das Projektierungshandbuch SIMATIC Logon.

3.3.3 Softwarekomponenten Engineering

Einige der wichtigsten Funktionen der SIMATIC PCS 7 Engineering Software sind nachfolgend beschrieben.

Siehe auch

- Handbuch "PCS 7 Engineering System", Kapitel 8.7, Online-Support unter Beitrags-ID 109800500 (https://support.industry.siemens.com/cs/ww/de/view/109800500)

Multiprojekt-Engineering

Das Einrichten und Nutzen von Multiprojekten ist in Kapitel "Projekteinrichtung (Seite 59)" dieses Handbuchs beschrieben.

Leittechnische Bibliotheken

Die leittechnischen Bibliotheken umfassen vorgefertigte und getestete Objekte (Bausteine, Bildbausteine und Symbole). Das Projektieren beschränkt sich beim Einsatz dieser Bibliotheken in der Regel auf die Konfiguration der entsprechenden Objekte. Ein entscheidender Vorteil des Einsatzes von vorgefertigten Objekten beim Projektieren von automatisierten Systemen ist die niedrigere Software-Kategorie (siehe Kapitel "Software-Kategorisierung gemäß GAMP 5-Leitfaden (Seite 144)") und die Update-Fähigkeit. Damit verbunden ist ein geringerer Validierungsaufwand gegenüber anwenderspezifischen Bausteinen.

WinCC Configuration Studio

Das WinCC Configuration Studio bietet eine übersichtliche Projektierung von Massendaten für OS-Projekte. Die Benutzeroberfläche gliedert sich in einen Navigationsbereich und einen an Microsoft Excel angelehnten Datenbereich.

Das WinCC Configuration Studio beinhaltet u. a. folgende Editoren und Funktionen:

- Variablenhaushalt
- Alarm Logging
- Tag Logging
- User Archive
- User Administrator

CFC (Continuous Function Chart)

Der CFC-Editor bietet eine grafische Oberfläche zur Projektierung der Automatisierungs- und Steuerungsfunktionen. Die Funktionsbausteine werden aus Bibliotheken in einem CFC-Plan per Drag&Drop platziert und entsprechend den Anforderungen verschaltet und parametriert.

SFC (Sequential Function Chart)

Der SFC-Editor ermöglicht die grafische Projektierung und Inbetriebnahme von Ablaufsteuerungen. Wesentliche Bestandteile dabei sind Schritte und Transitionen sowie Parallel- und Alternativverzweigungen.

Import-Export-Assistent (IEA)

Der Import-Export-Assistent ist ein Werkzeug zum Projektieren von Systemen mit wiederkehrenden Funktionen und/oder Anlagenteilen. Zur Projektierung werden bereits in der Planungsphase erstellte Messstellenlisten oder CAD-Pläne zur weitgehend automatischen Erstellung von CFC-Plänen für Messstellen genutzt. Hierbei werden Ableger von Musterlösungen erzeugt und anschließend mit spezifischen Daten versorgt, siehe Kapitel "Massendatenbearbeitung (Bulk Engineering) (Seite 92)".

Plant Automation Accelerator (PAA)

Durch die Objektorientierung und sein durchgängiges Typ-Instanz-Konzept zu SIMATIC PCS 7 ermöglicht der PAA ein optimiertes Bulk Engineering. Dadurch wird das Fehlerrisiko minimiert. Mittels Control Module Types (CMTs) werden Vorlagen angelegt, aus denen die Instanzen generiert werden. Die Instanzen sind mit der Vorlage verbunden und können nach einer Änderung der Vorlage aktualisiert werden.

Weitere Hinweise zur Konfiguration und vorteilhaften Nutzung des PAA enthält das Kapitel "Typ-Instanz-Konzept mit dem PAA (Seite 94)".

Bausteinschutz

Bausteine können vor Veränderungen und Einsicht geschützt werden, so dass nur noch die Ein- und Ausgänge zugänglich sind. "S7-Block Privacy" (ab PCS 7 V8.0) bietet eine höhere Sicherheit als der bisherige KNOW-HOW Schutz und sollte deshalb besonders für sensible Bereiche bevorzugt verwendet werden, siehe Kapitel "Schreibschutz von CFC/SFC-Plänen und SFC-Typen (Seite 160)" zum Schreibschutz und Kapitel "Bausteinverschlüsselung mit "S7-Block Privacy" (Seite 162)" zur Bausteinverschlüsselung.

Hinweis

Um mit "S7-Block Privacy" verschlüsselte Bausteine bearbeiten zu können, muss die AS mindestens eine CPU 4xx ab Firmwarestand V6.0 sein.

Version Trail

SIMATIC PCS 7 Version Trail erlaubt die Sicherung von Multiprojekten, Einzelprojekten und projektspezifischen Bibliotheken in Zusammenhang mit einer eindeutigen Versionskennzeichnung der archivierten Projekte.

Weiterhin ist es möglich, Multiprojekte, Projekte und Bibliotheken zu definierten Zeiten automatisch und versioniert zu sichern und Bausteinparameter zeitgesteuert zurück zu lesen.

Weitere Hinweise zu Konfiguration und Nutzung von "Version Trail" enthält das Kapitel "Versionieren von Projekten mit Version Trail (Seite 153)".

SIMATIC BATCH

SIMATIC BATCH ist ein Programmpaket von SIMATIC PCS 7, mit dem diskontinuierliche Prozesse, sogenannte Chargenprozesse, geplant, gesteuert und protokolliert werden können. Es kann als Einzelplatzsystem oder als Client-Server-System eingesetzt werden und lässt sich durch die modulare Architektur und die Skalierbarkeit in unterschiedlichen Anlagen einsetzen. SIMATIC BATCH Server können redundant aufgebaut werden.

Prinzipiell lassen sich die Funktionen von SIMATIC BATCH in vier Bereiche unterteilen:

- Rezeptsystem: Erstellung und Verwaltung von Grundrezepten und Bibliotheksoperationen
- Chargenplanung: Ein- und Umplanung von Chargen und Produktionsaufträgen

- Chargensteuerung: Bedienen und Visualisieren der zur Produktion freigegebenen Chargen bzw. der zugehörigen Steuerrezepte, inkl. Visualisieren der aktuellen Teilanlagenbelegung
- Chargendatenverwaltung: Erfassung, Speicherung und Berichterstellung von Chargendaten

Weitere Hinweise zur Konfiguration und Nutzung von SIMATIC BATCH enthält das Kapitel "Rezeptursteuerung mit SIMATIC BATCH (Seite 103)".

Route Control

Das Optionspaket SIMATIC Route Control dient der Projektierung, Überwachung und Diagnose von Materialtransporten (Wegen) in einer Anlage. Es ist in SIMATIC PCS 7 und SIMATIC BATCH voll integriert.

Weitere Hinweise zu Konfiguration und Nutzung von "SIMATIC Route Control" enthält das Kapitel "SIMATIC Route Control (Seite 110)".

Simulation mit S7-PLCSIM

S7-PLCSIM ist ein Simulationstool für S7-Anwenderprogramme. Diese optional erhältliche Softwarekomponente simuliert eine SIMATIC S7-CPU auf einem PG/PC. Die projektierte Applikationssoftware kann ohne den Einsatz von AS-Hardware (CPU und / oder Signalbaugruppen) getestet werden. Dabei können bis zu 8 CPU-Instanzen simuliert werden.

Kommunikationsprozessoren und Route Control können nicht simuliert werden.

Hinweis

Der Einsatz von S7-PLCSIM ist insbesondere für das Testsystem interessant, z. B. bei Typical-Tests.

Für einen späteren Betrieb mit Ethernet-Netzwerk sollte in PLCSIM bereits die Ethernet-Verbindung projektiert werden, da bei Verwendung von MPI alle Kommunikationsverbindungen umprojektiert werden müssten.

Simulation mit SIMIT und Virtual Controller

SIMIT kann von der Simulation der Feldebene bis hin zur Prozesssimulation genutzt werden, siehe Kapitel "Simulation für Testbetrieb (Seite 151)".

3.3.4 Softwarekomponenten Bedienebene

Basissoftware Operator System (OS)

Systeme zur Bedienung und Beobachtung der Anlage werden entweder als Einzelplatz- oder als Mehrplatzsystem realisiert.

Mit einem Einzelplatzsystem kann die komplette Bedienung und Beobachtung über einen PC erfolgen.

Ein Mehrplatzsystem (Client-Server-Architektur) besteht aus den Bedienplätzen (OS-Clients) und einem oder mehreren OS-Servern, welche die OS-Clients mit Daten versorgen.

Zur Erhöhung der Verfügbarkeit können redundante Systeme aufgebaut werden.

Hinweis

Die Lizenzgröße der Operator Stationen kann nachträglich über entsprechende Pakete erhöht werden. Bei Erweiterungen/Updates der Lizenzen muss die vorhandene Lizenz frei sein, d. h. die Runtime darf nicht aktiv sein. Eine Online-Erweiterung ist nur bei redundanten Servern möglich.

SIMATIC BATCH und Route Control

SIMATIC BATCH und SIMATIC Route Control verfügen jeweils über eigene Bedienkomponenten. Einige Funktionen sind aber auch in die Basis-OS integriert und von dort aus bedienbar.

Zusatzsoftware SFC-Visualisierung

Ein SFC (Sequential Function Chart) wird zur Ablaufsteuerung (auch sog. Schrittkette) von Prozessen eingesetzt. SFCs bestehen aus einer Folge von Schritten, die durch die jeweiligen Weiterschaltbedingungen (sog. Transitionen) voneinander getrennt sind. Solche Weiterschaltbedingungen können durch einfache Vergleiche oder auch durch eine komplexe Logik (SFC Berechnungen) realisiert werden.

Mit Hilfe der SFC-Visualisierung können die projektierten SFC auf der Operator Station dargestellt und im Handbetrieb bedient werden. Prozesse können in ihren Verfahrensschritten durch die SFC-Visualisierung übersichtlich dargestellt werden.

Zur Projektierung der SFC-Visualisierung ist kein zusätzlicher Aufwand nötig.

Zusatzsoftware OS Web Option

Die PCS 7 OS Web Option ermöglicht die Bedienung und Beobachtung der PCS 7-Anlage über Intranet bzw. Internet.

Seit SIMATIC PCS 7 V9.0 können mit der OS Web Option auch die SIMATIC BATCH OS Bedienelemente (SIMATIC BATCH OS Controls) angezeigt werden.

Hinweis

Der Einsatz der Web Option im regulierten Umfeld sollte mit dem Kunden eng abgestimmt werden. Aspekte wie Zugang zum Web Client, kritische oder unkritische Bedienungen bzw. Beobachtungen, Logon und Audit Trail sowie eine sichere Datenverbindung sollten hierbei berücksichtigt werden.

Weitere Hinweise zum Einsatz und zur Konfiguration der Web Option siehe Kapitel "PCS 7 OS Web Option (Seite 98)".

3.3.5 Langzeitarchivierung

Im regulierten Umfeld müssen relevante Produktions- und Qualitätsdaten teilweise für 5, 10 oder mehr Jahre aufbewahrt werden. Diese Daten gilt es zu definieren, sie sicher zu speichern und gestaffelt in externe Archive zu verlagern.

Konfigurationsmöglichkeiten für eine Archivierung sind im Basispaket enthalten. Je nach anfallender Datenmenge und Aufbewahrungszeitraum wird die Strategie zur Auslagerung auf einen anderen Rechner entsprechend definiert.

Eine Langzeitarchivierung von Prozesswerten und Meldungen kann z. B. mit einem Export/ Import von Archiven oder mit der Option SIMATIC Process Historian angelegt werden. Nachfolgend werden beide Konzepte vorgestellt.

OS-Archivierung

Die Prozesswerte und Meldungen werden in einem Umlaufarchiv auf Microsoft-SQL-Servertechnologie basierend gespeichert. Die im Umlaufarchiv gespeicherten Daten können auf einen anderen Rechner ausgelagert und bei Bedarf wieder eingelesen oder dauerhaft in ein Langzeitarchiv übergeben werden, siehe dazu Kapitel "Einrichten von Prozesswertarchiven (Seite 134)".

SIMATIC Process Historian

Auf einem SIMATIC Process Historian können Prozesswerte und Meldungen von mehreren SIMATIC PCS 7 OS-Servern (auch redundanten Systemen) sowie Batchdaten zentral erfasst und archiviert werden. Den transparenten Zugriff auf die archivierten Daten für die Ansicht der Meldungen und Prozesswerte in der Bedienoberfläche wickelt das System automatisch im Hintergrund ab. Die in den WinCC-Archiven gespeicherten Meldungen werden komplett in den Process Historian transferiert. Von den Variablen hingegen werden nur diejenigen übernommen, die mit der Eigenschaft "Langzeitrelevant" gekennzeichnet sind.

Falls der Process Historian nicht erreichbar ist, verbleiben die abgeschlossenen Archive auf den OS-Servern und werden zu einem späteren Zeitpunkt ausgelagert, wenn die Verbindung zum Process Historian wieder aktiv ist. Dazu ist ein ausreichendes Speichervolumen auf den OS-Servern einzuplanen. Auch eine Überwachung der Netzwerk-Verbindung kann sinnvoll sein.

Über definierte Schnittstellen besteht ein direkter Zugriff auf die archivierten Prozesswerte und Meldungen. Auf diese Weise stehen wichtige Produktionsdaten unternehmensweit zur Verfügung.

Siehe auch

- Handbuch "PCS 7 Kompendium Teil A", Kapitel 10.4.4 "Langzeitarchivierung", Online-Support unter Beitrags-ID 109809015 (https://support.industry.siemens.com/cs/ww/de/view/109809015)
- Handbuch "Process Historian 2020", Online-Support unter Beitrags-ID 109809287 (https://support.industry.siemens.com/cs/ww/de/view/109809287)

3.3.6 Protokollierung

Für einen erforderlichen Qualitätsnachweis wird definiert, welche Produktionsdaten relevant für die Ausgabe in einem Protokoll sind. Ein Protokoll kann Meldungen und Alarme, Chargendaten sowie Prozesswerte in Tabellen- oder Kurvenform enthalten.

Siehe auch

- Handbuch „PCS 7 Engineering System“, Kapitel 4.3.5, Online-Support unter Beitrags-ID 109800500 (https://support.industry.siemens.com/cs/ww/de/view/109800500)

Report Designer

Mit dem Report Designer werden die Prozessdaten kontinuierlich für einen definierbaren Zeitraum protokolliert. Die Protokollausgabe wird über einen Druckauftrag gestartet.

Der Report Designer wird auch zur Dokumentation des konfigurierten OS-Projektes genutzt. Dazu sind vorgefertigte Protokoll-Layouts und Druckaufträge im Lieferumfang von SIMATIC PCS 7 enthalten. Sowohl vorgefertigte Protokoll-Layouts als auch Druckaufträge können im Report Designer geöffnet und wunschgemäß modifiziert werden.

Information Server

Eine Berichterstellung zu aufgezeichneten Prozesswerten, Chargendaten und Meldungen bietet die Option SIMATIC Information Server. Sowohl vorgefertigte als auch auf Basis der Microsoft Reporting Services eigens konfigurierte Berichte können in der web-basierten Oberfläche dargestellt und in verschiedene Formate exportiert werden. Eine zusätzliche Integration in Microsoft Word, Excel oder PowerPoint zeigt die Berichte zu den Archivdaten im gewohnten Office-Umfeld.

Siehe auch

- Handbuch "PCS 7 Kompendium Teil A", Kapitel 10.4.4.1 und 10.4.4.3 "Information Server", Online-Support unter Beitrags-ID 109809015 (https://support.industry.siemens.com/cs/ww/de/view/109809015)

Datenaustausch über Open PCS 7

Mit Open PCS 7 können Daten mit externen Systemen wie z. B. Betriebs- und Produktionsleitebene, MES-Ebene oder ERP-Ebene über die OPC-Schnittstelle ausgetauscht werden, ohne dass dazu die Kenntnis der SIMATIC PCS 7 Projekttopologie erforderlich ist. OPC (Open Platform Communications) bezeichnet eine einheitliche und herstellerunabhängige Softwareschnittstelle, deren Standard von der OPC Foundation definiert wurde. In der OPC Foundation sind führende internationale Firmen der Industrieautomation zusammengeschlossen.

Informationen zu OPC sind im Internet (https://opcfoundation.org/) erhältlich. Der Einsatz von Open PCS 7 wird im Kapitel "Open PCS 7 (Seite 101)" näher erläutert.

3.4 Spezifikation der Applikationssoftware

Neben der Auswahl und Definition der Hardware (siehe Kapitel "Auswahl und Spezifikation der Hardware (Seite 26)") und der eingesetzten Standard-Softwarekomponenten (siehe Kapitel "Spezifikation der Basissoftware (Seite 29)") ist die Spezifikation der Applikationssoftware ein wesentlicher Bestandteil der gesamten Spezifikation. Die Spezifikationen für Konfiguration und Design des Systems dienen neben der Funktionsspezifikation später als Akzeptanzkriterium bei der System-Verifizierung (FAT, SAT, etc.).

Die Spezifikation von Konfiguration und Design kann aus einem, wird in den meisten Fällen aber aus mehreren Dokumenten bestehen. Ergänzend werden oft weitere separate Dokumente geführt, wie z. B. Messstellenliste, E/A-Liste, Parameterliste, R&I, etc. Der Status dieser Dokumente (Version, Freigabe) muss ebenso eindeutig definiert sein wie bei den anderen Spezifikationsdokumenten.

Siehe auch

- GAMP 5-Leitfaden, Anhang D3 "Konfigurierung und Entwurf"

Neben der bereits zuvor erwähnten Hardwarespezifikation kann die Spezifikation zum Beispiel folgendermaßen aufgeteilt werden:

Konfiguration und Design (allgemein)

- Organisation der Domäne, Domänenadministration, Arbeitsgruppe
- Benutzeradministration in Windows,
  Definition von Benutzergruppen, Benutzern, Berechtigungen, lokale Benutzer, Konfiguration von SIMATIC Logon, WinCC User Administrator, SIMATIC BATCH Rechteverwaltung, Route Control Benutzergruppen, etc.
- Domäne und PC Profile
- Druckerkonfiguration
- Archivkonfiguration (Archive, Archivzyklen, Batch Reports)
- Schnittstellen (S7-Verbindungen, OPC, Diskrete E/A Verarbeitung)

HMI Spezifikation

Bei der Bedienoberfläche werden u. a. die folgenden Aspekte spezifiziert:

- Bildschirmlayout & Navigation
- Anlagenbilder, Teilanlagenbilder, Detailbilder von Schnittstellen
- Bedienlevel, eventuell Zugriffsberechtigungen
- Bildhierarchie
- Bildschirmauflösung, Bildzyklen
- Block Icons, verwendete Faceplates
- Meldeverhalten, Meldeklassen, Prioritäten, Darstellung, siehe Kapitel "Spezifikation (Seite 112)"

Software Design Spezifikation

- Allgemeines wie z. B. Name des Multiprojektes, Name der Projekte, Name der Bibliotheken, Technologische Hierarchie
- Sinnvolle Aufteilung der Anlagen- und Teilanlagenbereiche zu den ASen, siehe auch Kapitel "Hardware-Spezifikation (Seite 26)"
- Software-Struktur, Typical- und Modulspezifikation, evtl. in eigenem Dokument
- Control Modules (CM) und Typen (CMT) (Zustände, Verhalten, Verhalten bei Neustart)
- Equipment Modules (EM) und Typen (EMT) (Zustände, Status Logik, Verhalten, Projektierung)
- Evtl. Route Control (Funktion, Interface-Blöcke)
- SIMATIC BATCH (Funktion, Aufteilung von Rezepten, Nutzung von Formulas)
- Evtl. weitere genutzte Funktionalitäten wie z. B. RFID etc.
- Verhalten bei Stromausfall und Wiederanlauf (Verhalten der PC-Stationen und ASen, Ausfall einer AS)
- Zeitsynchronisation, Festlegung von Uhrzeit-Master und –Slaves
- Beschreibung von Ausnahmezuständen zur sicheren Anlagenbedienung
- Not-Aus Verhalten

Hinweis

SIMATIC PCS 7 nutzt als Grundlage für die Projektierung von chargenorientierten Fahrweisen das Modell der ANSI/ISA-88.01, siehe auch Kapitel "Normkonformität mit ISA-88.01 (Seite 103)".

Siehe auch

- Anwendungsbeispiel zur Spezifikation technischer Funktionen mit SFC-Typen sowie zur Instanziierung, Online-Support unter Beitrags-ID 33412955 (https://support.industry.siemens.com/cs/ww/de/view/33412955)

3.5 Zusatzsoftware SIMATIC PCS 7 Add-ons

Der SIMATIC PCS 7 Add-on-Katalog enthält Lösungen für verschiedene Einsatzbereiche oder spezielle Branchen, wie z. B. die Prozessindustrien. Für die dort aufgeführten Add-ons sind in dem Katalog die Kontaktadressen der jeweils verantwortlichen Ansprechpartner angegeben.

Hinweis

Zur Realisierung von Funktionen, die über den Standardumfang von PCS 7 hinausgehen, sollten vorrangig Add-ons aus den aktuellen Katalogen eingesetzt werden. Siehe SIMATIC PCS 7 Add-ons (https://support.industry.siemens.com/cs/ww/de/view/109745636).

3.5.1 versiondog – Versionierung und Konfigurationskontrolle

Mit versiondog kann der gesamte Lebenszyklus einer SIMATIC PCS 7-Anlage über die Versionshistorie nachvollzogen werden – von der Projektierung über die Inbetriebnahme bis hin zur kontinuierlichen Optimierung während des Betriebs. Wird eine neue Version erstellt, ermittelt versiondog automatisch die Änderungen und macht sie für den Anwender transparent.

PCS 7-Smart Compare stellt die Unterschiede zwischen zwei Versionen in der gewohnten SIMATIC PCS 7-Projektstruktur dar. Unterschiede zwischen zwei CFC- oder SFC-Plänen werden in einer grafischen Gegenüberstellung farblich markiert. Im Audit Trail von versiondog lässt sich jederzeit verifizieren, wer wann was warum geändert hat.

Siehe auch

- PCS 7 Add-on Beschreibung im Internet (https://mall.industry.siemens.com/mall/de/de/Catalog/Products/10048340?tree=CatalogTree), einschl. Herstellerkontakt

3.5.2 OPD – Bedienerdialoge und elektronische Unterschriften

Die Software Operator Dialog (OPD) vereinfacht die Interaktion zwischen Bedienpersonal und Prozessleitsystem. Als leistungsfähiges Bedienwerkzeug erleichtert sie die Steuerung des Prozesses und führt einen lückenlosen Nachweis über alle manuellen Bedienhandlungen.

Die in einer SIMATIC PCS 7 / SIMATIC BATCH-Systemumgebung ausführbare OPD-Software basiert auf der Microsoft SQL Server-Software. Sie nutzt SIMATIC Logon zur Benutzerverifizierung und für elektronische Signaturen.

Siehe auch

- PCS 7 Add-on Beschreibung im Internet (https://mall.industry.siemens.com/mall/de/de/Catalog/Products/10037427?tree=CatalogTree), einschl. Herstellerkontakt

3.6 Hilfsprogramme und Treiber

3.6.1 Druckertreiber

Es wird empfohlen, die im Betriebssystem integrierten und für PCS 7 freigegebenen Druckertreiber zu verwenden. Bei Verwendung von externen Treibern wird keine Gewährleistung für den einwandfreien Betrieb des Systems übernommen.

3.6.2 Virenscanner

Der Einsatz von Virenscannern ist im Prozessbetrieb (Runtime) zulässig. Weitere Informationen bzgl. der Auswahl, Konfiguration und Aktualisierung von Virenscannern siehe:

- Kompatibilitätstool (www.siemens.de/kompatool)
- Handbuch "PCS 7 Kompendium Teil F", Kapitel 9, Online-Support unter Beitrags-ID 109804118 (https://support.industry.siemens.com/cs/ww/de/view/109804118)

Beim Einsatz von Virenscannern sollten folgende Einstellungen beachtet werden:

- Die Echtzeitsuche ist eine der wichtigsten Funktionen. Es ist jedoch ausreichend, den eingehenden Datenverkehr zur untersuchen.
- Die zeitgesteuerte Suche muss deaktiviert werden, da diese während des Prozessbetriebes die Performance des Systems erheblich einschränkt.
- Die manuelle Suche darf während des Prozessbetriebes nicht durchgeführt werden. Sie kann in regelmäßigen Abständen z. B. während Wartungsintervallen erfolgen.

Solche Festlegungen sollten in der Spezifikation und/oder gegebenenfalls in einer Arbeitsanweisung (SOP) der verantwortlichen IT-Abteilung beschrieben sein.

Weitergehende Hinweise zum Thema IT Security siehe Kapitel "Informationssicherheit und Datenintegrität (Seite 55)".

3.6.3 Image & Partition Tools

Zusatzsoftware zu den Themen "Image" und "Partition" ermöglicht das Erstellen einer Datensicherung von kompletten Festplatteninhalten, das sog. Image, sowie das Partitionieren von Festplatten. Mit der im Image gesicherten Systemsoftware ist eine schnelle Wiederherstellung des Systems möglich. Gesicherte Festplatteninhalte können auch auf baugleiche Geräte aufgespielt werden. Dies erleichtert den Austausch von Rechnern.

Siemens stellt mit dem "SIMATIC Image und Partition Creator" ein Softwarepaket zur Verfügung, mit dem diese Aufgaben erledigt werden können. Dies ist sogar ohne separate Installation möglich. Administrationskenntnisse sollten vorhanden sein.

Siehe auch

- SIMATIC IPC Image und Partition Creator im Online-Support unter Beitrags-ID 109781271 (https://support.industry.siemens.com/cs/ww/de/view/109781271)

Hinweis

Die erstellten Images dienen zur Wiederherstellung des installierten Systems, nicht aber zur Sicherung von Online-Daten, der Anwendersoftware (Projekt) sowie Autorisierungen und License Keys.

Ausführlichere Hinweise zu den Themen Datensicherung und Systemwiederherstellung beinhalten die jeweiligen Kapitel in diesem Handbuch.

3.6.4 SIDSI Backup & Restore Professional

Für die systematische und zuverlässige Sicherung und Wiederherstellung von virtuellen Maschinen dient das vorkonfigurierte System “SIDSI Backup & Restore Professional“.

Unter der Verwendung des Image-basierten Ansatzes zur Backup-Erstellung besteht die Möglichkeit, die Quellen und Zyklen individuell zu konfigurieren und automatisch ausführen zu lassen.

Folgende Tools zur Backup- und Restore-Erstellung kommen zum Einsatz:

- SIDSI Backup Wizard: Backups virtueller Maschinen auf SIVaaS Systemen und von IPCs mit Windows Betriebssystem
- SIVaas Back & Restore: Hypervisor Betriebssysteme und Konfiguration des Hypervisors
- Paragon Hard Disk Manager: Backup & Restore Server (inkl. Auslieferungszustand)

Systeminstallation und -konfiguration

4

4.1 Installation des Betriebssystems

Bei der Auswahl des Betriebssystems sind die Hinweise unter Kapitel "Systemspezifikation (Seite 25)" bzw. die darin genannten Quellen zu beachten.

Siehe auch

- Installationsanleitung für Betriebssystem
- Handbuch "PCS 7 PC-Konfiguration", Online-Support unter Beitrags-ID 109794377 (https://support.industry.siemens.com/cs/ww/de/view/109794377)

4.2 Installation SIMATIC PCS 7

Für die Installation von SIMATIC PCS 7 ist den Anweisungen des Setups zu folgen. Vor der PCS 7-Installation müssen gegebenenfalls die zugelassenen Fremdkomponenten (z. B. Office) installiert werden. Weitere Hinweise zur Installation sind enthalten in

- Handbuch "PCS 7 Kompendium Teil A", Kapitel 4.3.4, Online-Support unter Beitrags-ID 109809015 (https://support.industry.siemens.com/cs/ww/de/view/109809015)
- Handbuch "Sicherheitskonzept PCS 7 und WinCC", Online-Support unter Beitrags-ID 109780811 (https://support.industry.siemens.com/cs/ww/de/view/109780811)
- Handbuch "PCS 7 PC-Konfiguration", Online-Support unter Beitrags-ID 109794377 (https://support.industry.siemens.com/cs/ww/de/view/109794377)
- Handbuch PCS 7 "Freigegebene Baugruppen", Online-Support unter Beitrags-ID 109800496 (https://support.industry.siemens.com/cs/ww/de/view/109800496)
- PCS 7 Installations-DVD
- Liesmich/Readme-Dateien der einzelnen SIMATIC-Komponenten

Hinweis

Im Setup zur Installation muss SIMATIC Logon angewählt sein.

4.3 Einrichten der Benutzerverwaltung

Für den sicheren und vorschriftskonformen Betrieb wird ein kontrollierter Zugriff sowohl auf die Bedienebene und die Konfigurationsebene als auch auf Archivdaten und Sicherungskopien gefordert.

Eine benutzerbezogene An- und Abmeldung für Bedienaktionen ist dabei eine grundlegende Funktionalität zur Erfüllung dieser Anforderung.

Die Benutzerverwaltung mit SIMATIC Logon nutzt die Mechanismen des Windows-Betriebssystems und sorgt so für einen zuverlässigen Zugriffsschutz. Für die Organisation der Bedienberechtigung werden die Benutzer ihren Aufgaben entsprechend unterschiedlichen Benutzergruppen in der Windows-Benutzerverwaltung zugeordnet.

Diesen Benutzergruppen werden Berechtigungen für die einzelnen Bedienhandlungen zugeteilt.

Hinweis

Die Struktur der Benutzergruppen sollte bereits zu Projektbeginn in der Spezifikation festgelegt und zu Beginn der Projektierung eingerichtet werden.

Die individuellen Bedienrechte der Software-Module werden in der Modulbeschreibung definiert.

Alle Berechtigungsstufen zur Bedienung über die Visualisierungsoberfläche (Bildbausteine, Eingabefelder, Schaltflächen, etc.) und deren Zuordnung zu den Benutzergruppen sind gemäß den Spezifikationen einzurichten und im Projektverlauf zu testen.

Bei der Einrichtung wird differenziert, auf welcher Ebene ein Benutzer agiert. So ist die Zugehörigkeit zu bestimmten Windows-Benutzergruppen für den Start bzw. der Konfiguration von SIMATIC Komponenten wie SIMATIC PCS 7 OS oder SIMATIC Logon erforderlich. Diese Benutzergruppen werden bei der Installation der Software-Komponenten automatisch in der Windows-Benutzerverwaltung angelegt und dürfen nicht gelöscht werden.

Für die Bedienung des Prozessbetriebs werden projektspezifische Benutzergruppen eingerichtet und in der Projektierung mit den erforderlichen Bedienrechten ausgestattet.

Folgende Reihenfolge wird beim Einrichten der Benutzerverwaltung mit SIMATIC Logon empfohlen und in den nachfolgenden Kapiteln beschrieben:

- Einrichten der Benutzergruppen und Benutzer auf Betriebssystemebene, siehe Kapitel "Benutzerverwaltung auf Betriebssystemebene (Seite 44)"
- Sicherheitseinstellungen in Windows einrichten, siehe Kapitel "Sicherheitseinstellungen in Windows (Seite 46)"
- SIMATIC Benutzergruppen, siehe Kapitel "SIMATIC Benutzergruppen (Seite 46)"
- Einrichtung und Konfiguration von SIMATIC Logon, siehe Kapitel "Konfiguration von SIMATIC Logon (Seite 47)"
- Administration der Berechtigungen für die einzelnen Benutzergruppen in den SIMATIC Komponenten (ES, OS, BATCH), siehe Kapitel "Administration der Berechtigungen (Seite 49)"

4.3.1 Benutzerverwaltung auf Betriebssystemebene

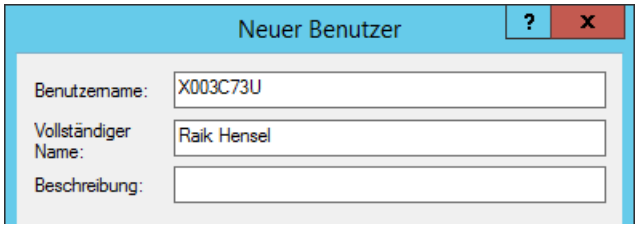
Die Verwaltung der Benutzerrechte mit SIMATIC Logon basiert auf den Mechanismen des Windows-Betriebssystems. Hier stehen zwei Möglichkeiten der Benutzerverwaltung zur Verfügung:

- Zentrale Verwaltung in einer Domänenstruktur
- Verwaltung auf einem Rechner einer Arbeitsgruppe

Beim Einsatz mehrerer Server bzw. bei redundanten Servern muss die Domänen-Struktur genutzt werden, um bei Ausfall eines Domänen-Servers die Bedienung bzw. Anmeldung von Benutzern zu gewährleisten. Die Domänen-Server-Funktionalität darf hierbei nicht auf einem System mit SIMATIC PCS 7 installiert werden.

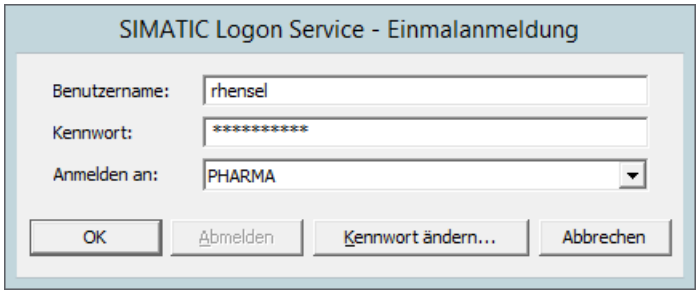
Hinweis

In der Windows-Computerverwaltung ist für jeden Benutzer außer dem Benutzernamen auch der Vollständige Name einzutragen. Dieser Name kann nach dem Einloggen zur Anzeige in SIMATIC PCS 7 benutzt werden und ist für elektronische Unterschriften erforderlich. Der Vollständige Name muss daher angegeben werden.



Siehe auch

- Handbuch "Sicherheitskonzept PCS 7 und WinCC", Online-Support unter Beitrags-ID 109780811 (https://support.industry.siemens.com/cs/ww/de/view/109780811)
- Handbuch "PCS 7 Kompendium Teil A", Kapitel 4.2.6 "Arbeitsgruppe und Domäne", Online-Support unter Beitrags-ID 109809015 (https://support.industry.siemens.com/cs/ww/de/view/109809015)



Während der Bediener durch seine Anmeldung in der SIMATIC-Umgebung für seine Bedienrechte authentifiziert wird, ist gleichzeitig im Windows Betriebssystem ein "Standardbenutzer" angemeldet, der die erforderlichen Rechte auf Betriebssystemebene besitzt. Diese sollten nicht höher sein als unbedingt erforderlich, siehe auch Kapitel "Zugriffskontrolle auf Betriebssystemebene (Seite 53)".

Der am Betriebssystem angemeldete Benutzer sollte systemweit der gleiche sein und beim Hochfahren eines OS-Rechners automatisch eingeloggt werden.

Hinweis

An- und Abmeldevorgänge sowie erfolglose Anmeldeversuche sind im SIMATIC Logon Eventlog Viewer einsehbar und exportierbar; Änderungen an der Benutzer- und Gruppenkonfiguration werden auf Betriebssystemebene im EventLog aufgezeichnet und können dort gesichert werden.

4.3.2 Sicherheitseinstellungen in Windows

Zugriffsberechtigungen sowie Einstellungen wie Passwortlänge, -komplexität und Gültigkeitsdauer können und sollten zur Erhöhung der Datensicherheit geeignet konfiguriert werden.

Bei Verwendung von SIMATIC Logon nimmt der Systemadministrator folgende Sicherheitseinstellungen in Windows unter *Systemsteuerung > Verwaltung > Lokale Sicherheitsrichtlinie > Sicherheitseinstellungen > Kontorichtlinien / Lokale Richtlinien* vor:

- Kennwortrichtlinien wie Komplexität, Kennwortlänge, Kennwortalterung
- Kontosperrungsrichtlinien
- Überwachungsrichtlinien (z. B. Anmeldeereignisse und Anmeldeversuche)

Hinweis

Nach der Installation von Windows sind bei den Kennwortrichtlinien, Kontosperrungsrichtlinien und den Überwachungsrichtlinien Default-Parameter eingestellt. Diese Einstellungen müssen überprüft und den geltenden Projektanforderungen entsprechend angepasst werden.

Siehe auch

- Kapitel "Zugriffskontrolle auf Betriebssystemebene (Seite 53)"
- Kapitel "Informationssicherheit und Datenintegrität (Seite 55)"
- Handbuch "PCS 7 Kompendium Teil F", Kapitel 7.4 "Passwortrichtlinien", Online-Support unter Beitrags-ID 109804118 (https://support.industry.siemens.com/cs/ww/de/view/109804118)
- Rundumschutz mit Industrial Security – Anlagensicherheit, Online-Support unter Beitrags-ID 50203404 (https://support.industry.siemens.com/cs/ww/de/view/50203404)

4.3.3 SIMATIC Benutzergruppen

Bei der Installation von PCS 7 werden im Betriebssystem automatisch lokale SIMATIC Standard-Benutzergruppen mit unterschiedlichen Rechten angelegt (SIMATIC HMI, etc.). Diese dürfen nicht verändert oder gelöscht werden.

Die definierten Benutzer und Benutzergruppen müssen entsprechend ihrer Berechtigungen zu Mitgliedern dieser SIMATIC Benutzergruppen gemacht werden.

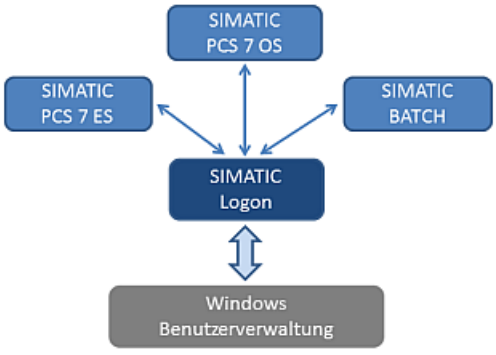
Durch eine Unterscheidung bei der Anmeldung auf Windowsebene zwischen Systemadministrator und Benutzer (Anlagenbediener) wird eine konsequente Trennung bei der Computerzugriffsberechtigung erreicht.

Siehe auch

- Kapitel "Zugriffskontrolle auf Betriebssystemebene (Seite 53)"
- Handbuch "Sicherheitskonzept PCS 7 und WinCC", Online-Support unter Beitrags-ID 109780811 (https://support.industry.siemens.com/cs/ww/de/view/109780811)

4.3.4 Konfiguration von SIMATIC Logon

SIMATIC Logon dient als Schnittstelle zwischen der Windows-Benutzerverwaltung und den SIMATIC Komponenten. Es prüft die Richtigkeit der Anmeldedaten eines Benutzers gegen die zentrale Benutzerverwaltung. Bei einer gültigen Anmeldung werden die zugehörigen Benutzergruppen an die Bedienstation zurückgegeben.



Die Grundeinstellungen von SIMATIC Logon werden mit dem Dialogfeld "SIMATIC Logon konfigurieren" durchgeführt. Die möglichen Einstellungen sind im Projektierungshandbuch SIMATIC Logon beschrieben und beinhalten z. B.:

- Die Anmeldung eines "Default User" nach Benutzerabmeldung
- Anmeldeserver ("Arbeitsumgebung")
- Automatisches Abmelden über SIMATIC Logon

Hinweis

Ereignisse wie z. B. erfolgreiche und fehlgeschlagene An-/Abmeldevorgänge, Passwortänderungen, etc. werden in der EventLog-Datenbank von SIMATIC Logon gespeichert. Dies muss bei der Datensicherung berücksichtigt werden, siehe auch Kapitel "Audit Trail und Änderungskontrolle (Seite 119)".

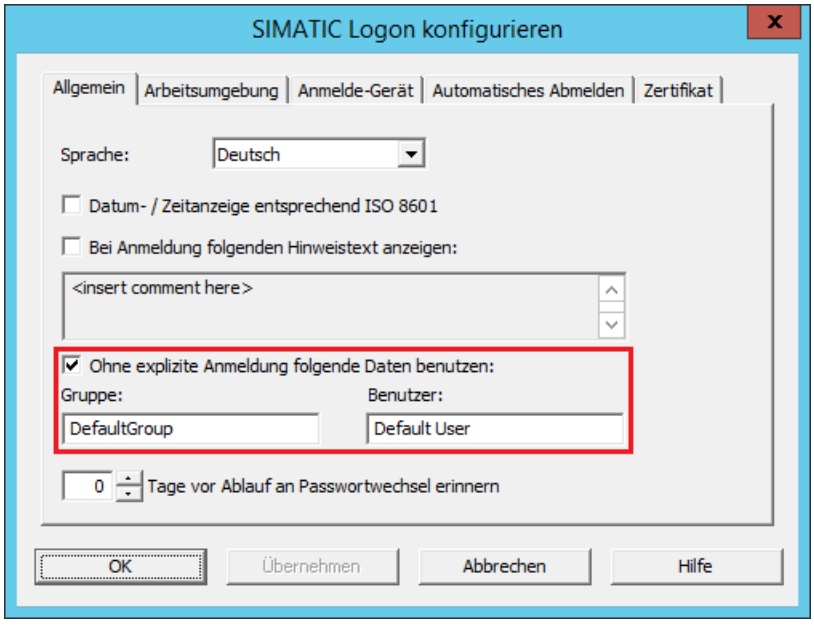
Siehe auch

- Handbuch "SIMATIC Logon", Online-Support unter Beitrags-ID 109804727 (https://support.industry.siemens.com/cs/ww/de/view/109804727)

Default User nach Benutzerabmeldung

Im Register "Allgemein" kann definiert werden, ob nach der Benutzerabmeldung ein Default User angemeldet werden soll.

Der Benutzer "Default User" muss im Gegensatz zu allen anderen Benutzern nicht als Windows-Benutzer angelegt sein. Der "Default User" ist Mitglied der Gruppe "DefaultGroup" oder einer anderen hier zugewiesenen Benutzergruppe. Die Rechte dieser Gruppe werden im WinCC User Administrator festgelegt.



Automatisches Abmelden (Auto-Logoff)

Um zu vermeiden, dass nicht autorisierte Zugriffe mit dem angemeldeten Benutzer erfolgen, sollte die Funktion "Auto-Logoff" in der Konfiguration von SIMATIC Logon mit einstellbarer Zeit aktiviert werden. Wenn die Verwendung des Default Users aktiviert wurde, wird dieser anschließend angemeldet.

Hinweis

Auf der Betriebssystemebene darf kein "Auto-Logoff" aktiviert sein, da sonst die Bedienoberfläche komplett geschlossen wird.

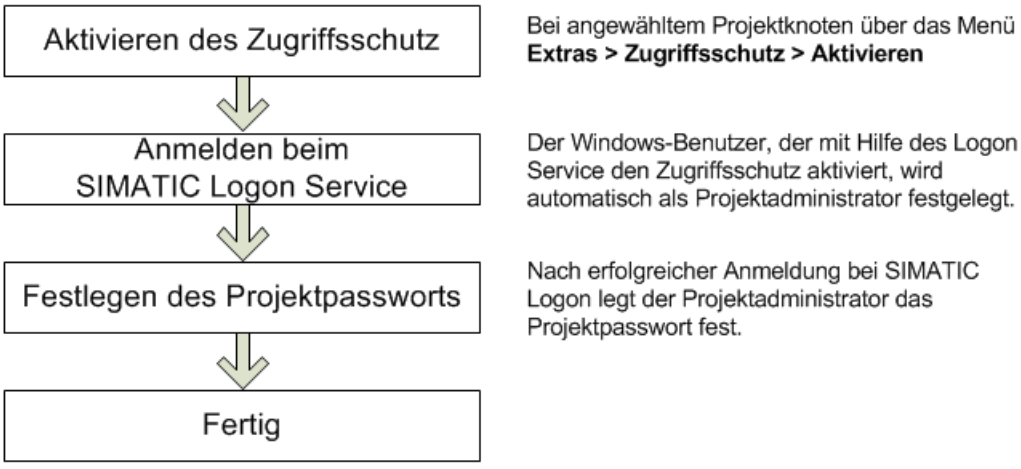
Des Weiteren ist die Aktivierung eines Bildschirmschoners in Verbindung mit SIMATIC Logon nicht zulässig. Beim Entsperren des Bildschirms würde sonst das Passwort des Windows-Benutzers abgefragt, welches der PCS 7 OS-Benutzer aber nicht kennen sollte.

4.4 Administration der Berechtigungen

4.4.1 Rechteverwaltung auf dem Engineering System (ES)

Der Zugriff auf Projekte und Bibliotheken kann mit Hilfe von SIMATIC Logon geregelt werden. Beim Aktivieren des Zugriffsschutzes von neuen oder ungeschützten Projekten wird der angemeldete Windows-Benutzer automatisch als Projekt-Administrator festgelegt. Er kann weitere Benutzer als Projekt-Bearbeiter oder Projekt-Administrator angeben.

Zum Abschluss der Aktivierung des Zugriffsschutzes muss er ein Projektpasswort festlegen, welches nur die Projekt-Administratoren kennen sollten.



Als Oberfläche für die Zuweisung von Benutzern zu den Gruppen der Projektbearbeiter oder als Projektadministrator dient die "SIMATIC Logon Rollenverwaltung".

Hinweis

Die Aktivierung des Zugriffsschutzes muss für jedes Projekt und jede dort eingesetzte Bibliothek im Multiprojekt erfolgen.

Abgleich: Innerhalb eines Multiprojektes kann der Zugriffsschutz eines Projektes oder einer Bibliothek auf alle anderen Projekte/Bibliotheken vererbt werden.

Mögliche Benutzerrechte auf der ES

Ein Benutzer auf der ES kann folgende Rechte haben:

Projekt-Bearbeiter

- Durchführung von Projektänderungen
- Änderungsprotokoll anzeigen

Projekt-Administrator

- Durchführung von Projektänderungen
- Änderungsprotokoll anzeigen
- Änderungsprotokoll aktivieren und deaktivieren
- Zugriffsschutz verwalten
- Zugriffsschutz deaktivieren
- Zugriffsschutz im Multiprojekt abgleichen

Hinweis

Voraussetzung für die Zuordnung der Benutzer zu den Berechtigungsrollen ist, dass sie bereits in der Windows-Benutzerverwaltung bekannt sind.

Nachfolgend werden drei denkbare Szenarien bei der Einrichtung und der Nutzung von geschützten Projekten / Bibliotheken betrachtet.

Szenario 1

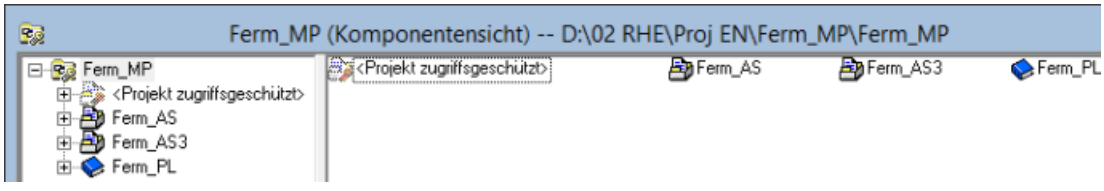
- SIMATIC Logon installiert
- Benutzer ist in Windows bekannt
- Zugriffsberechtigung auf das Projekt ist vorhanden

Sofern der Benutzer die Berechtigung hat, kann er ein Projekt ohne weitere Authentifizierung öffnen, sofern er sich im gleichen Netzwerk befindet. Das gilt auch, wenn das Projekt aus dem Multiprojekt ausgegliedert wurde.

Szenario 2

- SIMATIC Logon installiert
- Benutzer ist in Windows bekannt
- Zugriffsberechtigung auf das Projekt ist nicht vorhanden

Geschützte Projekte / Bibliotheken werden bei einem Benutzer in grau dargestellt, wenn er keine Zugriffberechtigung hat.



Wenn der Benutzer versucht, das Projekt zu öffnen, wird er nach dem Projektpasswort gefragt. Sofern er dieses kennt und es eingibt, wird der Benutzer automatisch als Projekt-Administrator eingetragen.

Hinweis

Das Projektpasswort sollte nur dem Projekt-Administrator bekannt sein.

Szenario 3

- SIMATIC Logon nicht installiert

Ohne installiertes SIMATIC Logon existiert keine Funktion der Projekt-Administration. Bei jedem Öffnen eines geschützten Projektes / Bibliothek muss das Projektpasswort eingegeben werden. Auch hier gilt es, das Projektpasswort nur dem entsprechenden Personenkreis bekannt zu geben. Kommt das geschützte Projekt aus einer Kundenumgebung, muss dort entschieden werden, ob das Passwort am Kundensystem geändert wird.

Hinweis

Der Umgang mit dem Projektpasswort sowie der Zeitpunkt der Aktivierung des Zugriffsschutzes auf ES-Ebene sollten mit Bedacht und frühzeitig definiert werden.

Siehe auch

- Handbuch "PCS 7 Engineering System", Online-Support unter Beitrags-ID 109800500 (https://support.industry.siemens.com/cs/ww/de/view/109800500)

Hinweis

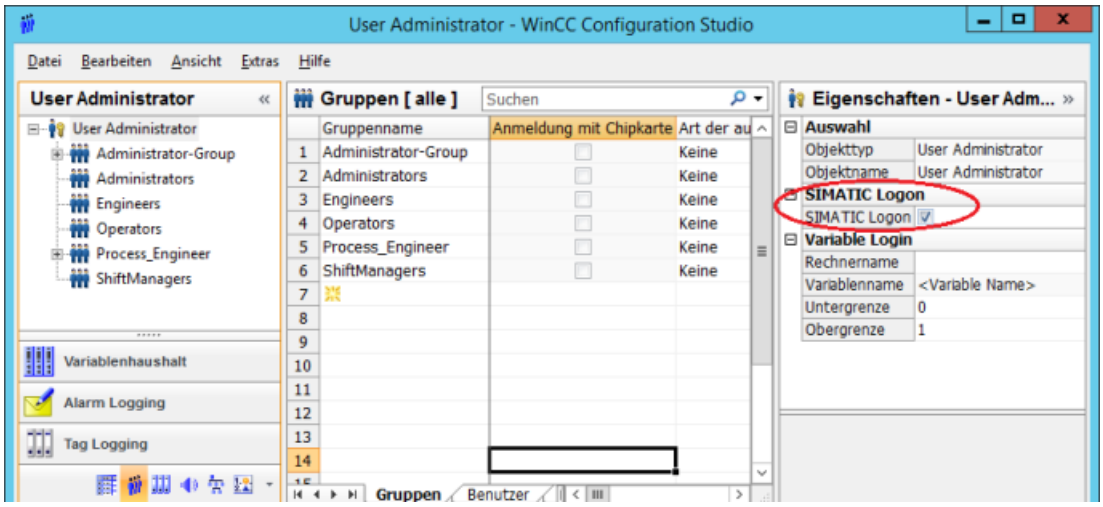
Zusätzlich zu den zuvor beschriebenen Szenarien kann ein Passwort für den Zugriff auf die CPU vergeben werden. Bei einer neu konfigurierten CPU ist ab V9.1 SP1 die Option "Lese-/Schreibschutz" in den Objekteigenschaften der CPU im Register "Schutz" standardmäßig aktiviert. Vergeben Sie hier ein Passwort oder ändern Sie die Schutzstufe.

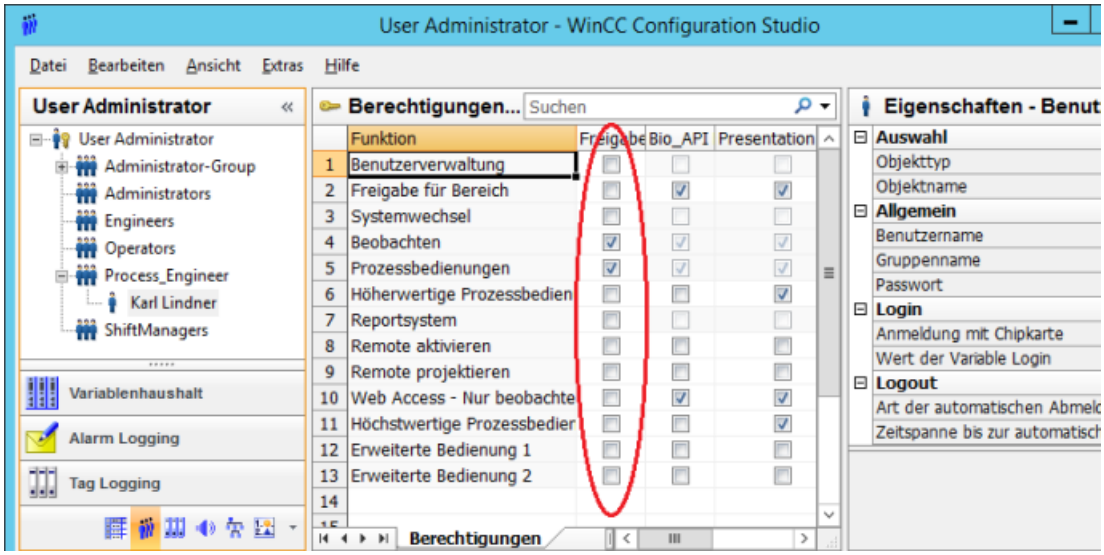
4.4.2 Rechteverwaltung auf dem Bediensystem (OS)

Die Zuordnung von Windows-Benutzergruppen zu PCS 7 OS-Gruppen erfolgt über deren Namensgleichheit. Will man z. B. eine Windows-Gruppe "Operator" zuordnen, dann muss man im PCS 7 OS User Administrator eine gleichnamige Gruppe "Operator" anlegen und die notwendigen Rechte vergeben. Folgende Vorgehensweise ist dabei einzuhalten:

- PCS 7 OS-Projekt öffnen
- User Administrator über WinCC Control Center öffnen
- Anlegen der Gruppe(n)
- Vergabe der Rechte pro Gruppe

Im nachfolgenden Bild ist beispielhaft die Vergabe der Bedienrechte zu den einzelnen Gruppen dargestellt.



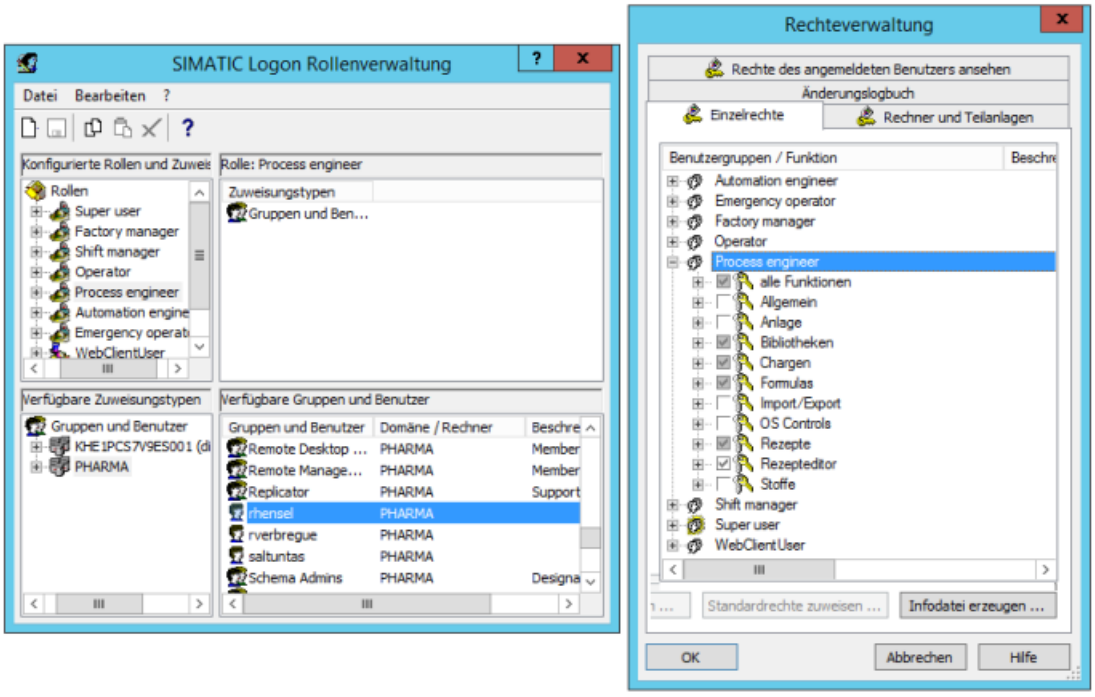


Hinweis

Insbesondere im regulierten Umfeld ist die zentrale Administration der Benutzer in vielen Fällen unabdingbar, was über SIMATIC Logon realisiert wird. Hierzu muss SIMATIC Logon in der PCS 7 OS "User Administration" des jeweiligen PCS 7 OS-Rechners durch Setzen des Hakens aktiviert werden.

4.4.3 Rechteverwaltung in SIMATIC BATCH

Die Zuordnung von Berechtigungen und Rollen in der Applikation von SIMATIC BATCH erfolgt in der "SIMATIC Logon Rollenverwaltung".



In SIMATIC BATCH erfolgt die Zuordnung der einzelnen Rollen zu den Bedienrechten. Ergänzend können festgelegt werden:

- Benutzerrechte einer Benutzerrolle
- Erlaubte Benutzerrollen pro Rechner
- Erlaubte Benutzerrollen pro Teilanlage

4.5 Zugriffskontrolle auf Betriebssystemebene

Für die allgemeine Netzwerkkonfiguration siehe Handbücher "Projektierung PCS 7 Engineering System" und "Sicherheitskonzept PCS 7 und WinCC".

Da Zugriffe auf die Windows-Betriebssystemebene aus Sicherheitsgründen zu vermeiden sind, müssen zusätzliche Konfigurationseinstellungen durchgeführt werden. Diese Einstellungen vermeiden ein unerlaubtes Zugreifen aus dem Prozessbetrieb von SIMATIC PCS 7 auf sensible Daten des Betriebssystems.

Hinweis

Der Zugriff auf die Betriebssystemebene sollte ausschließlich den Administratoren und technischem Wartungspersonal vorbehalten sein.

Automatisches Hochfahren und Anmelden

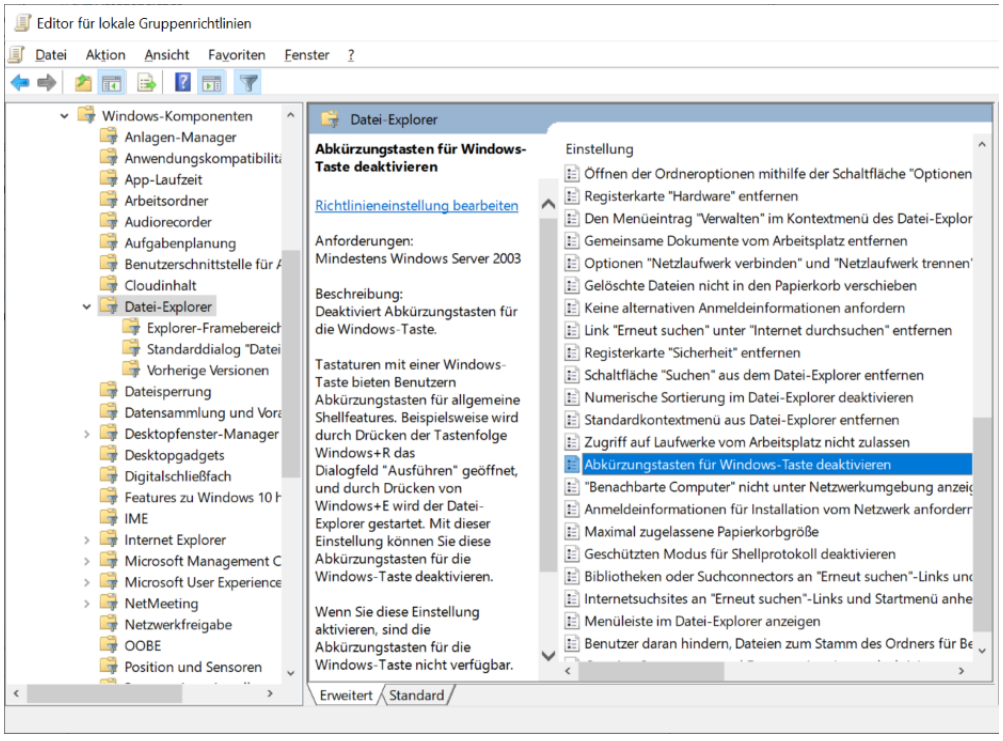
Der "Standardbenutzer" auf Betriebssystemebene sollte beim Starten jedes Servers bzw. Clients automatisch angemeldet werden.

Aktivieren der Bedienebene (Runtime)

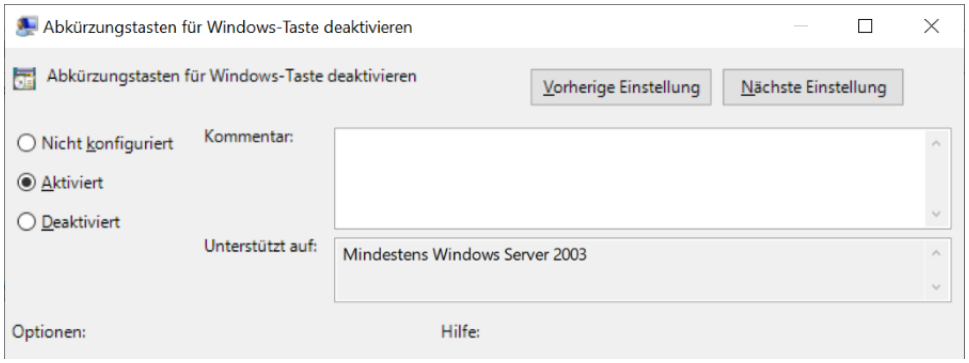
Das automatische Starten der SIMATIC PCS 7 Bedienebene (OS Runtime) ist zu aktivieren, damit kein Zugriff auf die Betriebssystemebene möglich ist.

4.5.1 Konfigurationseinstellung in Windows

Über die Verwendung von sog. Hotkeys (Abkürzungstasten) bestünde die Möglichkeit, auf die Betriebssystemoberfläche zu gelangen. Diese Option muss insbesondere für Bedienstationen deaktiviert werden. Diese Einstellung wird über die Computerrichtlinien vorgenommen.



Vorsicht: Das Deaktivieren der Abkürzungstasten muss aktiviert werden, damit sie wirksam deaktiviert sind. Siehe nachfolgender Screenshot.



4.5.2 Konfigurationseinstellung auf SIMATIC PCS 7 OS

Der Zugriff auf das Betriebssystem während der Prozessbedienung wird über die Parametereigenschaften der OS konfiguriert.

In der Benutzerverwaltung von SIMATIC PCS 7 OS ist außerdem sicherzustellen, dass die Betätigung der Schaltfläche zum Verlassen der Prozessbedienung (OS deaktivieren) nur mit entsprechender Berechtigung möglich ist.

4.5.3 Sichere Projektierung

Es sollten möglichst keine OLE-Objekte projektiert werden, da mit diesen OLE-Objekten oftmals die Möglichkeit des unerlaubten Zugriffs auf Ordner, Dateien und Programme besteht.

4.6 Informationssicherheit und Datenintegrität

Im regulierten Umfeld werden Produktionsprozesse und aufgezeichnete Daten kontrolliert und sicher aufbewahrt, um die Produktqualität nachweislich zu gewährleisten. Die sichere Handhabung von Daten ist eine Grundvoraussetzung für den vorschriftskonformen Betrieb.

Relevante Produktionsdaten und Bedieneingaben müssen gemäß nationaler und internationaler Vorschriften über viele Jahre aufbewahrt werden. Daher hat Daten- und Informationssicherheit viele Facetten, von denen einige hier erläutert werden.

Hinweis

Im System hinterlegte Standard-Passwörter müssen projektspezifisch geändert werden. Spätestens bei Übergabe des Systems müssen außerdem alle Testaccounts gelöscht werden.

Zum verbesserten Zugriffsschutz auf die WinCC Datenbanken durch Entfernen von Standardbenutzern siehe auch die Hinweise in den WinCC Installation Notes in Kapitel 1.2.2.3, Online-Support unter Beitrags-ID 109792613 (https://support.industry.siemens.com/cs/ww/de/view/109792613).

Definition einer geeigneten Systemstruktur

- Systemstruktur einschl. Benutzerverwaltung, siehe Windows-Einstellungen in den Kapiteln "Benutzerverwaltung auf Betriebssystemebene (Seite 44)", "Sicherheitseinstellungen in Windows (Seite 46)" sowie "SCALANCE S (Seite 57)".
- Planung der Datenablage sowie der Ein- und Ausgabegeräte
- Sichere Ablage sensibler Daten mit Redundanz und Zugriffskontrolle
- Einsatz von Virenscannern, siehe Kapitel "Virenscanner (Seite 40)"
- Definiertes Verhalten bei Anlauf und Betrieb der Bedienoberfläche, siehe Kapitel "Zugriffskontrolle auf Betriebssystemebene (Seite 53)"

Organisatorische Maßnahmen

- Planung und Vergabe der erforderlichen Zugriffsrechte
- Ergänzung durch Verhaltensanweisungen, z. B. Umgang mit USB-Sticks
- Arbeitsanweisungen für Archivierung, Rücklesen und evtl. Datenmigration

Betriebssystem-Einstellungen und Netzwerk-Sicherheit

Mit Hilfe von SIMATIC Security Control werden die Einstellungen im Windows-Betriebssystem konfiguriert, siehe Kapitel "SIMATIC Security Control (SSC) (Seite 57)".

Defense in Depth

Das Konzept "Defense in Depth" erfordert Maßnahmen auf verschiedenen Ebenen, um die Anlagensicherheit, die Netzwerksicherheit und die Systemintegrität herzustellen.

Die Experten der Industrial Security Services (https://www.siemens.com/global/de/home/produkte/services/industrie/digital-industry-services/industrial-security-services.html) unterstützen Sie gerne bei der Auslegung Ihres Sicherheits-Konzepts.

Siehe auch

- Umfassende Informationen zum Thema "Industrial Security", Online-Support unter Beitrags-ID 50203404 (https://support.industry.siemens.com/cs/ww/de/view/50203404)
- Handbuch "PCS 7 Kompendium Teil F – Industrial Security", Online-Support unter Beitrags-ID 109804118 (https://support.industry.siemens.com/cs/ww/de/view/109804118)

4.6.1 SIMATIC Security Control (SSC)

Der Einsatz von SIMATIC Security Control erhöht die Rechnersicherheit. Die Applikation kann zum Abschluss der SIMATIC PCS 7-Installation oder zu einem späteren Zeitpunkt ausgeführt werden. Dabei werden folgende Einstellungen funktionsspezifisch (OS-Client/-Server, ES, etc.) automatisch konfiguriert:

- Konfiguration der Windows-Firewall-Ausnahmeliste für die SIMATIC PCS 7-Kommunikation (Firewall kann eingeschaltet werden)
- DCOM-Einstellungen für SIMATIC PCS 7 (Distributed Component Object Model)
- Sicherheitsrelevante Registry-Einträge

Über den Menübefehl "Start > SIMATIC > SimaticSecurityControl" kann die Konfiguration nach der Installation jederzeit durchgeführt werden. SSC erlaubt auch die Dokumentation der im System vorgenommenen Einstellungen.

Hinweis

Wird die SIMATIC PC-Station in einer anderen Arbeitsumgebung (Domäne oder Arbeitsgruppe) aufgenommen, so muss eine erneute Konfiguration mittels SSC erfolgen.

4.6.2 SCALANCE S

Durch die zunehmende Integration der Anlagennetze in die Büronetze steigen die Sicherheits-Risiken, angefangen von Netzwerkproblemen wie z. B. die Vergabe von doppelten Netzwerkadressen über die Virenproblematik bis hin zu eventuellen Angriffen durch Cyberkriminalität.

Die Security-Module von SCALANCE S können in bestimmten Anwendungsfällen eingesetzt werden, um diesen Gefahren entgegenzuwirken. Sie bieten im Wesentlichen zwei unterschiedliche Funktionalitäten:

Firewall

Beim Einsatz einer Firewall können nur eingetragene Teilnehmer netzweit kommunizieren.

Siehe auch

- "Firewall von Industrial Security Appliance SCALANCE S", inkl. dort anhängendem Dokument, Online-Support unter Beitrags-ID 22376747 (https://support.industry.siemens.com/cs/ww/de/view/22376747)

VPN

Ein virtuelles privates Netzwerk (VPN) verbindet externe Rechner in zwei oder mehreren lokalen Netzwerken über das Internet und verschlüsselt gleichzeitig die übertragenen Daten. Mit einer VPN-Verbindung sind für externe Systeme auch sichere Remote-Zugriffe über das Internet möglich. Die SCALANCE-S-Technologie nutzt dabei das weit verbreitete IPSec-Protokoll, welches im Tunnel-Moduls (VPN-Tunnel) eine sehr hohe Sicherheit bietet.

Siehe auch

- "SIMATIC Net: VPN-Tunnel projektieren", Online-Support unter Beitrags-ID 109764618 (https://support.industry.siemens.com/cs/ww/de/view/109764618)

Hinweis

Die SCALANCE-S-Technologie bietet verschiedene Applikationen an. Weitere Informationen dazu enthalten die Handbücher der SCALANCE-Familie.

Projekteinstellungen und Definitionen 5

5.1 Projekteinrichtung

5.1.1 Multiprojekt

Das Multiprojekt-Engineering ermöglicht es, ein Projekt in mehrere Teilprojekte aufzuteilen und so mit mehreren Personen zu bearbeiten. Dazu wird im SIMATIC Manager ein übergeordnetes "Multiprojekt" definiert, das die einzelnen Projekte (AS, OS, SIMATIC BATCH) und die Stammdatenbibliothek beinhaltet. Dem Multiprojekt können Projekte hinzugefügt bzw. entnommen werden. Die Stammdatenbibliothek unterstützt dabei eine konsistente Datenhaltung innerhalb des Multiprojektes.

Hinweis

Die Nutzung der Stammdatenbibliothek zur zentralen Pflege von Messstellentypen, Einzelsteuereinheitstypen (CMT), Musterlösungen, Equipment Modul Typen (EMT), SFC-Typen und Globalen Deklarationen ist insbesondere im regulierten Umfeld zwingend erforderlich.

Der SIMATIC PCS 7 Assistent "Neues Projekt" unterstützt beim Anlegen von Projekten. Hierbei wird automatisch ein Multiprojekt angelegt. Ein neues (Teil-) Projekt kann in ein bestehendes Multiprojekt als leeres oder als vorkonfiguriertes Projekt eingefügt werden. Der anzugebende Projektname sollte zuvor bereits in der Softwarespezifikation definiert sein, denn eine nachträgliche Umbenennung des Projektes kann umständlich sein.

Beim Multiprojekt-Engineering mit SIMATIC BATCH ist ein verteiltes Engineering nur durch Einhaltung bestimmter Randbedingungen möglich, siehe hierzu nachfolgenden Beitrag im Online-Support.

Siehe auch

- Handbuch "PCS 7 Kompendium Teil A", Kapitel 5.2 "Notwendige Voreinstellungen im SIMATIC Manager" und 5.3 "Erstellen des Multiprojekts", Online-Support unter Beitrags-ID 109809015 (https://support.industry.siemens.com/cs/ww/de/view/109809015)
- "Multiprojekt-Engineering mit SIMATIC BATCH", Online-Support unter Beitrags-ID 23785345 (https://support.industry.siemens.com/cs/ww/de/view/23785345)

Bei Projekten einer Größenordnung, in der eine Aufteilung auf mehrere Multiprojekte sinnvoll erscheint, müssen die Projektstruktur und die Arbeitsweisen wohlüberlegt geplant und

dokumentiert werden. Hierbei sind die bekannten Ansprechpartner in Service und Support gerne behilflich.

Hinweis

Vor allem in größeren Projekten ist eine gute Koordination des Projektteams erforderlich. So sollten z. B. Aktionen wie Archivierungen, Kompilieren oder Downloads so terminiert werden, dass sie nicht das gesamte Team blockieren.

5.1.2 Multiprojekt- und Multiuser-Engineering

Die Konfiguration von umfangreichen Projekten kann von verschiedenen Rechnern und von verschiedenen Benutzern parallel durchgeführt werden, wobei die Benutzer unterschiedliche Ressourcen bearbeiten.

Das Multiuser-Engineering wird in einer Eigenschaft am PCS 7 OS Server aktiviert. Ein Ressourcen-Dialog gibt einen Überblick, auf welchem Rechner eine Ressource in Bearbeitung ist.

Im Gegensatz zur Remote-Projektierung über einen Projektierungs-Client müssen beim Multiuser-Engineering die Projektierungs-Clients nicht in der Rechnerliste eingetragen werden.

Beachten Sie auch die Hinweise im Handbuch "PCS 7 Engineering System" sowie in dem nachfolgend genannten Beitrag im Online-Support.

Siehe auch

- Handbuch "PCS 7 Engineering System" Kapitel 7.3, Online-Support unter Beitrags-ID 109800500 (https://support.industry.siemens.com/cs/ww/de/view/109800500)
- "Multiprojekt-/Multiuser-Engineering", Online-Support unter Beitrags-ID 22258951 (https://support.industry.siemens.com/cs/ww/de/view/22258951)

5.2 Referenzierte OS-Stationen

Der Einsatz einer "referenzierten OS-Station" bietet die Möglichkeit, eine Referenz auf eine bestehende OS-Station zu bilden. Dabei können eine oder mehrere OS-Typen als Muster konfiguriert und alle anderen OS-Stationen von diesen Mustern abgeleitet werden, ähnlich wie beim Typ-Instanz-Konzept.

Hinweis

Auf die Zuweisung eines Standardservers für den OS-Client wird an dieser Stelle nicht eingegangen. Siehe dazu Kapitel "Audit Trail PCS 7 OS (Seite 122)".

Konfigurationstypen

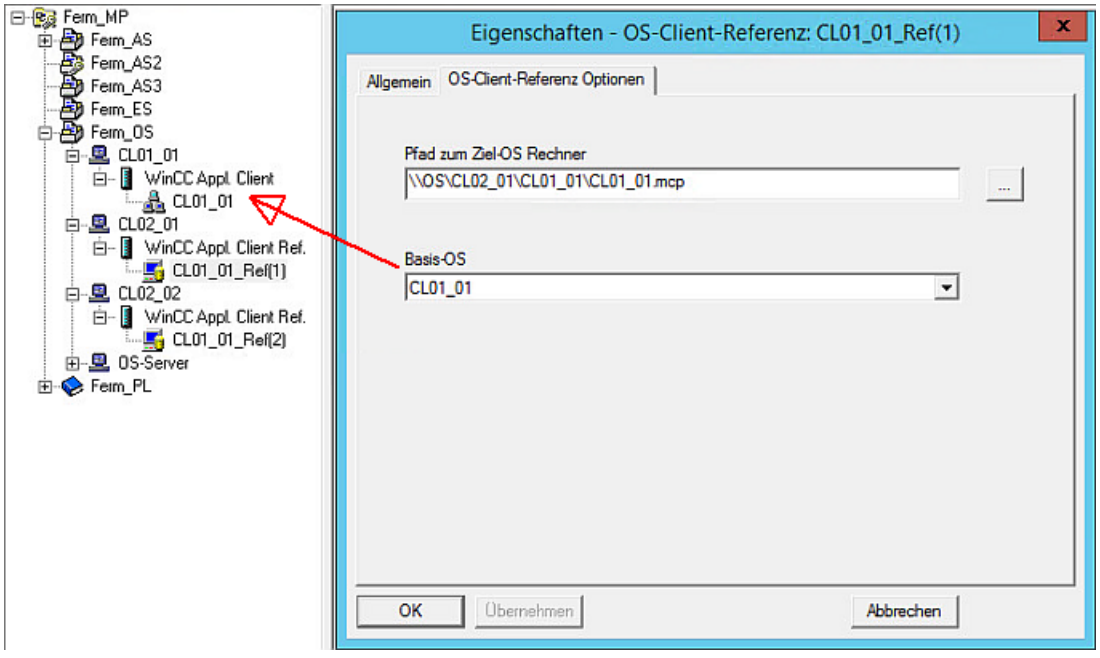
Es kann auf folgende Typen von OS-Stationen referenziert werden:

a) Referenzierte Station für OS Einzelplatz-Station (WinCC Applikation Ref.)

b) Referenzierte Station für OS-Client-Station (WinCC Applikation Client Ref.)

Softwarekonfiguration am Beispiel eines Clients

Die referenzierte OS-Client-Station benötigt als Referenz einen Standard-Multiclient. Es wird dann eine referenzierte OS-Client-Station in das Projekt eingefügt und in den Objekteigenschaften die "Basis OS" angegeben (siehe Abbildung). Die Anzahl der möglichen referenzierten OS-Client-Stationen ist durch die von SIMATIC PCS 7 vorgegebene maximale Anzahl an Bedienplätzen begrenzt.



Hinweis

Wird die Referenzstation geändert, so müssen alle OS-Stationen, die auf die Referenzstation verweisen, geladen werden.

Vorteile beim Einsatz von referenzierten Stationen

Referenzierte Stationen helfen Fehler und Arbeitsaufwand zu minimieren. Es muss lediglich die Referenzstation ausführlich gegen ihre Spezifikation getestet werden. Bezüglich der referenzierten Stationen müssen nur noch Besonderheiten in der Konfiguration wie z. B. Bildschirmauflösungen, PCS 7 OS Client-spezifische Arbeitsbereiche oder Benutzerrechte betrachtet sowie allgemeine Funktionstests durchgeführt werden.

5.3 Verwendung der Stammdatenbibliothek

SIMATIC PCS 7 bietet für die Erzeugung mehrerer gleicher Funktionen die Möglichkeit der Vervielfältigung auf Basis einer definierten Software-Vorgabe. Dies ist jedoch nur in der Verbindung mit der Stammdatenbibliothek möglich, die neben den Ordnern für Typen und Musterlösungen auch den Ordner für Globale Deklarationen (Einheiten, Aufzählungen und Ausrüstungseigenschaften) sowie OS-Bilder und OS-Reports enthält.

Auf Basis der verwendeten Bibliotheken (PCS 7-Standardbibliothek, Advanced Process Library APL, etc.) werden die Projekt-Typicals erstellt und in der Stammdatenbibliothek abgelegt und verwaltet. Die PCS 7 Standardbibliotheken enthalten bereits Templates, welche genutzt werden können. Auch Musterlösungen für Technische Einrichtungen und komplette Units können als Vorlage in der Stammdatenbibliothek abgelegt und hierüber vervielfältigt werden.

Hinweis

Die Module und Typicals sollten vor der Instanziierung in einem Modultest verifiziert und vom Kunden genehmigt werden.

In allen Projekten eines Multiprojektes sollten nicht nur die gleichen Versionen von Bausteinen, SFC-Typen und Typicals verwendet werden, sondern auch die gleiche Technologische Hierarchie und die gleichen Globalen Deklarationen zugrunde liegen. Dazu sind die einzelnen Projekte mit der Stammdatenbibliothek abzugleichen.

Hinweis

Mit Hilfe von SIMATIC Version Trail können Versionen der Stammdatenbibliothek im Projektverlauf übersichtlich archiviert und organisiert werden.

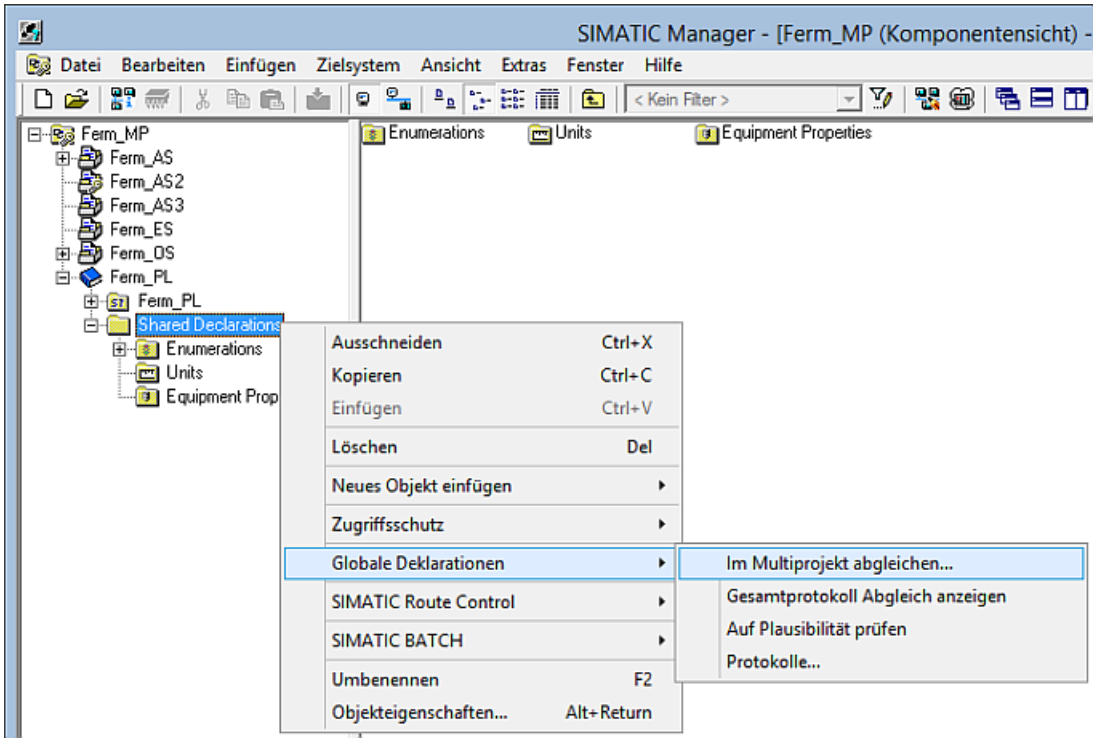
Die Bausteine, Typen und globalen Deklarationen sind die kleinsten Module der Anwendersoftware. Diese werden bei der Projektierung als Erstes erzeugt und freigegeben, bevor sie über die IEA-Schnittstelle oder manuell vervielfältigt werden, siehe hierzu auch Kapitel "Bulk Engineering mit dem IEA (Seite 92)" sowie Kapitel "Typ-Instanz-Konzept mit dem PAA (Seite 94)".

Siehe auch

- Handbuch "PCS 7 Kompendium Teil A", Kapitel 8.2.1 "Messstellentyp" und 8.2.2 "CMT", Online-Support unter Beitrags-ID 109809015 (https://support.industry.siemens.com/cs/ww/de/view/109809015)

5.3.1 Abgleich der Globalen Deklarationen

Die Globalen Deklarationen werden beim Anlegen des Multiprojektes automatisch in der Stammdatenbibliothek erzeugt. Damit diese in allen Projekten zur Verfügung stehen, können diese abgeglichen werden. Zur Gewährleistung der multiprojektweiten Konsistenz wird die zentrale Pflege in der Stammdatenbibliothek dringend empfohlen.

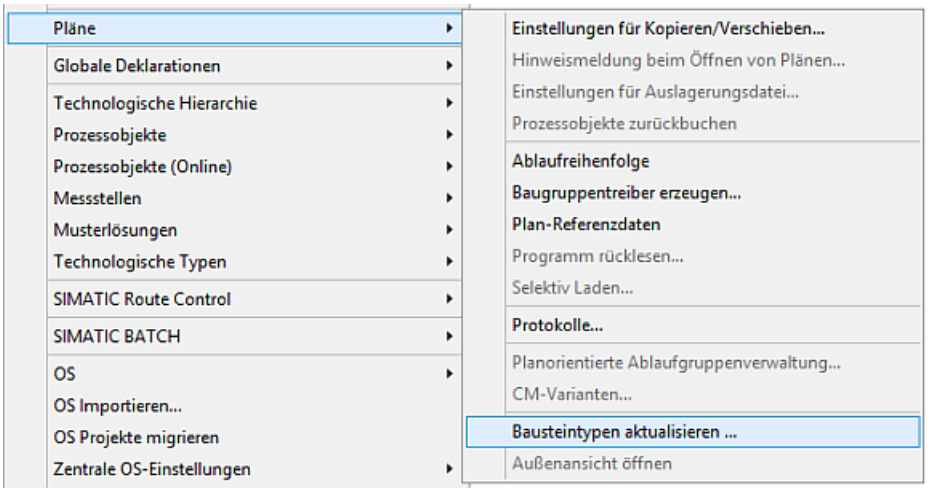


5.3.2 Abgleich von Vorlagentypen

Zur Sicherung der Datenkonsistenz werden Vorlagentypen (Bausteine, CFC, SFC, etc.) in der Stammdatenbibliothek erstellt und gepflegt. Damit die in den Projekten verwendeten Instanzen den aktuellen Vorlagentypen aus der Stammdatenbibliothek entsprechen, können diese miteinander abgeglichen werden.

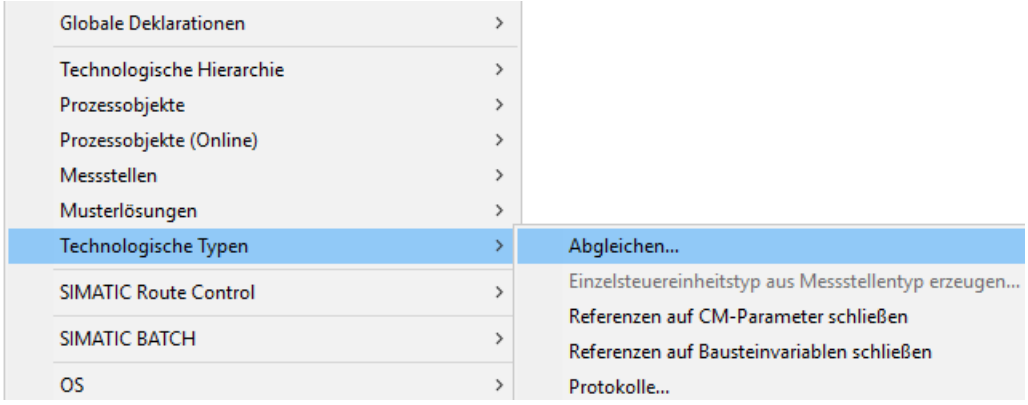
Vor dem Abgleich können die Unterschiede durch einen Versionenvergleich geprüft werden.

Wählen Sie zur Aktualisierung der Bausteintypen und SFC-Typen bei markiertem Bausteinordner oder einem markierten Baustein in der Stammdatenbibliothek die Funktion "Extras > Pläne > Bausteintypen aktualisieren ...".



Für Messstellentypen und Musterlösungen stehen zur zentralen Änderung der Ableger die Assistenten „Messstellentypen erstellen/ändern“ und „Musterlösungen erstellen/ändern“ zur Verfügung.

Den Abgleich für Einzelsteuereinheitstypen (CMs bzw. CMTs) starten Sie über das Kontextmenü "Technologische Typen > Abgleichen..." in der Technologischen Sicht des Projekts.



Siehe auch

- Handbuch "PCS 7 Engineering System" Kapitel 7.4, Online-Support unter Beitrags-ID 109800500 (https://support.industry.siemens.com/cs/ww/de/view/109800500)
- Handbuch "PCS 7 Kompendium Teil A", Kapitel 8.1.6 "Bausteintypen aktualisieren", Online-Support unter Beitrags-ID 109809015 (https://support.industry.siemens.com/cs/ww/de/view/109809015)
- Handbuch "Synchronisieren von Einzelsteuereinheitstypen", Online-Support unter Beitrags-ID 109758382 (https://support.industry.siemens.com/cs/ww/de/view/109758382)

5.3.3 Abgleich der Technologischen Hierarchie

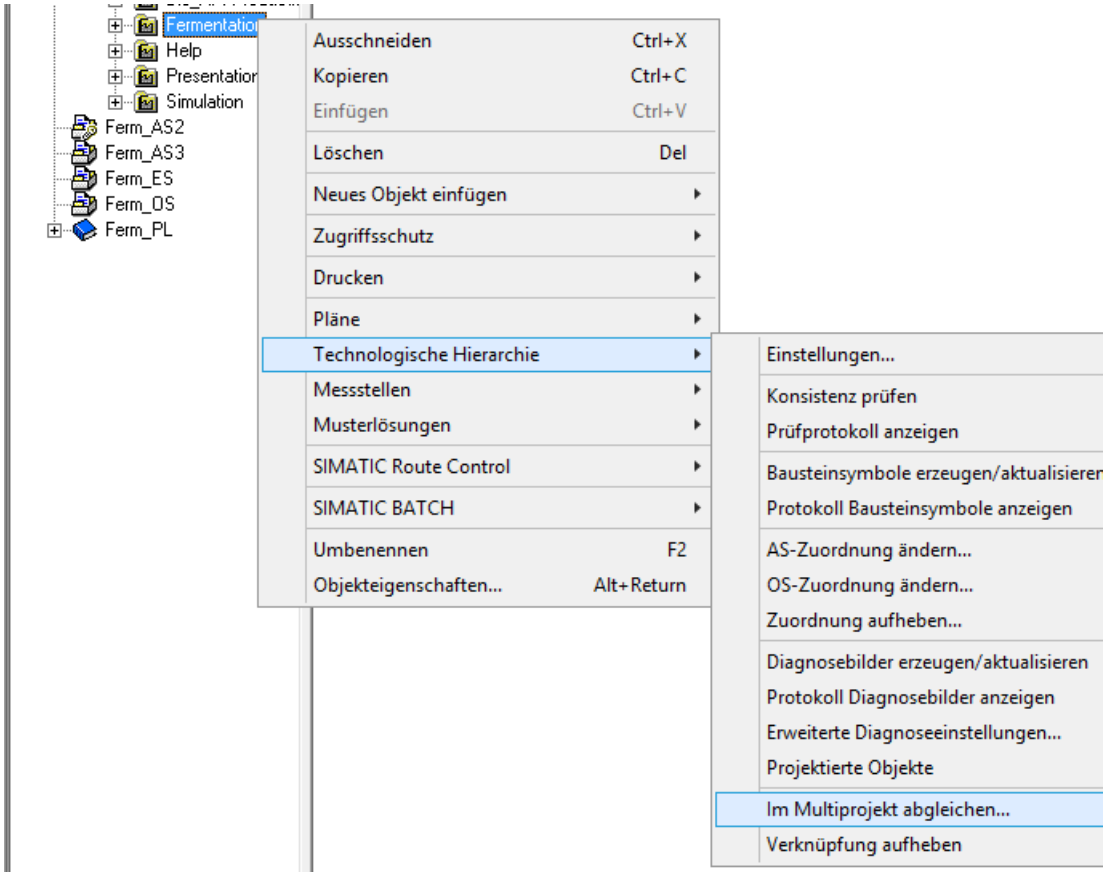
Für die Projektierung stehen in SIMATIC PCS 7 vier Sichtweisen zur Verfügung:

- Komponentensicht zur Konfiguration der Hardware
- Technologische Sicht zur Aufteilung der verfahrenstechnischen Hierarchie
- Prozessobjektsicht für die zentrale Bearbeitung von Parametern, Signalen, Meldungen, Bildobjekten, Archivvariablen, etc.
- Technologischer Listeneditor für das Engineering von Parametern, Signalen über Import/ Export unter Verwendung von Microsoft Excel

Es wird empfohlen, dass die Technologische Hierarchie (TH) in allen Projekten eines Multiprojektes gleich aufgebaut ist. Dazu legt man die TH in einem Projekt an (Empfehlung: OS Projekt) und überträgt diese Struktur an alle Projekte des Multiprojektes. Hierbei werden auch die Globalen Deklarationen des Vorlagenprojektes auf die ausgewählten Projekte übertragen. Dabei entsteht eine Verbindung zwischen den Hierarchieordnern.

Siehe auch

- Handbuch "PCS 7 Kompendium Teil A", Kapitel 5.6 "Anlegen der Technologischen Hierarchie", Online-Support unter Beitrags-ID 109809015 (https://support.industry.siemens.com/cs/ww/de/view/109809015)



Hinweis

Das Vorlagenprojekt erhält eine Art Masterrolle, d. h. Namensänderungen der erzeugten Hierarchieordner sind nur zentral in der Vorlage möglich. Namensänderungen in den Ablegern sind nur nach Aufhebung dieser Verbindung erlaubt.

5.4 SIMATIC NET

5.4.1 Projektierung von SIMATIC NET

SIMATIC NET spiegelt die im Projekt verwendeten Netzübergänge wieder. Bei der Konfiguration müssen die in der Spezifikation beschriebenen SIMATIC NET Netzwerkadressen und Einstellungen für AS, OS, dezentrale Peripherie, etc. verwendet werden. Dies ist später im Rahmen der Tests (z. B. FAT, IQ) zu verifizieren.

Die Konfiguration der Netzübergänge wird mit dem Verfahren "Advanced PC Configuration" durchgeführt. Unter Windows können von einer zentralen Engineering Station aus alle Automatisierungsstationen (AS) und Operator-Stationen (OS) projektiert und die Konfigurationsdateien geladen werden.

Im Einzelnen werden die folgenden Verbindungen projektiert:

- AS – OS Verbindungen
- AS – AS Verbindungen
- ES – AS Verbindungen
- Remote-I/O Verbindungen

Diese Verbindungen können auch hochverfügbar ausgeführt werden.

Weitere Informationen sind in der Dokumentation von SIMATIC NET enthalten.

5.4.2 Anlagenbus und Terminalbus

Industrial Ethernet bietet ein umfangreiches Spektrum von Netzwerkkomponenten für die elektrische und optische Übertragungstechnik. In SIMATIC PCS 7 unterscheidet man zwischen Anlagenbus und Terminalbus. Um höhere Sicherheit und Leistung sicherstellen zu können, wird der getrennte Aufbau dieser beiden Busse empfohlen.

Für den Anlagenbus wird Industrial Ethernet eingesetzt. Über den Anlagenbus sind die Automatisierungsstationen mit den OS-Servern und der Engineering Station verbunden.

Über den Terminalbus sind die PCS 7-Server mit den Clients, Archiv-Servern und übergeordneten MES-Systemen verbunden.

Siehe auch

- Handbuch "PCS 7 Kompendium Teil A", Kapitel 4.3.6 "Terminalbus konfigurieren" bzw. Kapitel 4.3.7 "Anlagenbus konfigurieren", Online-Support unter Beitrags-ID 109809015 (https://support.industry.siemens.com/cs/ww/de/view/109809015)

5.4.3 PROFIBUS

Eine Voraussetzung für den störungsfreien Anlagenbetrieb ist eine zuverlässige Kommunikation zur Feldebene. Grundlage hierfür ist ein leistungsfähiges Echtzeit-Bussystem wie der PROFIBUS mit den Ausführungen DP und PA.

Siehe auch

- Handbuch "SIMATIC NET PROFIBUS Netzhandbuch", Online-Support unter Beitrags-ID 35222591 (https://support.industry.siemens.com/cs/ww/de/view/35222591)
- Handbuch "PCS 7 Engineering System" Kapitel 4.6.7, Online-Support unter Beitrags-ID 109800500 (https://support.industry.siemens.com/cs/ww/de/view/109800500)
- Handbuch "PCS 7 Kompendium Teil A", Kapitel 6.4 "Einstellungen für CP 443-5 Ext als Profibus-Master", Online-Support unter Beitrags-ID 109809015 (https://support.industry.siemens.com/cs/ww/de/view/109809015)

Hinweis

Die Konfiguration der Profibusgeräte/-kommunikation ist integriert in das Gesamtprojekt im SIMATIC Manager. Ein Backup des Engineering-Projektes beinhaltet somit die komplette Anwender-Software. Dies hat entsprechende Vorteile bei der regelmäßigen Datensicherung sowie bei der Überprüfung der Software im Rahmen der Testphasen.

PROFIBUS DP

Remote I/O Stationen wie ET 200 können über elektrische oder optische Profibus DP-Netze in einfacher Ausführung oder auch redundant realisiert werden.

Mit Hilfe eines Trennübertragers (RS485iS Koppler) als Barriere und der eigensicheren ET 200iSP kann der Profibus DP gemäß Betriebsanleitung zur ET 200iSP auch im explosionsgefährdeten Bereich betrieben werden. Damit sind auch im Ex-Bereich Übertragungsraten bis 1,5 Mbit/s möglich.

Komplexe Prozessperipheriegeräte können mit Hilfe von vorgefertigten Add-on-Bausteinen in PCS 7 angebunden werden, wie z. B.

- Motormanagement-System SIMOCODE pro
- Frequenzumrichter MICROMASTER 4
- Wägesystem SIWAREX

Des Weiteren stehen zur Verfügung:

- Funktionsbaugruppen (z. B. Regler, Motor-Starter etc.)
- HART-Baugruppen (zur Anbindung von HART-Feldgeräten)

- F-Baugruppen (für fehlersichere Anwendungen)
- Ex-Baugruppen (Anschluss von Aktoren / Sensoren aus den Ex-Zone)

HART-Baugruppen können über PDM konfiguriert werden, siehe Kapitel "SIMATIC PDM (Seite 69)".

PROFIBUS PA

Auch der Profibus PA kann einfach oder höher verfügbar realisiert werden. Für einen redundanten Aufbau bietet sich hier die Ringtopologie an. Der Profibus PA kann über entsprechende Geräte (Ex-Koppler oder AFDiS(D)) ebenso als eigensicherer Bus ausgeführt werden. Hierdurch können Geräte aus den Ex-Zonen angeschlossen werden. Der AFDiSD zeichnet sich zusätzlich durch seine erweiterte Diagnosefähigkeit wie Signal Level, Jitter etc. gemäß NAMUR NE107 "Selbstüberwachung und Diagnose von Feldgeräten" für Haupt- und Stichleitungen aus.

Siehe auch

- Handbuch "Buskopplungen DP/PA-Koppler, DP/PA-Link und Y-Link", Online-Support unter Beitrags-ID 109805389 (https://support.industry.siemens.com/cs/ww/de/view/109805389)

Hinweis

Der DP/PA-Koppler FDC 157-0 ist vollständig in das anlagennahe Asset Management von PCS 7 integriert, wenn er als Diagnoseslave projektiert wurde.

5.4.4 PROFINET

Profinet IO ist ein herstellerunabhängiger Standard (IEC 61158-5-10) und ist im Rahmen von Totally Integrated Automation (TIA) die konsequente Zusammenführung und Erweiterung des Standards Profibus DP, dem etablierten Feldbus und Industrial Ethernet. PROFINET steht wie PROFIBUS für höchste Transparenz, offene IT-Kommunikation, Netzwerksicherheit sowie Echtzeitkommunikation bis in die Feldebene.

Siehe auch

- Handbuch "SIMATIC NET / PROFINET", Online-Support unter Beitrags-ID 27069465 (https://support.industry.siemens.com/cs/ww/de/view/27069465)
- Handbuch "PCS 7 Engineering System" Kapitel 4.6.8, Online-Support unter Beitrags-ID 109800500 (https://support.industry.siemens.com/cs/ww/de/view/109800500)

Profinet Remote-I/O Stationen wie die ET200M können über elektrische oder optische Ethernet Netze in einfacher Ausführung realisiert werden. Zusätzlich besteht die Möglichkeit, Profibus DP und Profibus PA Geräte über einen Proxy zu integrieren.

Nachfolgende Eigenschaften erfüllt PROFINET:

- Übertragung zeitkritischer Daten in garantierten Zeitintervallen
- Deterministisches System: Genaue Vorhersage bzgl. des Übertragungszeitpunktes

- Reibungslose Kommunikation über andere Standard-Protokolle im gleichen Netz
- Erhöhte Verfügbarkeit durch Medienredundanz (MRP)

Die nachfolgende Tabelle stellt PROFIBUS und PROFINET gegenüber:

	PROFIBUS	**PROFINET**
Übertragungsgeschwindigkeit	12Mbit/s	100Mbit/s
Zykluszeit	Min 300 µs	Min 31,25µs
Jitter	<1µs	<1µs
Nutzdaten pro Device (Slave)	244 Byte	64kByte (intern) 8kByte (extern)
Anzahl Devices / Schnittstellen	125	250 intern 128 extern
Anzahl Devices / Träger	1625 3 Onboard IF+10 CPs	768 1 Onboard IF+4 CPs
Konsistente Nutzdaten	244 Intern 128 extern	1440 intern 240 extern
E/A Adressraum	8kByte intern 8kByte extern	8kByte intern 4kByte extern

Die Vorteile für den Anwender von Profinet ist das Zusammenführen von Profibus und Ethernet zu einem standardisierten und flexiblen Gesamtkonzept.

5.4.5 SIMATIC PDM

SIMATIC PDM (Process Device Manager) ist ein Software-Paket zur Projektierung, Parametrierung, Inbetriebnahme und Wartung von Geräten (z. B. Messumformern). Es ermöglicht u. a. eine einfache Beobachtung der Prozesswerte und Alarme sowie Zustandsinformationen des Geräts. Außerdem wird die Inbetriebnahme und Wartung durch die Lifelist-Funktionalität unterstützt, wodurch Feldgeräte online am Bus erkannt und adressiert werden können.

Die Module und Feldgeräte können durch den Projektadministrator mit einem Schreibschutz versehen werden. Dadurch wird ein unbeabsichtigtes Verändern der Geräteparametrierung nach der Messstellenabnahme verhindert.

Zusätzlich können Module und Feldgeräte mit der Kennung „Gerät geprüft" gekennzeichnet werden. Durch diese Kennung kann der Arbeitsfortschritt schnell und einfach ermittelt werden.

Das Setzen des Schreibschutzes sowie der Kennung „Gerät geprüft" wird mit Datum und Uhrzeit hinterlegt.

Hinweis

Mit dem PDM "Änderungslogbuch (Change Log)" können Änderungen an Feldgerätkonfigurationen nachvollzogen werden. Diese Funktion ist standardmäßig deaktiviert und sollte unter den PDM Projekteinstellungen aktiviert werden.

Bei Verwendung der PDM Server-/Client- Funktionalität, welche eine anlagenweite Geräteliste per Webzugriff bereitstellt, wird eine verschlüsselte SSL Verbindung dringend empfohlen. Zusätzlich sind die Bedienberechtigungen, wie „Schreiben in das Gerät", auf das Notwendigste zu beschränken.

Electronic Device Description (EDD)

Die Basis für die Geräteintegration ist die EDD. Sie wird vom Gerätehersteller mitgeliefert, im Internet zur Verfügung gestellt oder in Gerätekataloge von EDD-Applikationen integriert.

SIMATIC PDM ist vollständig in PCS 7 integriert. Von einer zentralen Engineeringstation aus können sämtliche EDD integrierten Geräte eines Projektes durch ein einheitliches Tool parametriert, in Betrieb genommen und gewartet werden.

Hinweis

Bei der Auswahl der Geräte ist zu beachten, dass EDDs in PDM integriert werden müssen. PDM wird mit einer Bibliothek der bereits integrierten Gerätebeschreibungen ausgeliefert. Eine Auflistung der in der "SIMATIC PDM Device Library" integrierten EDDs, für die jeweilige Version, kann im Online-Support unter Beitrags-ID 109748100 (https://support.industry.siemens.com/cs/ww/de/view/109748100) abgerufen werden.

Die Integration von in dieser Bibliothek nicht enthaltenen EDDs kann kostspielig und in einigen Fällen sogar gar nicht möglich sein. Grundsätzlich ist darüber hinaus ein Integrationstest der Feldgeräte vor der Endauswahl sinnvoll.

Exportfunktionen in SIMATIC PDM

Über einen Export bietet SIMATIC PDM die Möglichkeit, u. a. folgende Daten eines oder mehrerer Feldgeräte zu sichern:

- Geräteparameter
- Änderungslogbuch, Änderungen objektweise sortiert
- Kalibrierprotokoll, beinhaltet relevante Informationen zur Inbetriebsetzung und Wartung sowie Prüfergebnisse

Hinweis

Eine Versionsinformation kann im Kommentarfeld des Gerätes hinterlegt werden. Diese wird gemeinsam mit den Gerätedaten exportiert. Zusätzlich kann eine Versionskennung über die Namensgebung der Exportdatei erfolgen.

Da die Exportdatei einen Verweis auf eine passende Transformationsdatei enthält, wird der Inhalt der Exportdatei im Webbrowser in HTML-Form leicht lesbar dargestellt. Die entsprechende Transformationsdatei ("PDMExportEddl.XSL" für Geräteparameter und Änderungslogbuch bzw. "PDMExportCalibration.XSL" für Kalibrierprotokoll) wird beim Export in den Pfad der Exportdatei kopiert.

Hinweis

Wenn die Exportdatei in ein anderes Verzeichnis oder auf einen anderen Rechner kopiert wird und die HTML-Darstellung genutzt werden soll, muss die entsprechende Transformationsdatei ebenfalls kopiert werden.

5.5 OS-Projekteditor

Der OS-Projekteditor in SIMATIC PCS 7 dient als Basis-Tool für das Einrichten der Bedienoberfläche, also z. B. zum Einstellen von Bildschirmaufteilung, Bildschirmauflösung, etc.

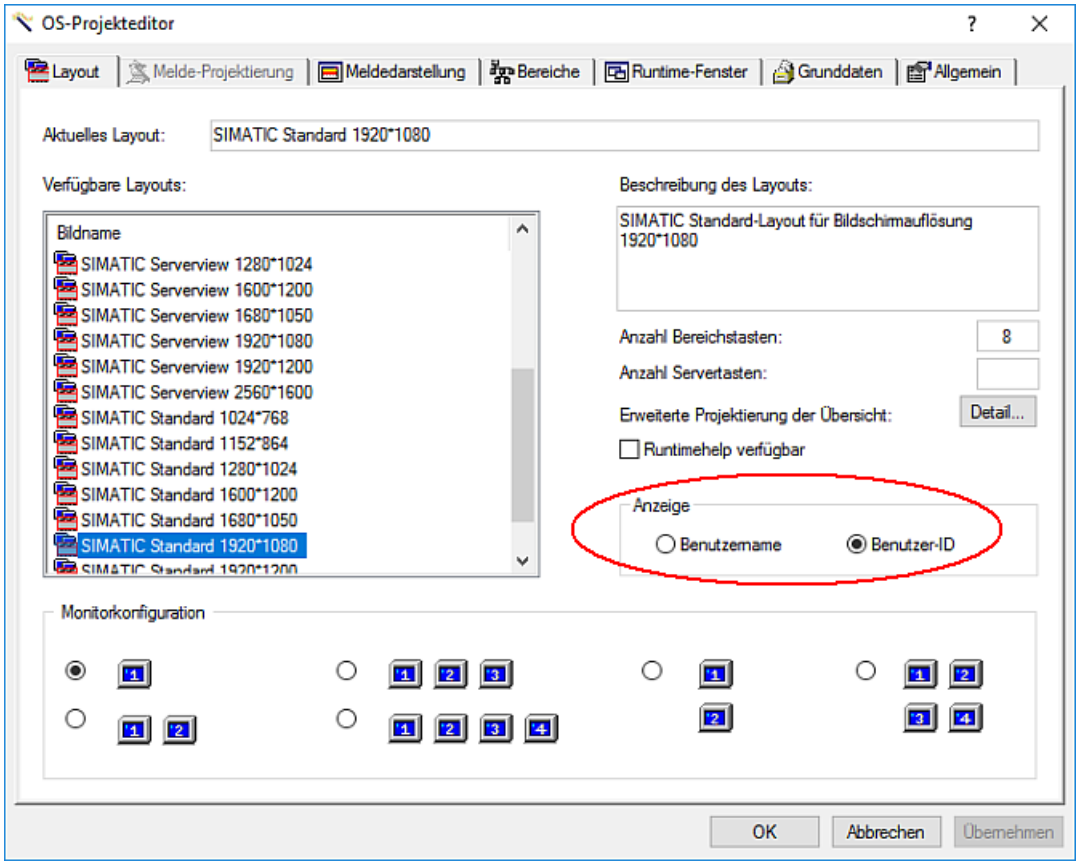
Beim Anlegen eines OS-Projektes in der SIMATIC PCS 7 ES wird der OS-Projekteditor mit den Default-Einstellungen initialisiert.

Viele dieser Default-Einstellungen können und sollten in Projekten so belassen werden. Abweichungen davon müssen dokumentiert sein und bedürfen besonderer Beachtung bei jedem Update des Systems.

Einige Einstellungen sind immer projektspezifisch. Diese sowie Änderungen auf Grund von Kundenanforderungen werden in der Spezifikation definiert.

Siehe auch

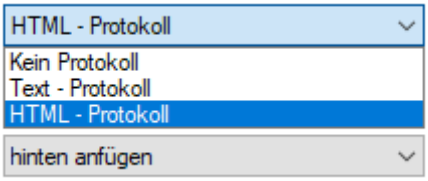
- Handbuch "PCS 7 Operator Station", Online-Support unter Beitrags-ID 109794374 (https://support.industry.siemens.com/cs/ww/de/view/109794374)
- Handbuch "PCS 7 Kompendium Teil A", Kapitel 10.1.4 "Arbeiten mit dem OS-Projekteditor", Online-Support unter Beitrags-ID 109809015 (https://support.industry.siemens.com/cs/ww/de/view/109809015)



Die obige Grafik zeigt den Aufbau des OS-Projekteditors. Darin wird z. B. auch festgelegt, ob auf der Bedienoberfläche der "Benutzername" oder die "Benutzer-ID" angezeigt wird.

- In der Registerlasche "Layout" wird die Darstellung des Layouts in Runtime konfiguriert. Hierzu zählen die Bildschirmformate, Anzahl an Monitore pro OS-Station sowie die Anzeige des Benutzernamens oder der Benutzer-ID in Runtime.
- In der Registerlasche "Melde-Projektierung" werden Meldeklassen, Meldearten, Meldeblöcke und die PCS 7 Standard Meldungen konfiguriert.
- In der Registerlasche "Meldedarstellung" wird das Meldeverhalten konfiguriert. Hierzu zählt die Darstellung von Meldungen in den Meldeseiten und den Sammelanzeigen, die Meldefilter sowie das Smart Alarm Hiding.
- Unter "Bereiche" wird die Darstellung von Bereichs- und Servertasten (z. B. Anlage, Teilanlage, Funktionen etc.) für den Übersichtsbereich konfiguriert.
- In der Registerlasche "Runtime-Fenster" wird die Anzahl und Anordnung von Bildfenstern konfiguriert. In den Bildfenstern werden die Bilder (Graphics) und Bildbausteine (Faceplates) in der Runtime geöffnet.

- In der Registerlasche "Grunddaten" wird festgelegt, welche geänderten Dateien des Projektes durch Dateien des Lieferzustandes überschrieben werden. Jedoch ist bei dieser Konfigurationsänderung zu beachten, dass der konsistente Runtime-Betrieb immer sichergestellt werden muss.
- Die Registerlasche "Allgemein" enthält die Einstellungen zum OS-Projekteditor. Damit eine durchgängige Protokollierung der Änderungen gewährleistet ist, sollte unter „Verhalten, wenn Protokolldatei bereits existiert" die Option „hinten anfügen" gewählt werden. Das Protokoll kann in den Datei-Formaten HTML oder Text abgelegt werden.



5.6 Uhrzeitsynchronisation

Die Uhrzeitsynchronisation spielt bei automatisierten Systemen im GMP-Umfeld eine wichtige Rolle. Beim Zusammenspiel von mehreren Automatisierungs- (AS) und/oder Bedienstationen (OS) kommt es darauf an, dass die Archivierung von Meldungen, Alarmen, Trends und Audit Trail-Daten mit synchronisierten Zeitstempeln erfolgt.

In SIMATIC PCS 7 entspricht die gesendete Uhrzeit auf den Bussen standardmäßig immer der normierten Weltuhrzeit UTC (Universal Time Coordinated).

Die Zeitstempel werden in UTC erzeugt und im Archiv des OS-Servers abgelegt. Im Anlagenbetrieb werden alle im Archiv abgelegten Prozessdaten (Meldungen und Trends) von UTC ausgehend in die im Windows-System eingestellte Zeitzone (unter Berücksichtigung der Sommer-/Winterzeiteinstellung) umgerechnet dargestellt.

Das Aktivieren der Uhrzeitsynchronisation in SIMATIC PCS 7 bedeutet, dass ein aktiver Uhrzeit-Master die Synchronisation aller OS-Server, Bedienstationen, Automatisierungsstationen und der Engineering Station übernimmt. Für die zeitliche Synchronität müssen alle zum System gehörenden Stationen synchronisiert werden, so dass anlagenweit eine zeitfolgerichtige Meldeverarbeitung (Archivierung von Trends, Meldungen, Redundanzabgleich von Servern) ermöglicht wird.

Uhrzeitsynchronisation in einer Windows-Arbeitsgruppe

In einer Arbeitsgruppen-Umgebung kann der Anlagenbus über eine zentrale Anlagenuhr synchronisiert werden. Die OS-Server erhalten die Uhrzeit über den Anlagenbus; sie werden als sogenannte kooperative Uhrzeit-Master projektiert. Wenn der Zeitgeber ausfällt, wird ein OS-Server aktiver Uhrzeit-Master. Die Automatisierungsstationen erhalten die Uhrzeit vom zentralen Zeitmaster; sie sind als Uhrzeit-Slaves projektiert. Die OS-Clients erhalten die Uhrzeit von einem OS-Server; sie erhalten nur von solchen OS-Servern die Uhrzeit, von denen sie auch die Serverdaten geladen haben.

Uhrzeitsynchronisation in einer Windows-Domäne

Wird das Automatisierungssystem in einer Windows-Domäne betrieben, dient der primäre Domänencontroller als Uhrzeit-Master am Terminalbus. Er erhält seine Zeit von einem seriell angeschlossenen zentralen Zeitmaster. Die OS-Server erhalten von diesem Domänencontroller die Uhrzeit über den Terminalbus. Die OS-Clients erhalten die Uhrzeit von einem ausgewählten OS-Server. Der Anlagenbus und damit die angeschlossenen Automatisierungsstationen (AS) werden ebenfalls von diesem OS-Server synchronisiert (der zuerst in den Prozessbetrieb genommene Server). Er wird damit zum aktiven Uhrzeit-Master.

Bei erhöhten Anforderungen an die Zeitstempelung müssen die ASen zusätzlich direkt von einem zentralen Zeitmaster über den Anlagenbus synchronisiert werden.

Wenn in der Anlage Komponenten wie z. B. SIMATIC BATCH-Server zum Einsatz kommen, auf denen keine Operator Station installiert ist, müssen diese zusätzlich synchronisiert werden. Dies kann über einen zusätzlichen DCF77-Dienst (zentraler Zeitmaster) oder GPS-Dienst sowie mit Hilfe einer Software per Netzwerk oder Internet erfolgen.

Uhrzeitsynchronisation für Package Units

In vielen PCS 7–Umgebungen werden Package Units mit eingebunden. Diese Package Units können über das standardisierte Network Time Protocol (NTP) die Uhrzeit von der Windows-Domäne erhalten. Des Weiteren besteht die Möglichkeit die Uhrzeit von einem Siemens Automatisierungssystem zu einem anderen Siemens Automatisierungssystem via S7-Protokoll zu übertragen.

Hinweis

Es muss darauf geachtet werden, dass die automatische Sommer- / Winterzeitumstellung im Betriebssystem korrekt eingestellt ist.

Wenn als Zeitgeber ein zentraler Zeitmaster verwendet und die Anzeige an der Operator-Station auf Sommerzeit umgestellt wird, muss auch der zentrale Zeitmaster auf Sommerzeit parametriert werden, damit alle Meldungen mit korrekten Zeitstempeln archiviert werden. Diese Umstellung ist auf der Operator-Station unter Systemsteuerung / Datum und Uhrzeit / Zeitzone zu aktivieren.

Siehe auch

- Handbuch "PCS 7 Uhrzeitsynchronisation", Online-Support unter Beitrags-ID 109794383 (https://support.industry.siemens.com/cs/ww/de/view/109794383)
- Handbuch "PCS 7 Engineering System", Kapitel 9.9.5.2 "Einstellen der Uhrzeitsynchronisation", Online-Support unter Beitrags-ID 109800500 (https://support.industry.siemens.com/cs/ww/de/view/109800500)
- Handbuch "PCS 7 Operator Station", Kapitel 13 "Uhrzeitsynchronisation", Online-Support unter Beitrags-ID 109794374 (https://support.industry.siemens.com/cs/ww/de/view/109794374)
- Handbuch "PCS 7 Kompendium Teil A", Kapitel 10.1.7 "Uhrzeitsynchronisation", Online-Support unter Beitrags-ID 109809015 (https://support.industry.siemens.com/cs/ww/de/view/109809015)
- Handbuch "Sicherheitskonzept PCS 7 und WinCC", Online-Support unter Beitrags-ID 109780811 (https://support.industry.siemens.com/cs/ww/de/view/109780811)

- Handbuch "Industrial Ethernet Security", Online-Support unter Beitrags-ID 109751632 (https://support.industry.siemens.com/cs/ww/de/view/109751632)
- FAQ "Uhrzeitsynchronisation mit DCF77", Online-Support unter Beitrags-ID 19693801 (https://support.industry.siemens.com/cs/ww/de/view/19693801)
- FAQ "Uhrzeitsynchronisation in Windows-Domänen", Online-Support unter Beitrags-ID 16620294 (https://support.industry.siemens.com/cs/ww/de/view/16620294)
- FAQ "Einstellungen bei der Uhrzeitsynchronisation", Online-Support unter Beitrags-ID 16622902 (https://support.industry.siemens.com/cs/ww/de/view/16622902)
- FDA-Guidance 21 CFR Part 11 – Time Stamps, 2002, withdrawn (zurückgezogen)

5.7 Konfigurationsmanagement

Die Konfiguration eines Computersystems besteht aus verschiedenen Komponenten an Hardware und Software; diese können unterschiedlich komplex sein und von käuflichen **Standardkomponenten** bis hin zu speziell zugeschnittenen **Anwenderkomponenten** reichen. Die aktuelle Systemkonfiguration sollte jederzeit vollständig und übersichtlich verfügbar sein. Hierzu wird das System in Konfigurationselemente unterteilt, welche mit Hilfe einer eindeutigen Bezeichnung und einer Versionsnummer identifizierbar und von der Vorversion unterscheidbar sind.

Definition der Konfigurationselemente

Bei der Hardware werden überwiegend Standardkomponenten eingesetzt, die mit Typbezeichnung, Versionsnummer etc. definiert und dokumentiert werden. Beim Einsatz von kundenspezifischer Hardware ist ein höherer Aufwand erforderlich, siehe hierzu Kapitel "Auswahl und Spezifikation der Hardware (Seite 26)".

Bei der Software kommen zumindest teilweise solche "Standardkomponenten" zum Einsatz, z. B. die Systemsoftware SIMATIC PCS 7, deren Bibliotheken und Optionen. Diese werden ebenso wie bei der Hardware mit Bezeichnung, Versionsnummer etc. definiert und dokumentiert.

Die Applikationssoftware wird auf Basis der Standardsoftware konfiguriert bzw. programmiert. In welche einzelnen Konfigurationselemente die Anwendersoftware zu unterteilen ist, kann wegen unterschiedlicher Kundenanforderungen und Systemausprägungen nicht pauschal definiert werden.

Versionierung der Konfigurationselemente

Während die Versionsbezeichnung der Standardsoftware vom Anwender / Projektierer nicht beeinflussbar ist, müssen für die Projektierung der Applikationssoftware in Arbeitsanweisungen u. a. die Vergabe von Versionsnummern und ein Verfahren für die Änderungskontrolle (Change Control) festgelegt werden. Ab Beginn der Systemerstellung sollten alle Konfigurationselemente übersichtlich gepflegt werden.

Hinweis

Beispiele, wie einzelne Software-Elemente versioniert werden können, zeigt das nachfolgende Kapitel "Versionieren von Softwareelementen (Seite 76)". Die Änderungskontrolle verschiedener Elemente wird in den Kapiteln "Audit Trail und Änderungskontrolle (Seite 119)" und "Kontrolle der Konfiguration (Seite 153)" erläutert.

Die Vorgehensweise im Falle von Änderungen an einer in Betrieb befindlichen Anlage sollte grundsätzlich mit dem Anlagenbetreiber abgestimmt werden, siehe Kapitel "Betriebliche Änderungskontrolle (Seite 170)".

Siehe auch

- GAMP 5-Leitfaden,
  Anhang M8 "Projekt-Änderungs- und Konfigurationsmanagement"

Schutz der Konfiguration

Neben der Kontrolle der Konfiguration im Rahmen des Änderungsverfahrens muss das System samt Konfiguration vor unbeabsichtigten oder unbefugten Eingriffen geschützt werden. Dies erfolgt durch eine Kombination verschiedener Maßnahmen. Hierzu zählen u.a.:

- Zugriffsbeschränkungen sowohl physisch als auch logisch
- Passwortschutz der CPU
- Schreibschutz bei Projekten und Plänen
- Geeignete Prozeduren und Training der Mitarbeiter

5.8 Versionieren von Softwareelementen

In den Projektrichtlinien muss definiert werden, welche Elemente wann versioniert werden, und ob dabei eine Neben- oder eine Hauptversion hochgezählt wird, z. B.:

"Die Hauptversion wird nach dem FAT auf 1.0 und nach der Inbetriebnahme auf 2.0 gesetzt. Alle anderen Änderungen werden in der Nebenversion hochgezählt."

Die Unterscheidung in Haupt- und Nebenversionsänderung kann z. B. aber auch von Umfang oder Auswirkung der Änderung abhängig gemacht werden.

Hinweis

Versions-, Autor- und Kommentarfelder können mittels Import-Export-Assistenten (IEA) beschrieben werden.

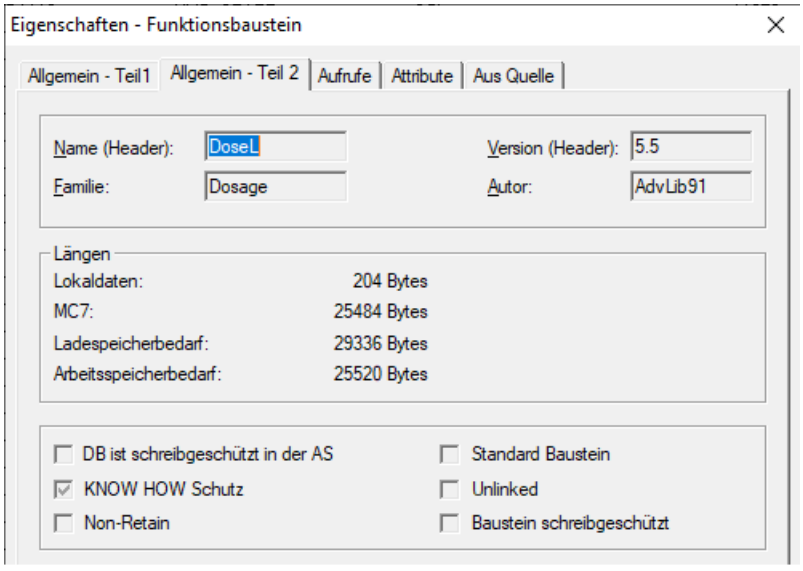
Die nachfolgenden Unterkapitel zeigen verschiedene Beispiele für die Versionierung von Softwareelementen, die im Wesentlichen aufgeteilt sind in

- AS-Elemente, die als Steuerungsfunktionen im Controller ablaufen
- OS-Elemente, die dem Bedienen und Beobachten dienen

5.8.1 Versionieren von AS-Elementen in PCS 7

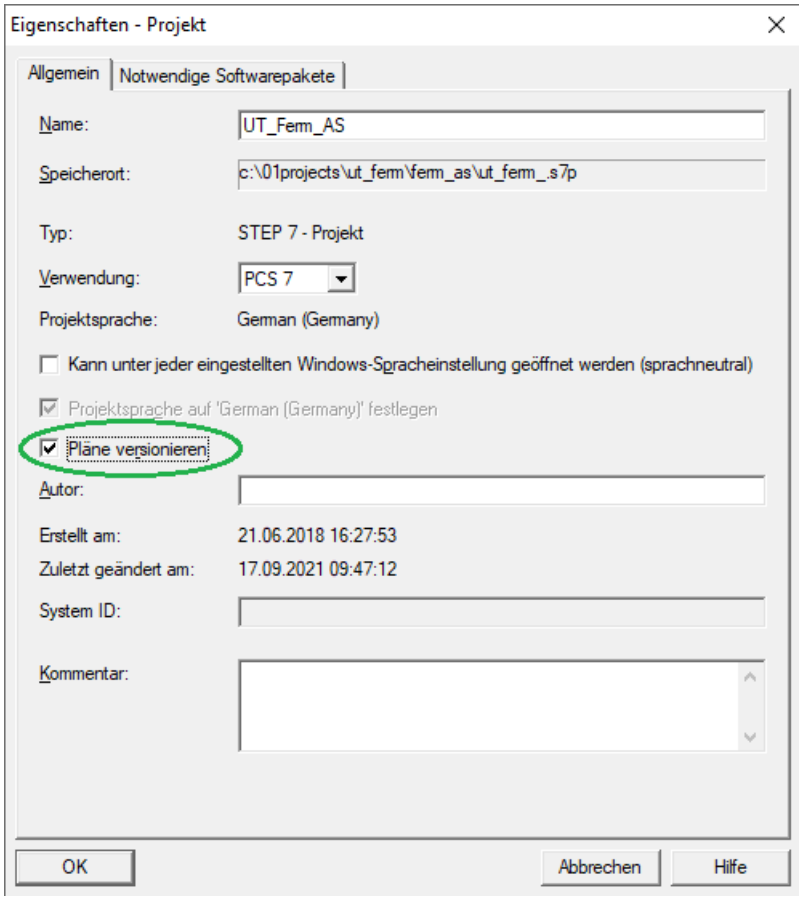
Die einzelnen Konfigurationsebenen in PCS 7 bieten unterschiedliche Möglichkeiten, die jeweiligen Elemente mit einer Versionskennung und teilweise mit Autor und Kommentar zu versehen.

Bei Bausteinen, CFC- und SFC-Plänen sowie bei SFC-Typen und Musterlösungen wird die Versionsnummer in den Eigenschaften des jeweiligen Objekts geführt.

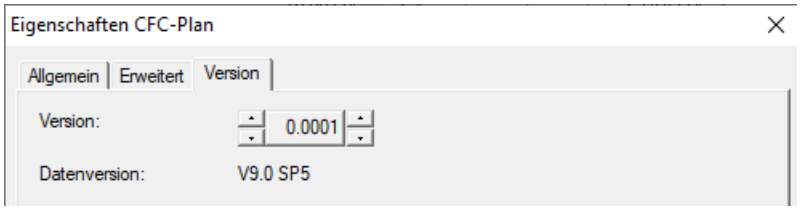


Versionieren von Bausteinen, CFC- und SFC-Plänen

PCS 7 unterstützt die Möglichkeit der teilautomatisierten Versionierung von CFC/SFC-Plänen und SFC-Typen. Hierzu muss die Versionierung in den Eigenschaften des jeweiligen Projektes oder Multiprojektes aktiviert werden.



Ist die Versionierung für das jeweilige Projekt aktiviert, so wird automatisch beim Schließen eines geänderten CFC/SFC-Planes oder SFC-Typs ein Dialogfeld geöffnet, im nachfolgenden Beispiel "Eigenschaften CFC-Plan".



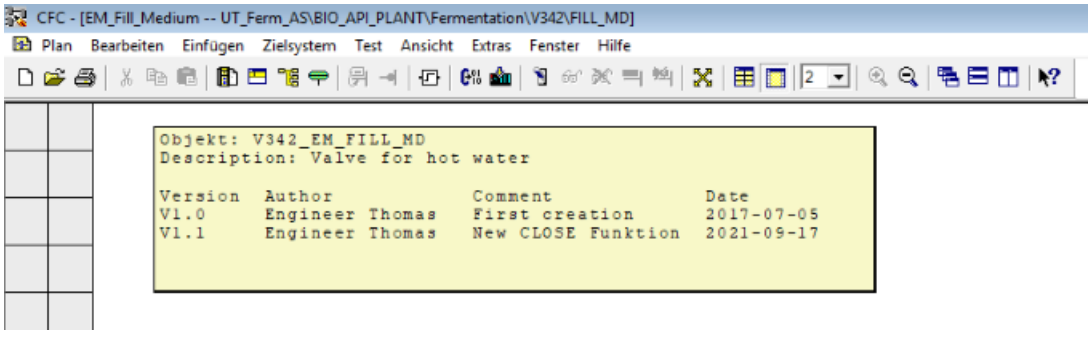
Über die Pfeiltasten rechts und links der Versionsnummer erfolgt eine Inkrementierung der Neben- bzw. Hauptversion. Bei einer falschen Eingabe kann lediglich bis zur letzten

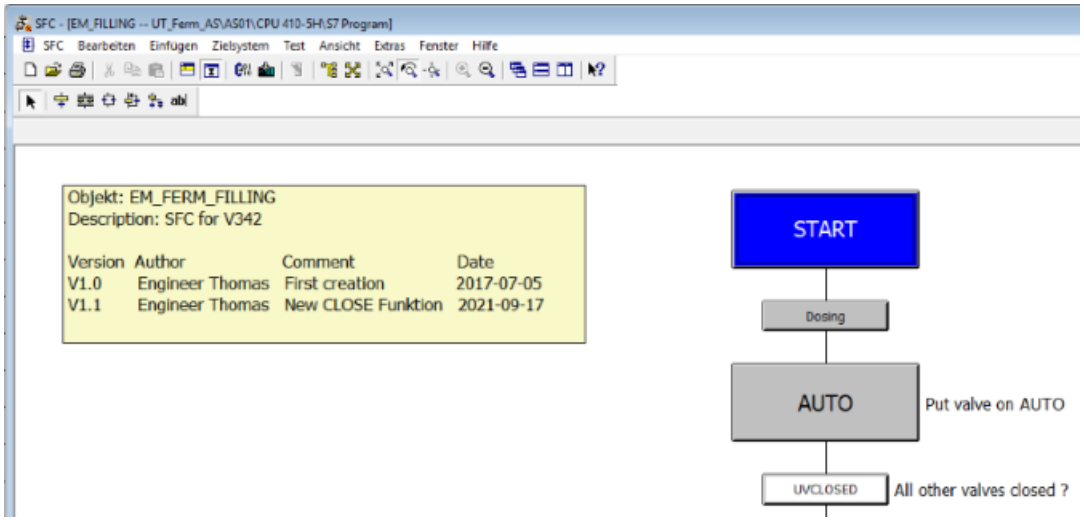
gespeicherten Versionsnummer dekrementiert werden. Änderungen der Versionsnummer müssen immer in Eigenverantwortung durch den Projektmitarbeiter durchgeführt werden.

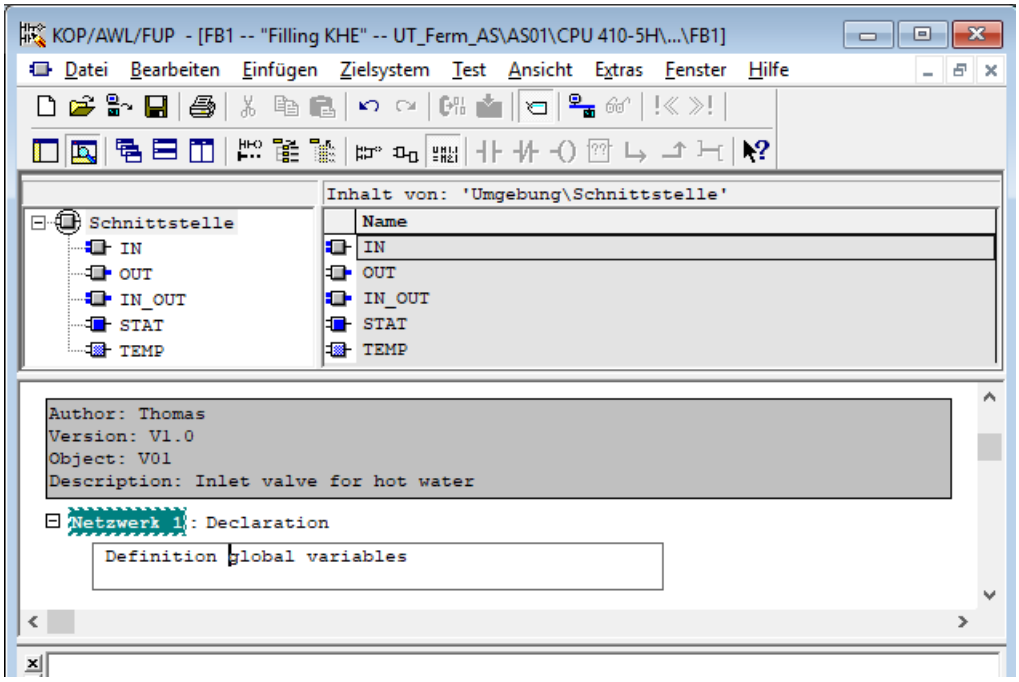
Hinweis

Eine gespeicherte Versionsnummer kann nicht mehr zurückgesetzt werden. Der Projektmitarbeiter muss folglich seine Eingaben prüfen, bevor er mittels OK bestätigt. Die Versionsnummer ist im Bereich 0.0001 – 255.4095 konfigurierbar.

Informationen zur Versionshistorie können mit einem separaten Kommentar als Textfeld im Plan eingefügt werden, siehe nachfolgende Grafik.

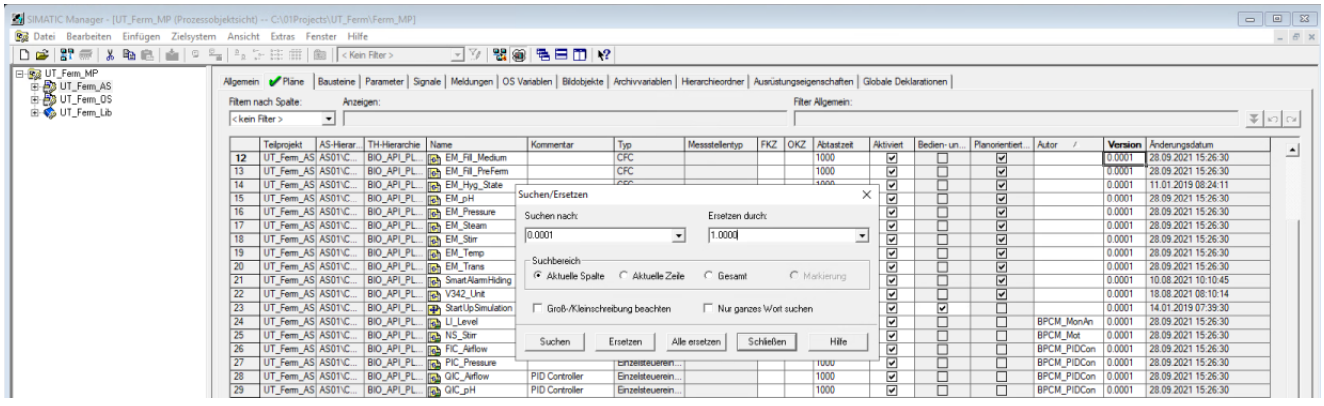






Hinweis

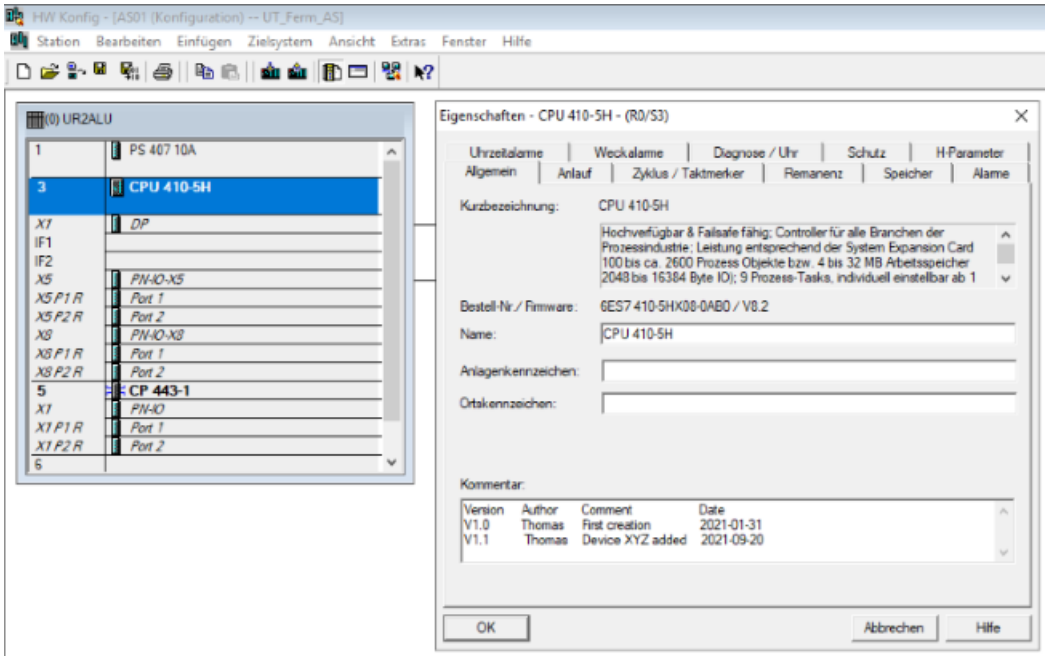
Eine Variante eines Versionskonzepts ist auch die Versionsführung auf Unit-Ebene bei entsprechend strukturierter Anlage. Die Unit und die unterlagerten Elemente werden als funktionale Einheit geführt und versioniert. Die Version der Unit kann in der Prozessobjektsicht über die Funktion "Suchen/Ersetzen" auf alle Elemente übertragen werden. Siehe nachfolgenden Screenshot. Versions- und Änderungskommentare sollten dann im Unit-CFC gepflegt werden.



Des Weiteren kann die Konfiguration auch übergeordnet auf Projekt- bzw. Teilprojektebene kontrolliert und versioniert werden. Hierbei helfen entsprechende Werkzeuge, wie sie in Kapitel "Kontrolle der Konfiguration (Seite 153)" beschrieben sind.

Grundlage von Änderungen ist immer ein Änderungsantrag, dem die erforderliche Änderungsdokumentation angehängt wird.

Versionieren der Hardware-Konfiguration in "HW Konfig"



In der Maske "Eigenschaften" kann das Kommentarfeld genutzt werden, um Versionskennzeichnung und weitere Informationen wie Versionshistorie einzutragen.

Versionieren der Konfiguration in SIMATIC NET

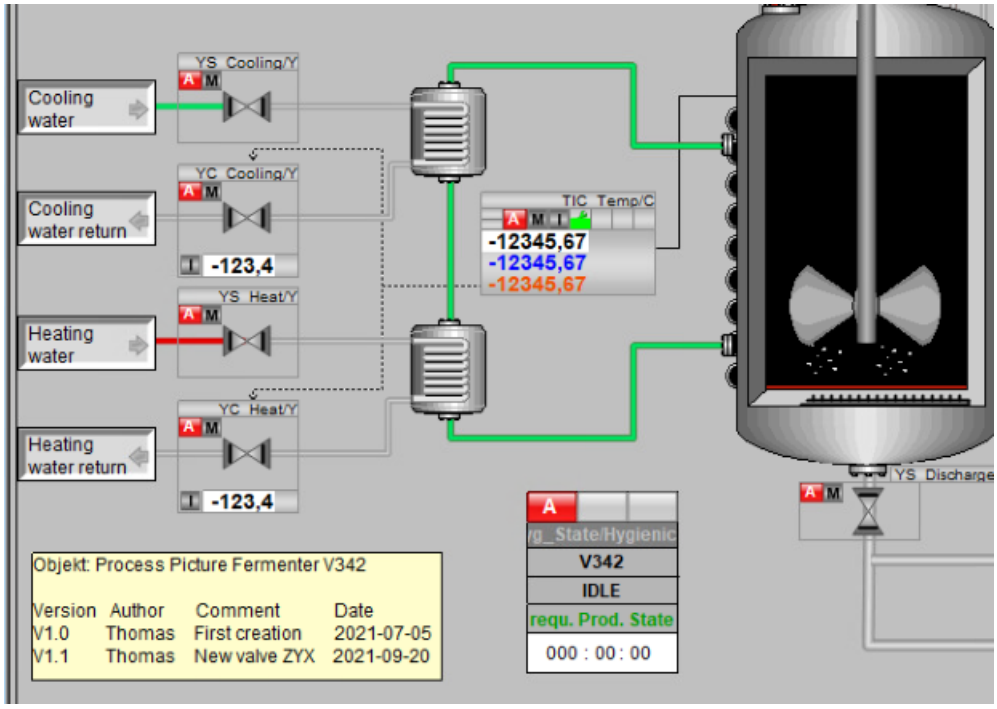
Auf der Busebene (Systembus, Profibus) kann in den Eigenschaften die Versionskennung eingetragen werden.

5.8.2 Versionieren von OS-Elementen in PCS 7

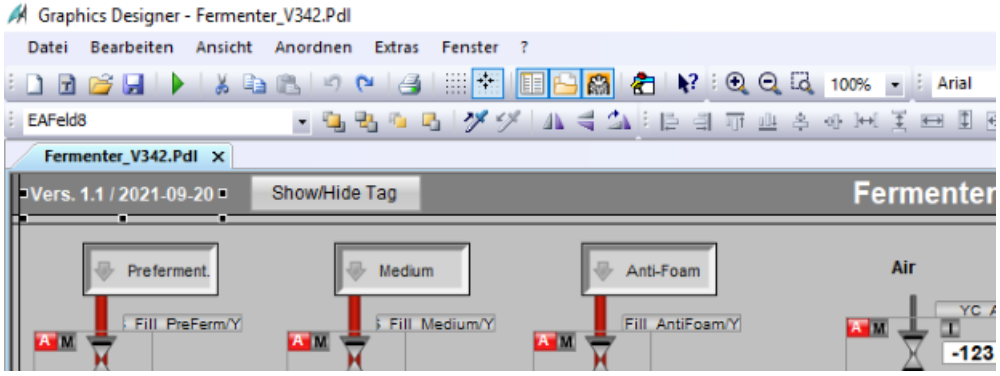
Bei der Software-Erstellung sollten alle selbst erstellten Grafiken, Reports, C-, VB-Skripte mit Angaben wie Autor, Datum, Kommentarfeld und Versionskennzeichen versehen werden. Hierfür gibt es z. B. bei Anwenderobjekten (Bildtypicals) ein Versionsfeld. Skripte und Anwender-FBs (SCL) können anhand des Änderungsdatums identifiziert werden, Versionskennung und Kommentar müssten im Skriptkopf als Text eingefügt werden.

Konfigurationseinstellungen müssen entsprechend dokumentiert werden, damit sie einerseits eine Referenz für die Validierung sind und andererseits im Falle einer Systemwiederherstellung zur Verfügung stehen.

Beispiele zur Versionierung von Grafikbildern

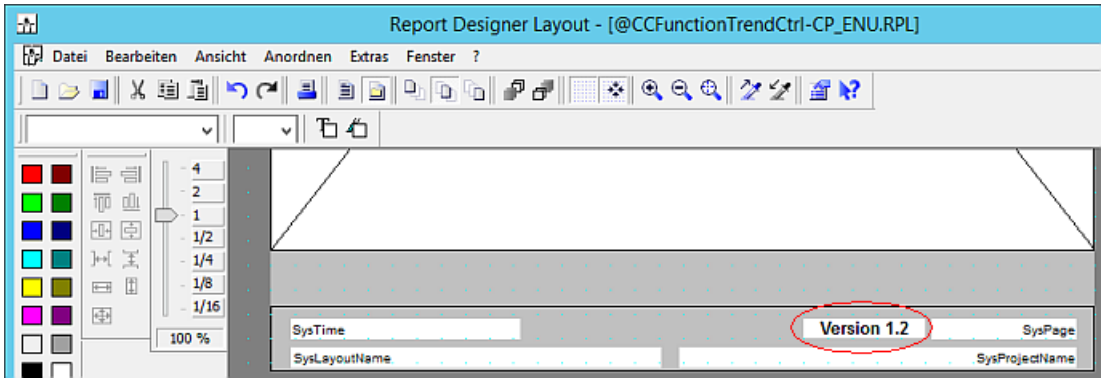


Versionsführung in einem in der Laufzeit unsichtbaren Feld innerhalb des Grafikbildes



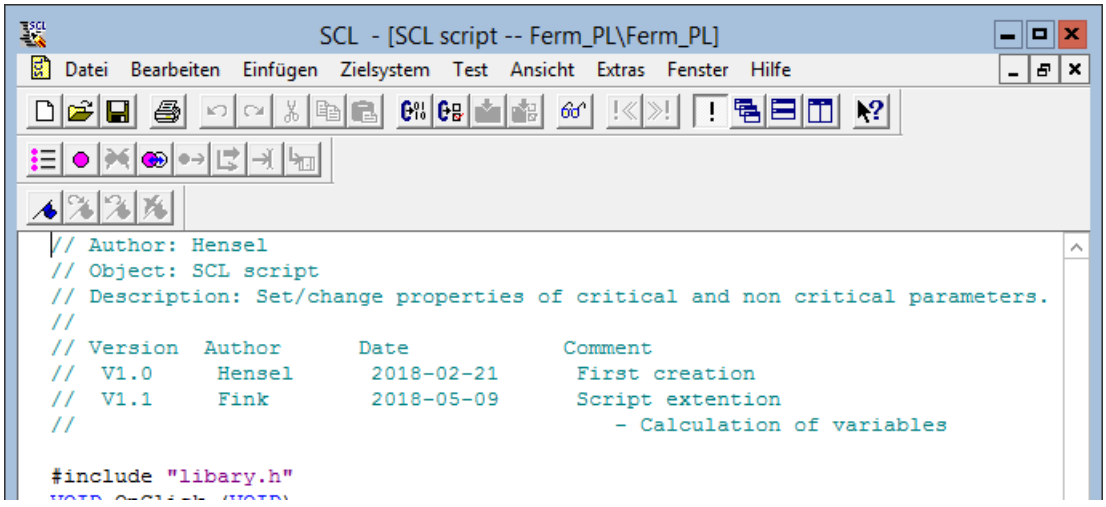
Versionskennung als sichtbares Feld im Grafikbild; Erläuterungen zur Versionshistorie außerhalb

Beispiel für Reports



Sichtbares Textfeld für die Versionierung z. B. in der Fußzeile des Reports

Beispiel für C-/VB-Skripte



Einfügen von Version und Kommentaren innerhalb eines Skripts

5.8.3 Weitere Hinweise zur Versionierung

Versionieren von Batch-Elementen

Das Versionieren von Rezepten wird unter dem Thema "Änderungskontrolle bei Rezepten" im Kapitel "SIMATIC BATCH (Seite 124)" erläutert.

Versionieren von Projekten, Multiprojekten und Bibliotheken

Unterstützende Systemfunktionen zum Versionieren von Projekten, etc. werden im Kapitel "Kontrolle der Konfiguration (Seite 153)" erläutert.

Erstellen der Applikationssoftware

6

Dieses Kapitel zeigt Hinweise und Empfehlungen auf, die bei der Erstellung von Applikationssoftware im GMP-pflichtigen Umfeld helfen sollen.

6.1 Softwaremodule, Typen und Kopiervorlagen

Software-Module bzw. Typ-Vorlagen in Form von Funktionsbausteinen, Funktionsplänen oder komplexen Schrittketten sind in der Prozessleittechnik weit verbreitet. Sie werden vorab erstellt und im Rahmen der Projektierung vervielfältigt.

Hinweis

Bei der Definition von Modulen bzw. Typen geht es neben der Reduzierung des Projektierungsaufwandes insbesondere um eine nachvollziehbare Struktur der Software. Dies trägt zur Vereinfachung der Dokumentation und einer risikobasierten Festlegung des Testaufwands bei und unterstützt darüber hinaus die spätere Pflege des Systems.

Siehe auch

- Verwendung von Typen bei der Programmierung in Kapitel "Software-Erstellung (Seite 18)"

6.1.1 Module und Typen in PCS 7

Für verschiedene Arten von Software-Elementen bietet SIMATIC PCS 7 die Möglichkeit der Erstellung und zentralen Pflege von Vorlagen, siehe hierzu Kapitel "Verwendung der Stammdatenbibliothek" (Seite 62). Technologisch zu unterscheiden sind dabei vor allem:

Messstellentyp / Einzelsteuereinheit (Typ)	**Projektspezifische Verschaltung von Blöcken** Verwendung der CFC-Technik, z. B. für Funktionen wie • Ventile • Pumpen • Motoren
Technische Einrichtung (Typ)	**Grafische Projektierung von Ablaufsteuerungen** Typ-Instanz-Konzept über die Stammdatenbibliothek Verwendung der SFC-Technik, z. B. für Rezeptfunktionen wie • Heizen • Rühren • Entleeren

Technische Funktion (Typ)	**Steuert mehrere unterlagerte Technische Einrichtungen** Typ-Instanz-Konzept über die Stammdatenbibliothek, Verwendung z. B. • Behälter
Musterlösung	**Kombination mehrerer CFC- und/oder SFC-Pläne** Verwendung z. B. für Funktionen wie • PID-Temperierung eines Behälters • Füllstandsüberwachung inkl. Sicherheitsabschaltung gegen Überlauf des Behälters • Unit

Die Arbeitsweise der Module ist in einer Beschreibung festzuhalten. Die projektspezifischen Parametrierungen (Archivieren, Bausteinkommentar, Messbereich, Alarme und Meldungen, MES-relevant, etc.) und Verschaltungen sind zu definieren.

Hinweis

Die Benennung der Module erfolgt gemäß Funktions- und Designspezifikation.

Bevor die Module / Typen vervielfältigt werden, müssen sie in einem Modultest überprüft und freigegeben werden.

Die verwendeten Softwaremodule müssen in einem Dokument mit Angabe ihrer jeweiligen Version für jede AS aktuell gepflegt werden.

Messstellentyp

SIMATIC PCS 7 bietet die Möglichkeit, für Teilkomponenten gleichen Typs einen Messstellentyp als Kopiervorlage zu erstellen, der aus einem oder mehreren CFC-Plänen bestehen kann. Das Erstellen von Messstellentypen für einander ähnliche Anlagenteile bringt Einsparungen beim Engineering und Testen mit sich. Nach dem Test eines Messstellentyps kann dieser beliebig oft im Multiprojekt vervielfältigt werden. Je Ableger können die Technologische Hierarchie, der CFC-Name, Meldungen, Anschlusspunkte für Parameter oder Signale sowie verschiedene Eigenschaften des Moduls angepasst werden.

Typen für Einzelsteuereinheit (CM)

Ein Control Module Type (CMT; auch Einzelsteuerungseinheitstyp) stellt eine abgeschlossene verfahrenstechnische Einheit dar (z. B. Ventil) und dient als Typdefinition für Control Module (CMs). Durch optionale Blöcke (z. B. Eingangs-/Ausgangsbausteintreiber) können Varianten des CMT erstellt werden. Dadurch reduziert sich die Gesamtzahl der Typen, die bereitgestellt und gepflegt werden müssen. Nach einer Instanziierung der Variante kann die CM-Instanz individuell auf die spezifischen Bedürfnisse angepasst werden. Änderungen am Typ oder der Variante können an die Instanz(en) weitergegeben werden.

Ein CMT besitzt zudem ein Automation Interface, das zum Datenaustausch zwischen PCS 7 Projekt und dem PAA (Plant Automation Accelerator) Projekt sowie SIMATIC SIMIT verwendet wird.

Siehe auch

- Handbuch "PCS 7 Engineering System", Kapitel 9.15.6 sowie Kapitel 14 "Technologisches Projektieren", Online-Support unter Beitrags-ID 109800500 (https://support.industry.siemens.com/cs/ww/de/view/109800500)

Hinweis

Bestehende Messstellentypen können in CMTs konvertiert werden und im Rahmen des Integrated Engineering über den PAA konfiguriert werden. Ein Datenaustausch reiner CFC Pläne zwischen SIMATIC PCS 7 und PAA ist nicht möglich; es werden hier nur Informationen des Automation Interface ausgetauscht. Daher ist ein Umstieg auf das Engineering mit CM(T)s anzuraten.

SFC-Typ

Das Typ-Instanz-Konzept von SIMATIC PCS 7 bietet die Möglichkeit, Typen von Ablaufsteuerungen zu erstellen. Der sogenannte SFC-Typ ermöglicht die Definition von Ablaufsteuerungen inklusive einer Schnittstelle in Form eines CFC-Bausteins. Die Ablauflogik des SFC-Typs basiert auf den Schnittstellenanschlüssen des SFC-Typs, d. h. der SFC-Typ kann, im Unterschied zum SFC-Plan, nicht auf beliebige Prozesssignale zugreifen.

Der SFC-Typ ist alleine nicht ablauffähig. Ein SFC-Typ muss wie ein Funktionsbaustein-Typ in einem CFC-Plan platziert werden, um ein ablaufrelevantes Objekt zu erhalten, in diesem Fall eine SFC-Instanz. Der SFC-Typ und die SFC-Instanzen werden im Kontext "Programm übersetzen" mit übersetzt. Um eine SFC-Instanz zum Ablauf zu bringen, werden sowohl der SFC-Typ als auch die SFC-Instanz in das Automatisierungssystem geladen.

Siehe auch

- Handbuch "SFC für SIMATIC S7", Online-Support unter Beitrags-ID 109792631 (https://support.industry.siemens.com/cs/ww/de/view/109792631)
- Handbuch "PCS 7 Engineering Kompendium Teil C", Kapitel 6, Online-Support unter Beitrags-ID 109804258 (https://support.industry.siemens.com/cs/ww/de/view/109804258)

Typen für Technische Einrichtung (EM) und Technische Funktion (EPH)

Technische Einrichtungen (EM=Equipment Module) und Technische Funktionen (EPH=Equipment Phase) nutzen ebenso wie CMTs das Typ-Instanz-Konzept und werden über die jeweiligen Typen EMT bzw. EPHT im Projekt instanziert. Bestandteil einer Technischen Einrichtung ist genau eine sogenannte Ablaufsteuerung, siehe SFC-Typ. Für die Zuordnung der Technischen Einrichtung zu den Aktoren und Sensoren auf der Einzelsteuerebene wird die Einzelsteuereinheit (CM bzw. CMT) eingesetzt.

Technische Funktionen steuern mehrere unterlagerte Technische Einrichtungen.

Siehe auch

- Handbuch "PCS 7 Engineering Kompendium Teil C", Kapitel 10, Online-Support unter Beitrags-ID 109804258 (https://support.industry.siemens.com/cs/ww/de/view/109804258)
- Handbuch "CFC für SIMATIC S7" Kapitel 10.13 "Technische Einrichtungen projektieren", Online-Support unter Beitrags-ID 109792630 (https://support.industry.siemens.com/cs/ww/de/view/109792630)

Musterlösung

SIMATIC PCS 7 bietet die Möglichkeit, für Teilkomponenten gleichen Typs eine Musterlösung zu erstellen, welche aus einem oder mehreren CFC- und/oder SFC-Plänen bestehen kann. Das Erstellen von Musterlösungen für einander ähnliche Anlagenteile bringt Einsparungen beim Engineering und Testen mit sich. Nach dem Test eine Musterlösung kann diese beliebig oft im Multiprojekt vervielfältigt werden. Je Ableger können die Technologische Hierarchie, der CFC-Name, Meldungen, Anschlusspunkte für Parameter oder Signale sowie verschiedene Eigenschaften des Moduls angepasst werden. Musterlösungen können auch Bilder und Reports beinhalten.

Jeder Baustein-Instanz kann ein Bildsymbol zugewiesen werden, welches dann bei der OS-Übersetzung durch die Ableitung der Bildschirmhierarchie automatisch in das im SIMATIC Manager definierte Fließbild inkl. der Variablenanbindung eingefügt wird. Das erspart Arbeit und gibt die Sicherheit, dass das Bildsymbol mit der richtigen Baustein-Instanz verbunden ist.

Zur Verwendung von Bausteinsymbolen siehe Kapitel "Automatische Generierung von Bausteinsymbolen (Seite 89)".

Hinweis

Die Bausteinsymbole sollten gemeinsam mit dem zugehörigen Software-Modul als Messstellentyp getestet und vom Kunden genehmigt werden, bevor sie vervielfältigt werden.

6.1.2 Beispiel eines Messstellentyps

Jedes Software-Modul wird in Form eines CFC-Plan als Vorlage erstellt. Dieser wird nach dem Software-Modultest zur Instanziierung freigegeben und kann im Rahmen der Projektierung genutzt werden.

Ein Beispiel für ein solches Modul zeigt das Handbuch "PCS 7 Kompendium Teil A".

Die Parametrierung und die Verschaltung der Ein- und Ausgänge sind gemäß GMP-Anforderungen in einer entsprechenden Spezifikation (z. B. "Software Modul Design Spezifikation") detailliert zu beschreiben und in einem Test ("Software Modul Test" oder "Typical Test") entsprechend zu überprüfen.

Siehe auch

- Handbuch "PCS 7 Kompendium Teil A", Kapitel 8.2.1 "Messstellentypen (Templates)", Online-Support unter Beitrags-ID 109809015 (https://support.industry.siemens.com/cs/ww/de/view/109809015).

Hinweis

Auch Einstellungen z. B. für die Prozesswert-Archivierung können bereits im Messstellentyp berücksichtigt werden.

6.1.3 Automatische Generierung von Bausteinsymbolen

Grafische Bausteinsymbole werden eingesetzt, um Informationen über Prozesszustände (z. B. Ventil offen, geschlossen, gestört, etc.) in der Bedienstation (OS) von PCS 7 darzustellen.

PCS 7 bietet Grafik-Vorlagen für alle in der PCS 7-Bibliothek enthaltenen Bausteine und unterstützt somit das Typ-Instanz-Konzept vom Funktionsbaustein in der AS bis hin zur Bedienkomponente in den Anlagenbildern der PCS 7 OS. PCS 7 bietet die Möglichkeit, mehrere Vorlagenbilder zu verwenden.

Hinweis

Die automatische Generierung von Bausteinsymbolen reduziert das Fehlerrisiko.

Siehe auch

- PCS 7 on Tour – Basic,
  Kapitel 10 Abschnitt 5 "Angepasste Bausteinsymbole und Bildbausteine"
- Handbuch "PCS 7 Operator Station", Kapitel 10.2, Online-Support unter
  Beitrags-ID 109794374 (https://support.industry.siemens.com/cs/ww/de/view/109794374)

Wird die Funktion *Bausteinsymbole erzeugen/aktualisieren* ausgeführt, werden die Bausteinsymbole anhand der Namen und Prioritäten aus der Technologischen Hierarchie des Projektes abgeleitet, aus den Vorlagenbildern herauskopiert und automatisch mit der Variablenanbindung des jeweiligen Bedienbausteins verknüpft.

Priorität	Bildname	Bemerkung
1.	@PCS7Typicals_MyAPL.pdl	beginnend mit dem alphabetisch letzten Bild
2.	@PCS7TypicalsAPLV9.pdl	ist im Standard enthalten
3.	@PCS7TypicalsAPLV8.pdl	

Das Vorlagenbild @PCS7TypicalsAPL<Version>.pdl

Das Bild "@PCS7TypicalsAPL<Version>.pdl" ist in jedem PCS 7 OS Projekt standardmäßig enthalten. Es enthält die Standard-Bausteinsymbole.

Hinweis

Die Originaldatei "@PCS7TypicalsAPL<Version>.pdl" sollte keinesfalls verändert werden. Änderungen in der Originaldatei werden bei einem Update bzw. bei Hochrüstungen überschrieben.

Für kundenspezifische Bausteinsymbole sollten eigene Vorlagenbilder erstellt werden, "@PCS7Typicals_MyAPL.pdl".

Projektspezifisches Vorlagenbild

Ein projektspezifisches Vorlagenbild, "@PCS7Typicals_MyAPL.pdl", kann durch Kopieren des Vorlagenbildes "@PCS7TypicalsAPL<Version>.pdl" erstellt werden. Im "neuen" Vorlagenbild können kundenspezifische Änderungen vorgenommen werden.

Das Vorlagenbild @Template.pdl

Das Vorlagenbild "@TemplateAPL<Version>.pdl" wird hauptsächlich dann benutzt, wenn Bausteinsymbole manuell in Bilder eingefügt werden. Diese Bausteinsymbole stehen nicht in Verbindung mit der Technologischen Hierarchie und werden somit auch nicht vom System erzeugt oder aktualisiert.

Dennoch kann die Nutzung der Vorlagendatei von Vorteil sein. Zum einen ist man nicht an die Technologische Hierarchie gebunden und zum anderen kann man mit Hilfe eines Wizards die Bildobjekte von einem Fließbild oder allen Fließbildern in eine Konfigurationsdatei exportieren, die Bausteinsymbole und deren Verbindungen ändern und anschließend die Bildobjekte wieder importieren. Die Konfigurationsdatei kann mit Hilfsmitteln wie z. B. Excel bearbeitet werden.

Hinweis

Die Datei "@TemplateAPL<Version>.pdl" wird vom PCS 7-System gepflegt und wird bei Updates bzw. bei Hochrüstungen überschrieben. Es empfiehlt sich daher, die Datei "@TemplateAPL<Version>.pdl" regelmäßig zu sichern.

Weitere Vorlagenbilder

@@ConfigTypicals.pdl
Dient zur Erzeugung/Aktualisierung des Lifebeat-Monitorings.

@@MaintenanceTypicals.pdl
Dient zur Erzeugung/Aktualisierung der Diagnosebilder.

@PCS7elementsAPL.pdl
Das Vorlagenbild enthält eine Sammlung vorgefertigter Objekte zur Erzeugung von Bausteinsymbolen.

@PCS7Typicals_Batch.pdl
Dient zur Erzeugung/Aktualisierung von Bausteinsymbolen für SIMATIC BATCH.

@PCS7Typicalsrc.pdl
Dient zur Erzeugung/Aktualisierung von Bausteinsymbolen für SIMATIC Route Control.

Diese Aufzählung erhebt keinen Anspruch auf Vollständigkeit.

Zentrale Änderbarkeit von Bildobjekten

SIMATIC PCS 7 bietet bei der Typisierung die Möglichkeit der zentralen Änderbarkeit von Objekten, d. h. nachträgliche Änderungen an Bildobjekten werden in den Vorlagenbildern vorgenommen.

Hinweis

Die zentrale Änderbarkeit von Bildobjekten bedeutet nicht, dass Änderungen automatisch an die Instanzen durchgereicht ("vererbt") werden. Hierzu muss vor dem Vererben über den "Dynamic Wizard" die Funktion "Export Bildobjekte" durchgeführt werden, damit nach dem "Import Bildobjekte" alle Objekte wieder an ihrer ursprünglichen Position liegen.

Übernahme anwenderspezifischer Anpassungen

Wenn im Projekt ein eigenes Vorlagenbild verwendet wird, dessen Bausteinsymbole auf der APL basieren, können diese bei einer Hochrüstung ebenfalls migriert werden. Im Migrationsfall werden die geänderten Eigenschaften beibehalten und neue Funktionen oder Bestandteile aus der Vorlage @PCS7TypicalsAPLV9.pdl übernommen.

Siehe auch

- Handbuch "PCS 7 Kompendium Teil A", Kapitel 10.2.4 "Eigene Bausteinsymbole/ Anwenderobjekte", Online-Support unter Beitrags-ID 109809015 (https://support.industry.siemens.com/cs/ww/de/view/109809015).

6.1.4 Type Change in Run (TciR)

TciR ermöglicht es, Änderungen an den Blockverbindungen (Ein-, Ausgängen) von Bausteinen im laufenden Betrieb (Run) zu laden. Diese Funktionalität ist auf Grund der notwendigen Validierungsverfahren im Pharmaumfeld sicherlich nur eingeschränkt von Vorteil, denn wie bei jeder Änderung müssen deren Auswirkungen bewertet und kontrolliert werden. Ein möglicher Anwendungsfall könnte z. B. eine Reinstwasseranlage in einem Anlagenverbund sein.

6.2 Massendatenbearbeitung (Bulk Engineering)

6.2.1 Bulk Engineering mit der Prozessobjektsicht

Wenn es darum geht, schnell viele Parameter zu überprüfen oder zu ändern, kann dies in der Prozessobjektsicht erfolgen. Mit Ihrer Hilfe lassen sich Parameter nach bestimmten Kriterien filtern und deren Werte ansehen bzw. bearbeiten.

Die Prozessobjektsicht ermöglicht das Suchen von Plänen über das gesamte Multiprojekt.

6.2.2 Bulk Engineering mit dem CM-Generator

Der CM-Generator nutzt den Mechanismus des Bulk Engineering zum Erstellen, Aktualisieren und Löschen von Instanzen von CMTs, EMTs und EPHTs in einem Projekt mithilfe einer Liste (als "Generator-Liste" bezeichnet).

Die CM-Generator-Funktionalität wird zum Beispiel für folgende Zwecke verwendet:

- Generieren von Einzelsteuereinheiten für Prozessanlagen auf Sensoren- und Aktorenebene
- Generieren von Technischen Einrichtungen bzw. Technischen Funktionen auf Gruppensteuerungsebene (abhängig von spezifiziertem EMT/EPHT)

Eine ausführliche Beschreibung zur Verwendung des CM-Generators enthält das Handbuch "PCS 7 Engineering System".

Siehe auch

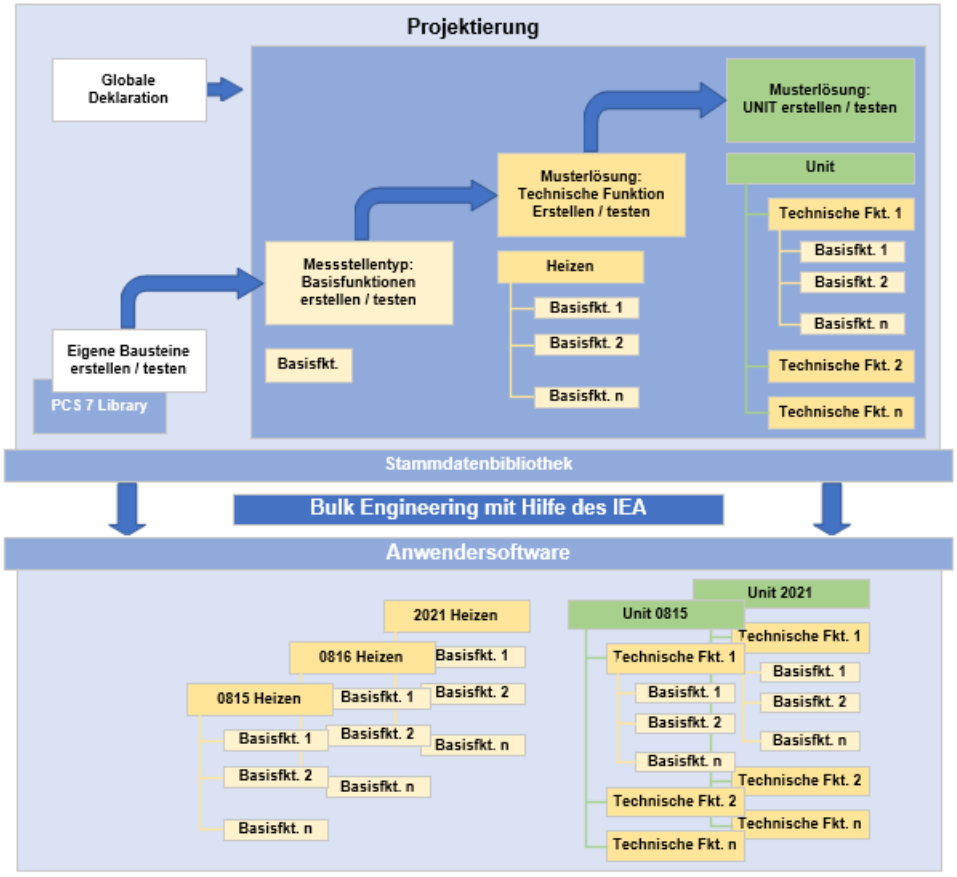
- Handbuch "PCS 7 Engineering System", Kapitel 14.9, Online-Support unter Beitrags-ID 109800500 (https://support.industry.siemens.com/cs/ww/de/view/109800500)

6.2.3 Bulk Engineering mit dem IEA

Der Import-Export-Assistent (IEA) wird für zwei Aufgabengebiete eingesetzt.

Vervielfältigung mit dem IEA

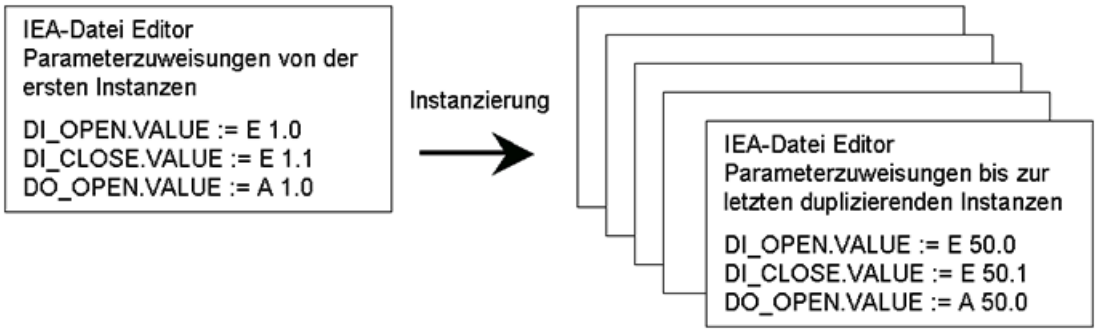
Der Import-Export-Assistent wird eingesetzt, um Messstellentypen oder Musterlösungen zu vervielfältigen. Hierzu werden projektabhängige Typicals auf Basis von Standardbibliotheken definiert, die dann durch Instanziierung mit Hilfe des Import-Export-Assistenten beliebig oft kopiert werden können.



Durch einen modularen Aufbau der Software sowie die Vervielfältigung mit Hilfe des IEA werden sowohl der Engineering- als auch der Testaufwand und damit das Fehlerrisiko deutlich reduziert.

Parameterbearbeitung mit dem IEA

Des Weiteren werden mit Hilfe des IEA-Datei-Editors in einer Tabelle jeder Instanz die Parameter und die Signalverarbeitung entsprechend der in der Spezifikation definierten Vorgaben eingetragen.



Siehe auch

- Handbuch "PCS 7 Engineering System", Kapitel 9.15.7 "Erstellen von Messstellen aus Messstellentypen (Multiprojekt)", Online-Support unter Beitrags-ID 109800500 (https://support.industry.siemens.com/cs/ww/de/view/109800500)
- Handbuch "PCS 7 Engineering System", Kapitel 10.3 und 10.4 "Arbeiten mit dem Import-Export-Assistenten", Online-Support unter Beitrags-ID 109800500 (https://support.industry.siemens.com/cs/ww/de/view/109800500)

6.2.4 Typ-Instanz-Konzept mit dem PAA

Für den integrierten Planungs-Workflow von der Prozessbeschreibung bis zum Automatisierungsprogramm ist der SIMATIC PCS 7 Plant Automation Accelerator (kurz: PAA) verfügbar. Ähnlich wie der IEA stellt der PAA eine Anwendung zum Vervielfältigen, Bearbeiten und Importieren von Software-/ Hardwarekomponenten in Form eines Massenengineering dar. Darüber hinaus bietet der PAA aber auch Möglichkeiten zur Dokumentation direkt aus dem Engineering Tool sowie zur Verwaltung von Dokumenten einschließlich Revisionierung.

Bereits existierende Projektdaten können aus SIMATIC PCS 7 in den PAA übernommen werden. Mit dem Excel Import können Messstellenlisten und Signallisten in den PAA importiert werden. Die Technologische Hierarchie, Signal- und Parametereinstellungen können automatisch aus den importierten Messstellenlisten und Signallisten übernommen werden. Die Hardware (dezentrale Peripherie inklusive Kanalbelegung) kann aus Signallisten generiert werden. Anschließend können alle im PAA projektierten Software-/Hardwarekomponenten nach SIMATIC PCS 7 transferiert und dort genutzt werden.

Während im IEA das Vervielfältigen ein reiner (meist einmaliger) Kopiervorgang ist, so bietet das Typ-Instanz-Konzept des PAA gleichzeitig auch ein Werkzeug für die spätere Pflege der Typen (Control Module Type, CMT) und der zugehörigen Instanzen (Control Module, CM).

Vergleich des PAA mit dem IEA

Oberfläche

PAA basiert auf COMOS und hat daher dieselbe Oberfläche wie die der COMOS Applikation. Sie wird jedoch durch verschiedene Tools (PCS 7 Import/Export; Typ-Konfigurator, Excel Import ....) erweitert. Durch das Arbeitsschichtenkonzept kann die Bearbeitung des Projektes an verschiedene User gleichzeitig zur Bearbeitung zugewiesen werden. Dadurch eignet sich die Projektierung mit dem PAA auch für die Erweiterungsprojektierung bereits existierender Anlagenteile, kann jedoch auch zum reinen Hardware- oder Softwareengineering verwendet werden.

Typ-Instanz versus Kopieren

Eine nachträgliche Änderung eines Typicals im IEA macht einen kompletten Re-Import der "Instanzen" (Kopien) notwendig. Das bedeutet, dass Parametrierungen und Verschaltungen zu anderen oder höheren Funktionen verloren gehen und eine Nachbearbeitung inklusive Revalidierung durchgeführt werden muss.

Der PAA bietet die Möglichkeit, Änderungen an den Control Module Typen (CMT) vorzunehmen und dessen Instanzen (CM) zu aktualisieren. Bereits erzeugte CMs können auf Abweichungen zum CMT überprüft und die Änderungen übernommen werden. Falsch instanziierte CMTs können mit dem Tool ‚Neuzuweisung der Typen' korrigiert werden. Die Projektierung mit CMTs ist somit flexibler als die Projektierung mit IEA-Typicals.

Typ-Varianten mit optionalen Bausteinen

Bei der Projektierung eines CMT ist es möglich, optionale Bausteine zu definieren. Im Typ-Konfigurator können durch An- und Abwahl dieser optionalen Bausteine Varianten des CMT erzeugt werden. Diese Varianten werden instanziiert und können wie CMTs nachbearbeitet und deren Instanzen aktualisiert werden.

So wird beispielsweise ein Ventil mit einem Interlock-Baustein und ein weiteres Ventil ohne Interlock-Baustein aus demselben CMT generiert. Mit dem IEA wären für diese beiden Ventile zwei Typicals notwendig.

Bei Verwendung des IEA müssten statt eines CMT mit z. B. drei optionalen Bausteinen je nach Kombination bis zu 8 Typicals erstellt und auch getestet werden.

Projektierung mit PAA

Zu Beginn wird ein Projekt im PAA angelegt. Zum Datenaustausch muss in SIMATIC PCS 7 bereits ein Multiprojekt angelegt und die Stammbibliothek definiert sein. Diese kann, wenn sie CMTs enthält, nach PAA importiert werden.

Der PAA bringt eine eigenständige Benutzerverwaltung mit. Dadurch ist es möglich, bereits im Engineering vordefinierte Bereiche (Arbeitschichten, Projekte, Funktionen) für den Bearbeiter freizugeben oder verschiedene Berechtigungsstufen zu definieren.

Control Module Type (CMT)

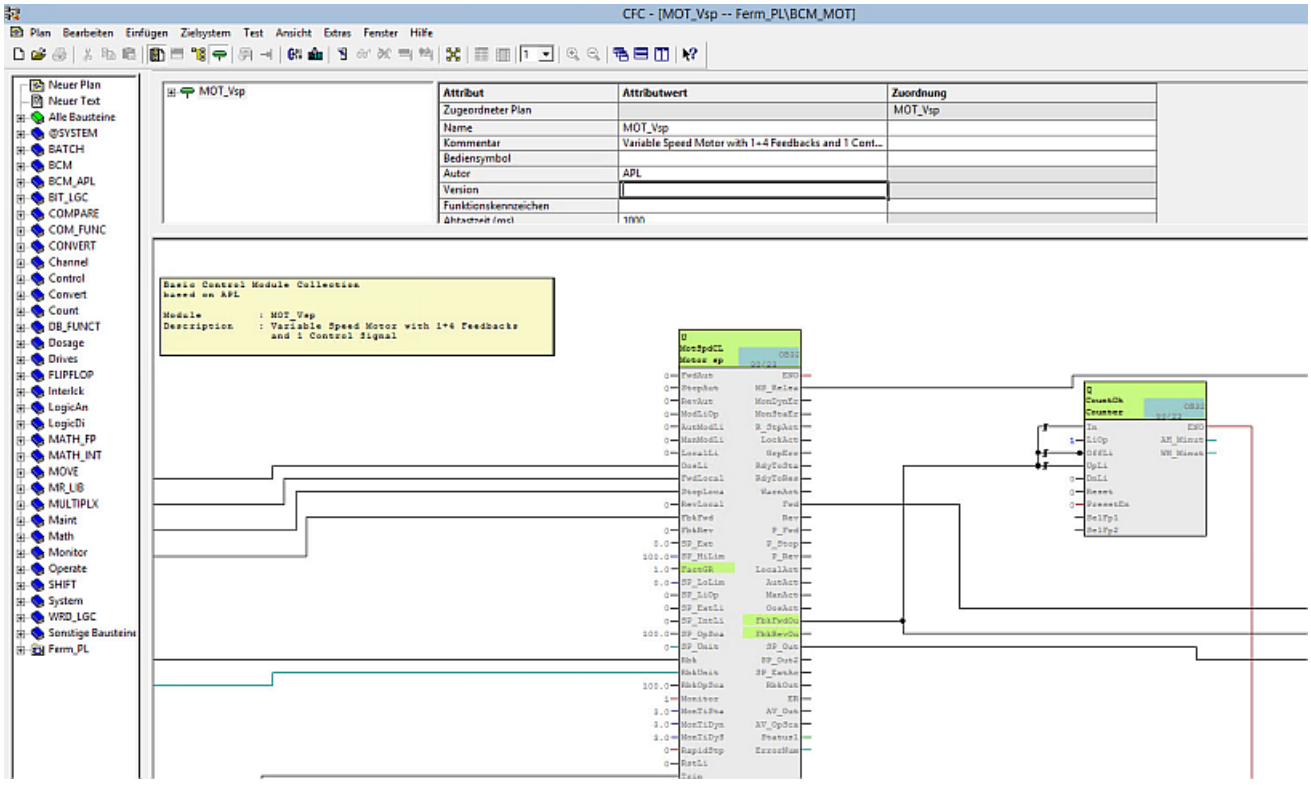
CMTs kann der Bearbeiter aus einem Messstellentyp aus der Stammdatenbibliothek erzeugen oder komplett neu erstellen. CMTs können Einzelsteuereinheiten, Steuervariablen und Meldungen enthalten. Sowohl die grün eingefärbten Bausteinköpfe in der folgenden Abbildung als auch der obere Bildbereich verdeutlichen, dass es sich um einen CMT handelt.

Equipment Module Type (EMT)

In gleicher Weise geschieht dies auch bei technischen Einrichtungen (Equipment Modules, EM) und technischen Funktionen (Equipment Phases, EPH). Statt einzelne Bausteinanschlüsse miteinander zu verschalten, erfüllt eine CM-Instanz eine Rolle aus Sicht des EM, und die natürlich weiterhin notwendigen Einzelverschaltungen erfolgen automatisch im Hintergrund. Dabei sind weder die Equipment Phase Types (EPHTs) noch die Equipment Module Types (EMTs) als Ersatz für SFC-Typen zu verstehen. Sie verwenden vielmehr intern das bewährte SFC-Typ-Instanz-Konzept. Ein EPHT bzw. ein EMT ist wie ein CMT, der genau eine Instanz eines SFC-Typs enthält. Darüber hinaus können noch weitere Bausteine enthalten sein.

Hinweis

Im PAA können nur die grün eingefärbten Technologischen Anschlüsse bearbeitet werden. In PCS 7 können natürlich nach wie vor alle Anschlüsse bearbeitet werden. Die Idee dahinter ist, dass ein Typ gewisse statische Elemente hat, die an jeder Instanz gleich sein sollen. Diese werden folglich nicht zur Bearbeitung im PAA benötigt. Die grünen Anschlüsse wiederum stellen die instanzspezifischen Anschlüsse und Parameter dar, die bearbeitet werden können.



CMTs, deren Attribute, Steuervariablen und Meldungen können im PAA bearbeitet werden.

CMs werden generiert, indem eine Variante des CMT in der Technologischen Hierarchie zugewiesen wird. Bei der Erstellung der Variante kann ausgewählt werden, ob und welche optionalen Blöcke des CMT verwendet werden sollen.

Nach Bearbeitung des Projektes im PAA werden alle relevanten Daten wieder in das PCS 7 Projekt exportiert. Die weitere Bearbeitung des Projektes findet im SIMATIC Manager statt.

Siehe auch

- "SIMATIC PCS 7 Plant Automation Accelerator", Online-Support unter Beitrags-ID 109742154 (https://support.industry.siemens.com/cs/ww/de/view/109742154)

6.3 Erstellen der Prozessbilder

Die Prozessbilder sind in Anlehnung an die Vorgaben der Spezifikation (z. B. URS, FS und R&I) zu erstellen. Wie bei allen anderen Arbeitsschritten im GMP-Umfeld wird also auch hier zuerst **geplant**, dann **umgesetzt** und anschließend **getestet**.

Die Bausteinsymbole sollten mit Hilfe der automatischen Generierung von Bausteinsymbolen zugeordnet werden, d. h. jedem instanzspezifischen Modul (Ventil, Pumpe, Regler, etc.) wird ein Bausteinsymbol im Prozessbild über die IEA-Datei zugeordnet. Die Voraussetzung für die Generierung der Bausteinsymbole ist, dass Bild und Bausteinpläne im selben bzw. gleichnamigen technologischen Hierarchieordner projektiert sind.

In SIMATIC PCS 7 gibt es SVG-Grafiken (skalierbare Vektorgrafiken). Diese haben beim Skalieren der Anlagenbilder keine Qualitätsverluste können und somit auf unterschiedlichen Bildschirmformaten in guter Qualität ausgegeben werden.

Nach Erstellung der Grafiken sollten diese dem Kunden zur Genehmigung in Form von Screenshots vorgelegt werden.

Siehe auch

- Kapitel "Automatische Generierung von Bausteinsymbolen (Seite 89)" zur Verwendung von Templatebildern als Bibliothek
- Handbuch "PCS 7 OS Prozessführung", Kapitel 8.3, Online-Support unter Beitrags-ID 109794375 (https://support.industry.siemens.com/cs/ww/de/view/109794375)
- Handbuch "PCS 7 Kompendium Teil A", Kapitel 10.2 "Visualisierungsoberfläche", Online-Support unter Beitrags-ID 109809015 (https://support.industry.siemens.com/cs/ww/de/view/109809015)

Hinweis

Bei Verwendung des WinCC OnlineTableControls muss in den Eigenschaften "Bearbeitung erlauben" deaktiviert sein, damit über die Maske keine Werte verändert werden können.

6.4 Anwenderspezifische Bausteine und Skripte

Bei der Erstellung von anwenderspezifischen Bausteinen (FB, FC) und Skripten (C-, VB-) handelt es sich um selbst geschriebene Programme, die der GAMP-Software-Kategorie 5 zugeordnet werden. Diese Art von Software wird entwickelt, um kundenspezifische Anforderungen zu erfüllen, welche durch vorhandene Funktionen und Bibliotheken nicht abgedeckt werden.

Generell muss bei solchen kundenspezifischen Bausteinen und Skripten erhöhter Aufwand für die Validierung in Form von ausführlicher Funktions- und Schnittstellenbeschreibung sowie

dokumentierten Tests einkalkuliert werden, siehe auch Kapitel "Software-Kategorisierung gemäß GAMP 5-Leitfaden (Seite 144)".

Hinweis

Bei der Erstellung von Anwenderspezifischen Bausteinen und Skripten sollten in projekt-/abteilungsspezifischen Anweisungen (Coding Standards, Style Guide PCS 7, etc.) die Regeln zur Erstellung von Softwareelementen definiert sein.

Siehe auch

- Handbuch "PCS 7 APL Styleguide", Online-Support unter Beitrags-ID 65601446 (https://support.industry.siemens.com/cs/ww/de/view/65601446)
- Handbuch "PCS 7 Kompendium Teil A", Kapitel 8.1.2 "Erstellung eigener technologischer Bausteinen", Online-Support unter Beitrags-ID 109809015 (https://support.industry.siemens.com/cs/ww/de/view/109809015)

6.5 Schnittstellen zu SIMATIC PCS 7

6.5.1 PCS 7 OS Web Option

Diese Option ermöglicht die Prozessbedienung und –beobachtung des PCS 7-Systems über eine Internet-/Intranetverbindung. Dazu sind ein PCS 7 OS Web Server und mindestens ein PCS 7 Web Client erforderlich.

Innerhalb eines PCS 7 OS Mehrplatzsystems ist der PCS 7 OS Web Server installiert als OS-Client mit PCS 7 OS Web Server-Funktionalität. Dieser sollte nicht zusätzlich als Bedienstation (OS-Client) genutzt werden. Dies kann durch die Deaktivierung der Graphics Runtime sichergestellt werden.

Beim Installieren des Web Clients wird automatisch der **WebViewer** installiert. Es wird empfohlen für Remote-Zugriffe diesen anstelle des Internet Explorers vorrangig zu nutzen, da der WebViewer individuell konfiguriert werden kann.

Der Web Server selbst sollte mit einem Zertifikat ausgestattet werden, damit ein gesicherter, authentifizierter und verschlüsselter Zugriff auf die Web Server-Funktionalität stattfindet (Stichwort: https-Zugriff).

Auf dem OS Web Server werden alle Bilder und erforderlichen Skripte abgelegt, sodass sie auf dem Web Client angezeigt werden bzw. ablaufen können. Dazu müssen alle Bilder und Skripte publiziert werden. Hierzu wird der "Web View Publisher" verwendet.

Siehe auch

- Handbuch "PCS 7 Web Option für OS", Online-Support unter Beitrags-ID 109794376 (https://support.industry.siemens.com/cs/ww/de/view/109794376)
- Handbuch "PCS 7 Kompendium Teil A", Kapitel 10.2 "Visualisierungsoberfläche", Online-Support unter Beitrags-ID 109809015 (https://support.industry.siemens.com/cs/ww/de/view/109809015)

Hinweis

Bei der Verwendung von Skripten sollte ereignisgesteuerte Skriptbearbeitung soweit wie möglich bevorzugt werden, da diese ressourcenschonender ist. Zyklische Skripte hingegen sollten nur gezielt bei Bedarf eingesetzt werden.

SIMATIC Logon muss auf dem Web Server installiert werden und bindet dadurch den Web Client in die Funktionen von SIMATIC Logon mit ein. Der Zugriff der Web Clients erfolgt somit passwortgeschützt. Die Benutzerrechte werden in der OS User Administration vergeben. Sie entsprechen denen der Standard-Clients, nur die Option Intranet-/Internet-Zugriff muss zusätzlich aktiviert werden.

Siehe auch

- Kapitel "Informationssicherheit und Datenintegrität (Seite 55)"
- Handbuch "Sicherheitskonzept PCS 7 und WinCC", Online-Support unter Beitrags-ID 109780811 (https://support.industry.siemens.com/cs/ww/de/view/109780811)

Load Balancing (Lastverteilung) Funktionalität

Beim Einsatz mehrerer Web Navigator Server ist es mit Hilfe der Funktionalität "Load Balancing" möglich eine gleichmäßige Lastverteilung zu erreichen. Außerdem werden die Web Clients bei Ausfall eines Web Servers automatisch auf andere Web Server umverteilt. Dies funktioniert indem aus den teilnehmenden Web Navigation Servern vorher ein Load Balancing Server ausgewählt wurde. Meldet sich dann ein Web Client an einem Load Balancing Server an, so verteilt dieser den Web Client an den Server mit der geringsten Last.

Um die Funktionalität von Load Balancing nutzen zu können, muss diese auf jedem teilnehmenden Web Server projektiert werden. Voraussetzung ist, dass das WinCC Basissystem und der Web Navigator Server installiert sind. Die Web Server sind identisch (gilt auch für die Benutzeradministration) einzurichten und die Standard-Webseite ist für Web Navigator einzustellen.

Im WinCC Explorer ist über das Kontextmenü des Web Navigators die Konfiguration der Funktion Load Balancing zu öffnen. In dem sich öffnenden Fenster ist jeder einzelne Web Server mittels seiner IP-Adresse in die Liste aufzunehmen. Bei dem Load Balancing Server ist zusätzlich das Häkchen "Load Balancing erlauben" zu aktivieren und ein Polling-Intervall einzustellen.

Hinweis

Web Server mit einer "Web Navigator Diagnose Server" Lizenz dürfen nicht in die Load Balancing Teilnehmerliste aufgenommen werden.

Die Anwendung "WinCCViewerRT.exe" unterstützt die Funktion "Load Balancing" nicht.

Thin Client

Bei einer Thin Client Lösung können der Terminal Server und der Web Server auf einem Rechner betrieben werden. Dabei wird auf dem Terminal Server für jeden Thin Client eine Terminal Session geöffnet. Über Remote Desktop Protokoll (RDP) kann dann von den Thin Clients auf den Terminal- und Web Server zugegriffen werden. Da es sich um eine dienst-basierte Funktionalität handelt, muss kein Benutzer am Terminal Server angemeldet sein.

Eine Thin Client Lösung zeichnet sich durch eine hohe Wartungsfreundlichkeit aus, da Änderungen nur noch einmalig am Terminal Server vorgenommen werden müssen und dann jedem Thin Client zur Verfügung stehen.

Siehe auch

- Handbuch "Industrial Thin Clients", Online-Support unter Beitrags-ID 109801145 (https://support.industry.siemens.com/cs/ww/de/view/109801145)

WebUX

WebUX ermöglicht den Zugriff über einen HTML 5 fähigen Browser auf für WebUX geeignete Prozessbilder. Die Funktionalität ist im Vergleich zum Web Client stark eingeschränkt.

Im Interesse der Prozesssicherheit werden ausschließlich verschlüsselte HTTPS-Verbindungen mit SSL Zertifikaten unterstützt.

Die Benutzerrechte mit Zugriff auf den WebUX Server sind im WinCC User Administrator in Verbindung mit SIMATIC Logon zu konfigurieren. Empfohlen wird insbesondere bei kritischen Bedienhandlungen ein reiner Lesezugriff.

Siehe auch

- Handbuch "WinCC Basic Options", Online-Support unter Beitrags-ID 109792604 (https://support.industry.siemens.com/cs/ww/de/view/109792604)

Hinweis

Das Einrichten eines Web-Servers ermöglicht eventuell den Zugang zu Ihrer Anlageninfrastruktur. Schützen Sie darum den Rechner, auf dem der Web-Server installiert ist. Stellen Sie sicher, dass folgende Regeln eingehalten werden:

- Der Rechner ist nur über gesicherte Verbindungen erreichbar.
- Die von Software-Herstellern vorgesehenen Prüfmechanismen sind aktiviert und werden in keinem Fall umgangen.

6.5.2 OS Client in einer virtuellen Umgebung

Auf leistungsfähigen Rechnern (siehe VMware Systemanforderungen (https://www.vmware.com/resources/compatibility/search.php)) können mehrere virtuelle Umgebungen geschaffen werden. Diese dienen dann von der eigentlichen Hardware unabhängig als Basis für einen OS Client. OS Clients sind in einer virtuellen Umgebung freigegeben.

Beim Betrieb eines OS Clients in einer virtuellen Umgebung erfolgt das Bedienen und Beobachten über einen Thin Client, der an die VMware ESXi Plattform angebunden wird. Auf der ESXi Plattform können mehrere Virtualisierungen gleichzeitig ablaufen, jedoch ist lediglich eine Remote Desktop-Verbindung pro Virtualisierung möglich. Über die Auswahl des Thin-Client können bis zu 4 Monitore angeschlossen werden. Ist eine Anbindung von USB-Geräten am OS-Client erforderlich, erfolgt die Verbindung über den zugeordneten Thin Client bzw. über einen zentralverwalteten USB-Device-Server.

Siehe auch

- Freigabe von PCS 7 Komponenten für virtuelle Umgebung, Online-Support unter Beitrags-ID 109795917 (https://support.industry.siemens.com/cs/ww/de/view/109795917)
- Handbuch "PCS 7 Virtualisierung - Projektierung und Konfiguration", Online-Support unter Beitrags-ID 109801455 (https://support.industry.siemens.com/cs/ww/de/view/109801455)
- GAMP Good Practice Guide "IT Infrastructure" 2nd Edition, Kapitel 19

6.5.3 Open PCS 7

Mit Open PCS 7 stehen Daten aus PCS 7 auch übergeordneten Systemen wie z. B. der Betriebsleitebene zur Verfügung. Folgende Standardschnittstellen werden zum Datenaustausch von Open PCS 7-Stationen angeboten:

- OPC UA (Unified Architecture)
- OPC "Classic"
  - OPC DA (Data Access)
  - OPC A&E (Alarm & Events)
  - OPC HDA (Historical Data Access)
  - OPC H A&E (Historical Alarm & Events)
- OLE/DB für OLE-fähige Anwendungen, z. B. Microsoft Office Produkte;
  OLE/DB erlaubt Zugriff auf historische Werte, Alarme und Meldungen über standardisierte Datenbankaufrufe

Mit der Open PCS 7-Station kann auf mehrere redundante Server-Paare zugegriffen werden. Bei Ausfall des aktiven Servers wird automatisch auf den verbliebenen Server umgeschaltet, so dass der nächste Leseauftrag von diesem Server erfolgt.

Eine Verbindung über OPC UA (Unified Architecture) bietet eine erhöhte Sicherheit in der Datenkommunikation im Vergleich zur OPC DA Verbindung. OPC UA Server und OPC UA Client stellen jeweils ein Zertifikat bereit. Diese Zertifikate müssen die Verbindungspartner austauschen und jeweils akzeptieren. Nur dann kann eine erfolgreiche Datenkommunikation stattfinden.

Zugriff auf die Station	OPC Schnittstelle	Datentyp
OS-Server	UA	Prozesswerte und Meldungen
OS-Server	DA	Variablen des Prozessbildes
OS-Server	A&E	Alarme und Meldungen
OS-Server	HDA	Historische Messwerte (Tag Logging)

Zugriff auf die Station	OPC Schnittstelle	Datentyp
OS-Server	H A&E	Historische Alarme und Meldungen (Alarm Logging)
OS-Server	OLE-DB	Direktzugriff auf Archivdaten

Siehe auch

- Handbuch "OpenPCS 7", Kapitel 7.1 "Zugriffsmöglichkeiten", Online-Support unter Beitrags-ID 109794368 (https://support.industry.siemens.com/cs/ww/de/view/109794368)

Vorteile von OPC UA gegenüber vorherigen OPC Spezifikationen sind:

- Integriertes Sicherheitskonzept (Authentifizierung und Autorisierung, Verschlüsselung und Datenintegrität)
- Unabhängig von DCOM, keine DCOM Settings erforderlich
- Betriebssystemunabhängig, Herstellerunabhängig
- Vereinheitlichung der bisherigen OPC-Normen zu einer Schnittstelle; ein gemeinsamer OPC Standard für Tags, Alarme und historische Daten
- Kommunikation über einen einzigen Firewall Port

Hinweis

Die OPC-Verbindung soll nicht als erweiterte Bedienquelle dienen, sondern im Wesentlichen der Datenauswertung oder Information. Bei der Einrichtung einer OPC-Verbindung muss daher besonderer Wert auf die Datensicherheit und die Vergabe von Schreibrechten gelegt werden. Für jede OS-Variable können Sichtbarkeit und Schreibrechte einzeln konfiguriert werden.

Für eine eventuell erwünschte Bedienung von außerhalb der PCS 7 Umgebung sollte die PCS 7 OS Web Option gewählt werden, siehe Kapitel "PCS 7 OS Web Option (Seite 98)".

6.5.4 SIMATIC BATCH API

SIMATIC BATCH API (Application Programming Interface) bietet als Programmier-Schnittstelle folgende Funktionsaufrufe:

- Zugriff auf BATCH Objekte und Daten
- Durch SIMATIC BATCH Objekt-Hierarchien navigieren
- Benachrichtigungen über Ereignisse

Als Anwendungsgebiet ist z. B. die Datenschnittstelle zur Übertragung von Ereignissen und Methoden (z. B. CreateBatch, ArchiveBatch, GetParameter etc.) zu einer MES-oder ERP-Ebene zu erwähnen.

6.6 Rezeptursteuerung mit SIMATIC BATCH

SIMATIC BATCH ist ein Softwarepaket für SIMATIC PCS 7, welches diskontinuierliche Prozesse, sogenannte Chargenprozesse, plant, überwacht und steuert.

Ein wesentlicher Vorteil der Chargenproduktion ist die Erfassung und Archivierung von Produktionsdaten. Diese Produktionsdaten werden sowohl für die behördlichen Anforderungen zur Rückverfolgung (Audit Trail) als auch zur betrieblichen Analyse des Produktionsvorganges benötigt.

6.6.1 Batch Begriffsdefinitionen

Nachfolgend werden einige häufig verwendete Batch-Begriffe beschrieben.

Begriff	Beschreibung
Grundrezept	Vorschrift zur Herstellung eines Produktes nach einer bestimmten Prozedur
Steuerrezept	Kopie des Grundrezeptes, ergänzt um anlagenspezifische Informationen und entsprechende Skalierung der gewünschten Produktionsmenge
Charge	Apparateabhängige Menge eines Produktes, welche in einem definierten Produktionsablauf diskontinuierlich hergestellt wird
Verfahren	Ablauf von chemischen, physikalischen oder biologischen Vorgängen zur Herstellung von Stoffen oder Produkten

6.6.2 Normkonformität mit ISA-88.01

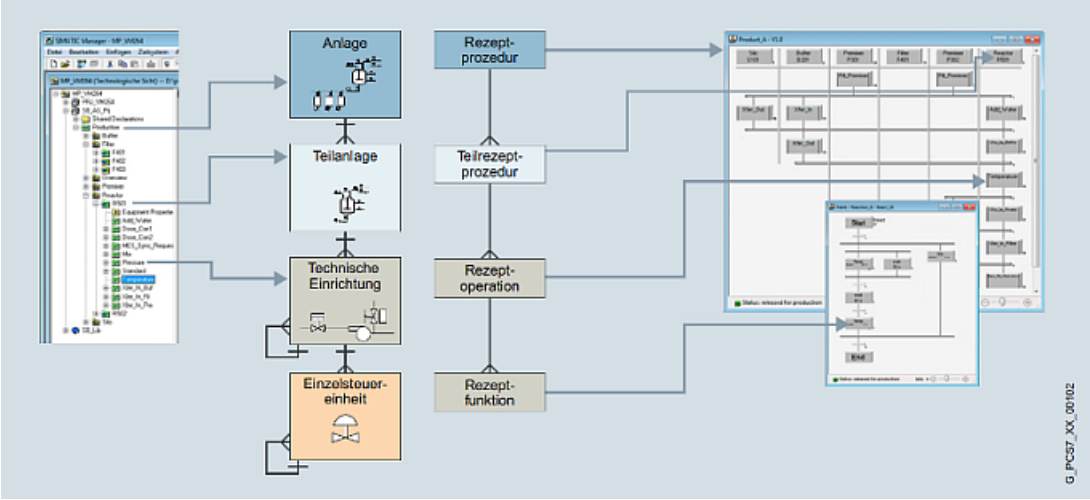
ISA-88 ist eine internationale Norm für die chargenorientierte Fahrweise, die Designvorgaben für Software, Ausrüstung und den Verfahrensablauf darstellt. SIMATIC BATCH wurde auf Basis der Norm *ANSI/ISA-88.00.01 (Batch Control, Part 1: Models and Terminology)* entwickelt.

Im "Technical Report" *ISA-TR88.0.03* wird u. a. die Verwendung von SFC (Sequential Function Charts, DIN/IEC 1131) als grafische Sprache zur Beschreibung von Rezeptabläufen empfohlen. Die Rezepterstellung mit dem SIMATIC BATCH Rezepteditor folgt den in dieser Norm beschriebenen Strukturen und Funktionalitäten.

SIMATIC BATCH stellt Produktionsdaten gemäß *ISA-88.00.04 (Batch Production Records)* bereit.

Software-Modell SIMATIC PCS 7

Die ISA-88.01 beschreibt verschiedene Modelle, die mit PCS 7 und SIMATIC BATCH vollständig abgedeckt werden können.



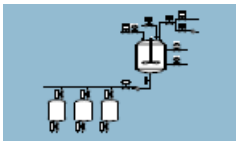
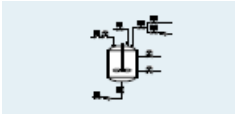
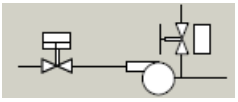
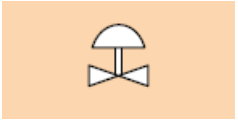
Das **Anlagenmodell** (physisches Modell) beschreibt die Anlage, Teilanlage, Technische Einrichtung und Einzelsteuerebene, die über die Technologische Hierarchie in der Anlagensicht des SIMATIC Managers abgebildet wird.

Das **prozedurale Modell** (Prozedur, Teilprozedur, Operation, Funktion) spiegelt in SIMATIC BATCH das Anlagenmodell aus Sicht des Steuerungsablaufs wieder.

Begriff	Beschreibung
Rezeptprozedur	Eine Rezeptprozedur läuft auf einer Anlage, um einen Prozess zu steuern und eine Charge eines Produktes herzustellen.
Teilrezeptprozedur	Eine Teilrezeptprozedur läuft auf einer Teilanlage, um eine Rezeptstufe zu steuern. Eine Teilanlage kann zu einem Zeitpunkt nur von einer Charge belegt werden.
Rezeptoperation / Rezeptfunktion	Eine Rezeptoperation oder eine Rezeptfunktion läuft auf einer Technischen Einrichtung, um eine verfahrenstechnische Aufgabe oder Funktion zu erfüllen.
Einzelsteuerebene	Die Einzelsteuerebene liegt nicht im Scope des Batch-Systems und wird nur über die Technische Einrichtung angesprochen. Die Einzelsteuerebene befindet sich komplett im Automatisierungssystem.

Anwendung der Norm ISA-88.01 auf SIMATIC PCS 7

Das ISA-88.01 Software-Modell teilt den Prozess in verschiedene Module auf, wodurch der Prozess der Validierung vereinfacht wird. Der Prozess wird hierbei in folgende Teile hierarchisch aufgespaltet.

Physisches Modell (de - en)	**Grafik**	**Prozedurale Elemente (de - en)**	**Umsetzung in PCS 7**	**Umsetzung durch**
Anlage Process Cell		Prozedur Procedure	Komponente Batch: Rezept	Betreiber / unterstützend durch Lieferant
Teilanlage Unit		Teilprozedur Unit Procedure(s)	Komponente CFC: Unit Baustein Komponente Batch: Teilrezepte	Betreiber / unterstützend durch Lieferant
Technische Einrichtung Equipment Module (EM)		Rezeptoperation / -funktion Recipe Operation / Phase (kann Fahrweisen enthalten)	Komponente SFC-Typ: Einsatz von SFC-Typen zur Instanzierbarkeit. (Equipment Phasen, Equipment Operationen)	Lieferant / unterstützend durch Betreiber
Einzelsteuer-funktion Control Module (CM)		-	Komponente CFC: Einsatz der PCS 7 Library und Nutzung von CFC-Plänen.	Lieferant

Die SIMATIC PCS 7 Industry Library beinhaltet spezifische Funktionen, die ein durchgängiges und ISA-88-konformes Engineering- & Bedienkonzept inklusive Batch-Integration ermöglichen..

Hinweis

Die Benennung und Funktionalität der Module erfolgt gemäß den Vorgaben aus der Spezifikation.

Siehe auch

- Handbuch "PCS 7 SIMATIC BATCH", Online Support unter Beitrags-ID 109794450 (https://support.industry.siemens.com/cs/ww/de/view/109794450)
- Anwendungsbeispiel "Projektierung von Batch-Prozessen anhand von ISA-88", Online Support unter Beitrags-ID 109784331 (https://support.industry.siemens.com/cs/ww/de/view/109784331)

6.6.3 Projektierung von SIMATIC BATCH

Grundlagen und Optionen von SIMATIC BATCH sind im Kapitel "Softwarekomponenten Engineering (Seite 30)" erläutert.

Siehe auch

- Handbuch "Getting Started PCS 7 SIMATIC BATCH", Online-Support unter Beitrags-ID 109781909 (https://support.industry.siemens.com/cs/ww/de/view/109781909)
- Handbuch "PCS 7 Kompendium Teil C", Online-Support unter Beitrags-ID 109804258 (https://support.industry.siemens.com/cs/ww/de/view/109804258)

Die einzelnen Projektierungsschritte teilen sich auf in:

Arbeiten im SIMATIC Manager

Unter anderem folgende Schritte erfolgen im SIMATIC Manager:

- Anlegen und Konfigurieren von Batch-Systemen (Server, Clients)
- Erstellen der Technologischen Hierarchie
- Übersetzen der OS-Daten
- Batch-Typen generieren und propagieren
- Daten an OS übertragen
- Laden der Anlagendaten

Arbeiten im BATCH Control Center (BCC) und Rezepteditor (RP)

Hier werden unter anderem diese Schritte durchgeführt:

- Einlesen / Aktualisieren der Batchdaten
- Anlegen der Grundrezepte
- Erstellen der Rezeptstruktur
- Erstellen ROP-Bibliotheken, Formula-Kategorien und Formulas
- Anlegen von Auftragskategorie, Auftrag und Charge(n)
- Freigaben für Grundrezepte sowie für abgeschlossene Chargen
- Exportieren / Importieren von Rezepten, Parametersätzen usw.

Siehe auch

- Anwendungsbeispiele zur Spezifikation technischer Funktionen mit SFC-Typen sowie zur Instanziierung, Online-Support unter Beitrags-ID 33412955 (https://support.industry.siemens.com/cs/ww/de/view/33412955)

6.6.4 Funktionen und Einstellungen in SIMATIC BATCH

Verschiedene Funktionen und Projekteinstellungen können in SIMATIC BATCH genutzt werden. Einige dieser Einstellungen werden im Folgenden vorgestellt. Detaillierte Ausführungen enthält das Bedienhandbuch zu SIMATIC BATCH.

Vordefinierte Chargennamen

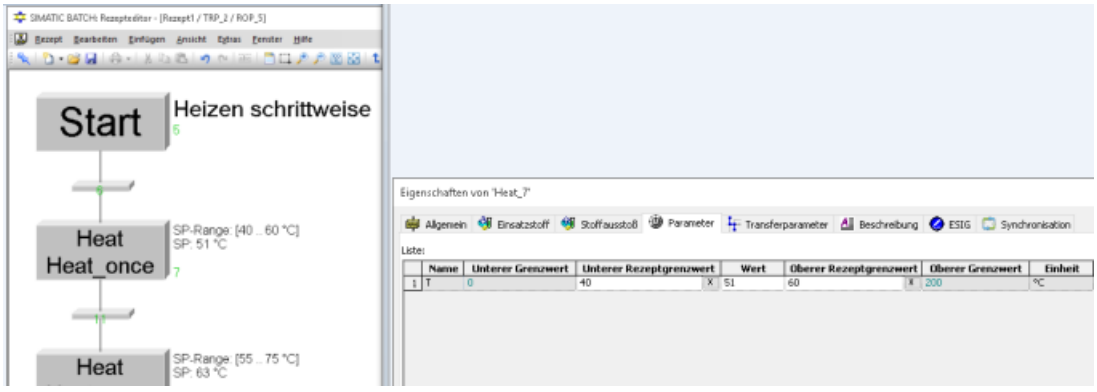
Mit der Funktion "Vordefinierte Chargennamen benutzen" können Chargennamen automatisch aus verschiedenen statischen und dynamischen Elementen erstellt werden.

Hinweis

Die Länge des Chargennamens ist auf 32 Zeichen begrenzt.

Rezeptschrittspezifische Sollwerte

Innerhalb der definierten Equipment-Grenzen kann die Spanne für Sollwerte zusätzlich für jeden Rezeptschritt eingegrenzt werden. So kann der Prozess noch besser geführt und die Qualität des Endprodukts erhöht werden.



Editieren von Rezepten im Zustand "Freigabe aufgehoben/ungültig"

Mit der Einstellung "Nein" verhindern Sie, dass Rezepte im Zustand "Freigabe aufgehoben/ ungültig" und unter gleichem Namen/Version erneut freigegeben werden.

Hinweis

Die Standardeinstellung ist "Ja" und sollte im regulierten Umfeld auf "Nein" gesetzt werden.

Chargen automatisch freigeben

Neu hinzugefügte Chargen werden beim Erzeugen automatisch freigegeben zur Produktion. Die Standard-Einstellung ist "Nein". Bei der Einstellung "Ja" erspart man sich den separaten Freigabeschritt, der bei unterschiedlichen Berechtigungen aber durchaus Sinn machen kann. Eine projektierte Unterschrift zur Freigabe wird auch bei Nutzung der automatischen Freigabe vom System abgefragt.

Exportieren/Importieren von Batch-Objekten

Für den Export / Import von

- Bibliotheken
- Grundrezepten
- Formula-Kategorien und Formulas

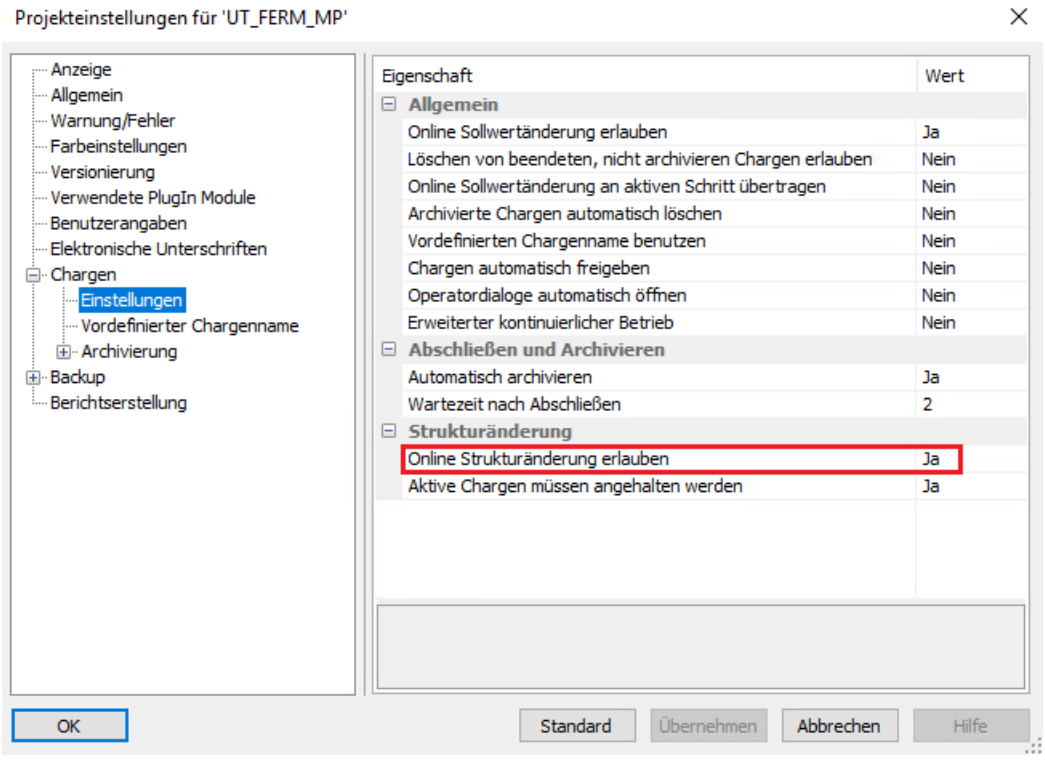
siehe Handbuch "SIMATIC BATCH", Kapitel 9.5.8, Online-Support unter Beitrags-ID 109794450 (https://support.industry.siemens.com/cs/ww/de/view/109794450).

Online Strukturänderungen für Rezeptstrukturen

SIMATIC BATCH bietet die Möglichkeit, Rezeptstrukturen online zu ändern. Dieses gilt für Steuerrezepte, die den Status "freigegeben", "geplant" oder "gestartet" besitzen.

Es gelten die folgenden Bedingungen zur Einstellung:

- Das Grundrezept muss sich im Status "Freigabe zum Test" befinden.
- Der Benutzer muss über das Recht "Strukturänderungen beginnen" verfügen.
- In den Projekteinstellungen muss "Online Strukturänderungen erlauben" gesetzt sein.



Wird die Option "Aktive Chargen müssen angehalten werden" gewählt, so bietet dies bei Änderungen an Rezeptstrukturen den Schutz, eine laufende Charge in einem sicheren Zustand

zu hinterlassen. Nach Durchführung der Änderung muss dann die Charge vom Bediener fortgesetzt werden.

Hinweis

Online-Strukturänderungen sind eine zusätzliche Funktionalität für Grundrezepte im Testbetrieb. Sie dienen zur Vereinfachung während der Optimierung von Rezepten. Online-Strukturänderungen sind nicht im produktiven Betrieb (Grundrezept für Produktion freigegeben) möglich. Standardeinstellung ist "Nein".

Hinweise und Einschränkungen

- Während der Online-Strukturänderung an einer Charge ist der Zugriff auf diese Charge von anderen Clients ausgeschlossen. Ein visueller Abgleich der Änderungen auf alle SIMATIC BATCH Clients erfolgt nach Abschluss der Online-Strukturänderungen.
- Es empfiehlt sich, die Charge bei Strukturänderungen anzuhalten.

Wird die Option "Aktive Chargen müssen angehalten werden" deaktiviert, so kann die Änderung im laufenden Betrieb stattfinden, jedoch mit dem Nachteil, dass die Charge nach Beendigung der Änderungen automatisch die Änderungen übernimmt und aktiviert.

Abgebrochene Chargen löschen

Beachtung sollte z. B. auch der Punkt "Löschen von beendeten, nicht archivierten Chargen erlauben" finden, d. h. abgebrochene Chargen können ohne Archivierung der Daten gelöscht werden. Dies wird im pharmazeutischen Umfeld nur selten gewünscht, daher sollte diese Einstellung abgewählt bleiben, sofern der Kunde es nicht ausdrücklich anders wünscht.

Weitere Einstellungen in SIMATIC BATCH

Wichtige Parameter und Einstellungen sind auch enthalten in

- Kapitel "SIMATIC BATCH (Seite 124)"
- Kapitel "Elektronische Unterschrift in SIMATIC BATCH (Seite 127)"

6.6.5 Meldungen in SIMATIC BATCH

Alle Meldungen der Chargensteuerung, die in den WinCC-Archiven verwaltet werden, können auch auf dem SIMATIC BATCH Client zur Anzeige gebracht werden. Voraussetzung ist, dass eine PCS 7 OS-Applikation auf dem Rechner läuft.

Siehe auch

- Handbuch "SIMATIC BATCH", Kapitel 9.8.7 "Bedien-und Zustandsmeldungen" und Kapitel 15.1.2.3 "Warn- und Fehlermeldungen", Online-Support unter Beitrags-ID 109794450 (https://support.industry.siemens.com/cs/ww/de/view/109794450)

6.6.6 Erstellen von Protokollen in SIMATIC BATCH

Das SIMATIC BATCH Protokoll gewährleistet die Dokumentation der Rezepte und Chargendaten in Form von Protokollen:

- Das Rezeptprotokoll enthält alle Daten, die zur Produktion notwendig sind. Hierzu gehören die Rezeptkopfdaten, die Einsatzstoff- und Stoffausstoßliste sowie die Verfahrensvorschrift.
- Das Chargenprotokoll enthält alle Informationen der produzierten Charge, die für die Reproduzierbarkeit des Chargenprozesses, den Qualitätsnachweis und die Erfüllung gesetzlicher Auflagen notwendig sind.
- Die Protokolle können automatisch als PDF-Datei gespeichert werden.

Das Protokoll ist in die Bedienoberfläche des BATCH Control Center integriert.

Siehe auch

- Handbuch "SIMATIC BATCH", Kapitel 9.5.7 und Kapitel 9.9, Online-Support unter Beitrags-ID 109794450 (https://support.industry.siemens.com/cs/ww/de/view/109794450)
- Erstellen von Berichtsvorlagen für den Information Server auf Datenbasis des Process Historian, Online-Support unter Beitrags-ID 64906050 (https://support.industry.siemens.com/cs/ww/de/view/64906050)

6.7 SIMATIC Route Control

SIMATIC Route Control ist ein Programmpaket von SIMATIC PCS 7, welches das gesamte Prozess-Wegenetz einer Produktionsanlage verwalten und automatisiert aussteuern kann. Durch seine matrixbasierte Konfiguration können Prozess-Wege flexibel ermittelt und mittels unterschiedlicher Fahrweisen (Modes) automatisch ausgesteuert werden. Eine der Hauptanwendungen von SIMATIC Route Control ist der automatisierte Transport von Materialien in Anlagen.

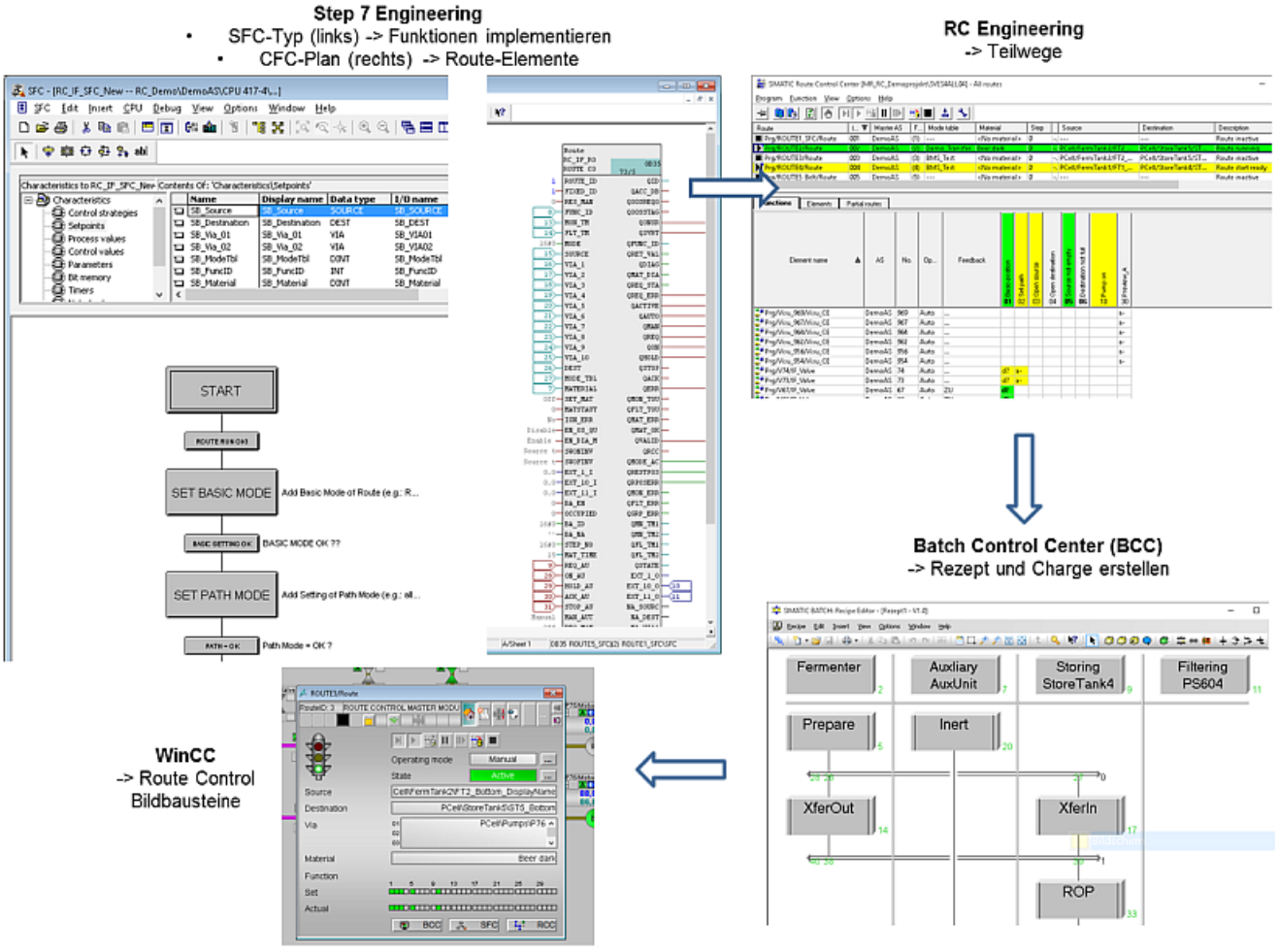
Durch die verständliche Darstellung im SIMATIC Route Control Center lassen sich Produktions- und Reinigungswege einfach belegen, wodurch der Aufwand an Verifizierung erheblich reduziert wird. Des Weiteren wird die Rückverfolgung, das sogenannte Material Tracking, durch SIMATIC Route Control (Route Control Log) sichergestellt.

Typische Applikationsbeispiele sind:

- Transport von Feststoffen und Flüssigkeiten
- Pufferansätze sowie deren Bereitstellung zur Produktion
- Bio-Reaktoren wie z. B. Zellkulturanlagen mit Up-Stream und Down-Stream
- CIP und SIP Prozeduren mit verschiedenen Spülwegen

Für die Nutzung von SIMATIC Route Control wird ein Route Control Server benötigt. Route Control Server können auch redundant ausgelegt werden.

SIMATIC Route Control wird in der Engineering Station von SIMATIC PCS 7 mit Hilfe der Applikation Route Control Engineering konfiguriert. Die nachfolgende Abbildung veranschaulicht die einzelnen Etappen der Projektierung.



Der Einsatz von SIMATIC Route Control rechnet sich bereits ab 5 parallelen Materialtransporten. Ein erheblicher Nutzen liegt hierbei im Engineering. Durch das SIMATIC Route Control Engineering werden Wege und Teilwege systemunterstützt erstellt.

Wichtige Funktionen von SIMATIC Route Control sind:

- Automatische Prüfung und Berücksichtigung von Materialverträglichkeiten (z.B. Materialfolgen)
- Alternative Transferwege im Störfall (Automatik)
- Status-Check der Leitung
- Skalierung je nach Anlagengröße
- Anlagenerweiterung ohne Programmieraufwand

Siehe auch

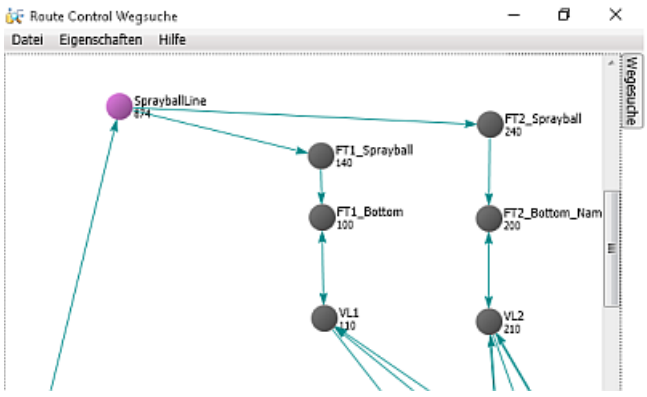
- Handbuch "SIMATIC PCS 7 Route Control", Online-Support unter Beitrags-ID 109794449 (https://support.industry.siemens.com/cs/ww/de/view/109794449)
- Produktbeschreibung im Internet (https://new.siemens.com/de/de/produkte/automatisierung/prozessleittechnik/simatic-pcs-7/wegesteuerung.html)

Import / Export

Mit Hilfe der CSV-Schnittstelle (CSV-Export/-Import) kann die Projektierung in SIMATIC Route Control noch weiter vereinfacht und beschleunigt werden. So können z. B. Teilwege und weitere Daten komfortabel in Excel bearbeitet und anschließend in Route Control Engineering importiert werden. Die Excel-Bearbeitung kann auch zur effizienten Definition der Wege in der Spezifikationsphase und anschließendem Import genutzt werden.

Graphische Wegesuche

Eine weitere Funktion ist die Graphische Wegesuche. Hiermit können Wegenetze auf graphische Art geprüft werden.



Außerdem können Wege gespeichert und bevorzugt anstelle der automatischen Wegesuche verwendet werden.

6.8 Alarm Management

Ein Alarmsystem sollte grundsätzlich die folgenden Anforderungen erfüllen:

- Warnen des Bedieners bei Anlagenstörungen
- Bereitstellung von Informationen über die Eigenschaften der Störung
- Hinführen des Bedieners zur wichtigsten Störung
- Unterstützung bei der Bewertung mehrerer anstehender Störungen

6.8.1 Spezifikation

Zur Spezifikation eines Alarm Systems gehören

- Definition der Formate für Meldezeile und Meldeseite
- Meldeklassen, -farben und -prioritäten
- Quittierungskonzept (z. B. Einzelquittierung)

- Ereignistexte, z. B. "zu hoch" für einen oberen Alarm
- Prozessabhängige Unterdrückung von Alarmen, z. B. Unterdrückung der Durchflussüberwachung bei ausgeschalteter Pumpe,

sofern diese vom Standard abweichen.

Die voreingestellten Standards für die Darstellung von Meldeklasse, -farbe und -priorität sollten nach Möglichkeit beibehalten und nur auf Kundenwunsch verändert werden.

Hinweis

Bei vom Standard abweichender Konfiguration des Alarm-Systems müssen diese Abweichungen dokumentiert sowie ein Vorgehen im Falle von Updates beschrieben werden, siehe hierzu auch Kapitel "System Updates und Migration (Seite 175)".

Siehe auch

- Handbuch "PCS 7 Kompendium Teil A", Kapitel 8.1.4 "Meldeklasse, Priorität ...", Online-Support unter Beitrags-ID 109809015 (https://support.industry.siemens.com/cs/ww/de/view/109809015)

6.8.2 Meldeklassen

Die verschiedenen Meldeklassen wie Störung, Alarm, Warnung oder Leittechnik-Meldung werden üblicherweise funktions- und ereignisspezifisch festgelegt. So werden bei einer Messung z. B. die äußeren Grenzen als Alarme und die inneren als Warnungen gemeldet, während ein Laufzeitfehler an einem Ventil z. B. eine Störungsmeldung auslöst.

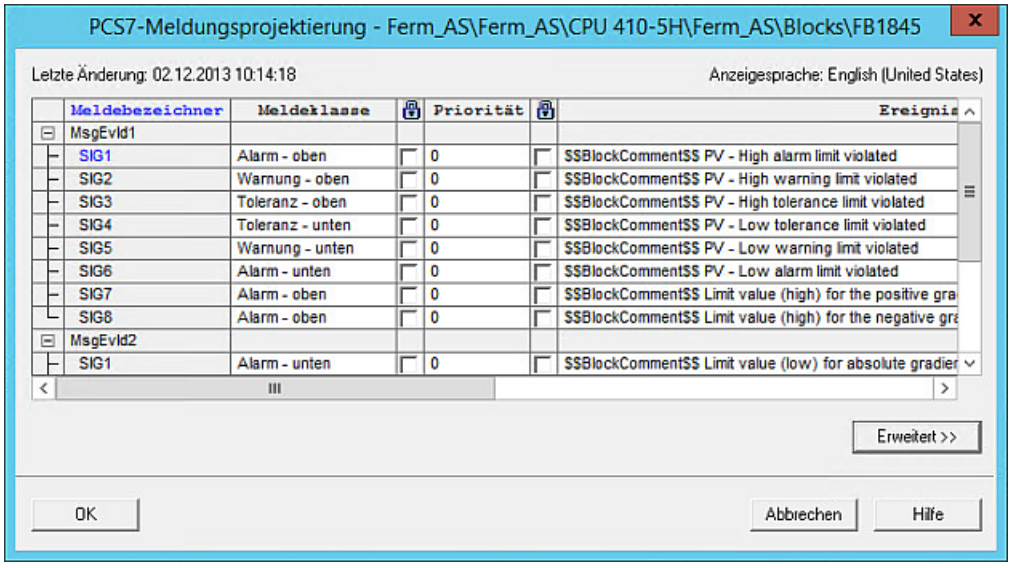
Siehe auch

- Handbuch "PCS 7 Kompendium Teil A", Kapitel 10.3.1 "Meldeklassen und Meldearten", Online-Support unter Beitrags-ID 109809015 (https://support.industry.siemens.com/cs/ww/de/view/109809015)

6.8.3 Prioritäten

Damit die Handlungsfähigkeit der Anlagenfahrer auch in kritischen Situationen erhalten bleibt, können Meldungen abhängig von ihrer möglichen Auswirkung (Anlagenstillstand, Qualitätsverlust für Produkt bzw. Produktionsverzögerung) und der verfügbaren Reaktionszeit (z. B. < 5 Minuten, 5 – 20 Minuten, > 20 Minuten) in PCS 7 zusätzlich priorisiert werden.

Die Priorität wird in SIMATIC PCS 7 bei der Meldeprojektierung instanzspezifisch festgelegt und ist zunächst auf "0" voreingestellt. Die Einstellung der Prioritäten erfolgt in der Prozessobjektsicht im Reiter ‚Meldungen', wie die folgende Abbildung zeigt.



Tipp: Die Meldepriorität eignet sich auch dazu, alle GMP relevanten Meldungen z. B. als Priorität 1 zu kennzeichnen. So sind diese später beim Audit Trail Review leicht filterbar.

6.8.4 Unterdrücken, filtern, verbergen

Sperren von Meldungen

Im Prozessbetrieb hat der Anlagenbediener die Möglichkeit, einzelne Messstellen in den Status "Out of Service" zu setzen und dadurch alle Meldungen von dieser Messstelle zu unterdrücken, sofern er die entsprechenden Rechte besitzt.

Diese Funktion wird z. B. dann verwendet, wenn eine Messstelle neu in Betrieb genommen wird. Der Bediener kann durch diese Maßnahme momentan "sinnlose" Meldungen unterdrücken und seine volle Aufmerksamkeit auf die relevanten Meldungen fokussieren.

Objekte mit unterdrücktem Meldeverhalten sind für den Bediener auf allen Ebenen der Bedienstation erkennbar.

Filtern von Meldungen

Das Filtern von Meldungen innerhalb der Alarmlisten kann benutzerspezifisch angepasst werden. Filterkriterien sind die Eigenschaften einer Meldung (Datum, Zeit, Meldeklasse, Meldungstext, etc.). Das Ziel der Onlineänderung der Filterkriterien ist die temporäre Fokussierung auf einen bestimmten Zeitraum, Ereignis usw. bei der Fehleranalyse.

Verbergen von Meldungen (Smart Alarm Hiding)

Diese Funktion ermöglicht das situationsbedingte Ausblenden von Alarmen.

Diese Meldungen werden bei der Sammelstatusbildung nicht berücksichtigt, d. h. der Sammelstatus einer Messung mit anstehendem, verstecktem Alarm zeigt im Prozessbild keinen

Alarmstatus an, wird bei der Bildung der Sammelanzeige für das Bild ignoriert und löst kein akustisches Signal (Hupe) aus.

Die aktuell anstehenden und ausgeblendeten Meldungen sind zu jeder Zeit in der Liste der ausgeblendeten Meldungen ersichtlich. Alle Meldungen, die mit der aktuellen Einstellung ausgeblendet werden, sind in der Liste "Auszublendende Meldungen" zusammengefasst. Das Ausblenden bezieht sich ausschließlich auf die Visualisierung, d. h. ausgeblendete Meldungen werden sowohl archiviert als auch bei einer Redundanzumschaltung der Server bei dem Archivabgleich berücksichtigt.

Das "Smart Alarm Hiding" bietet zwei Möglichkeiten zum Ausblenden von Alarmen:

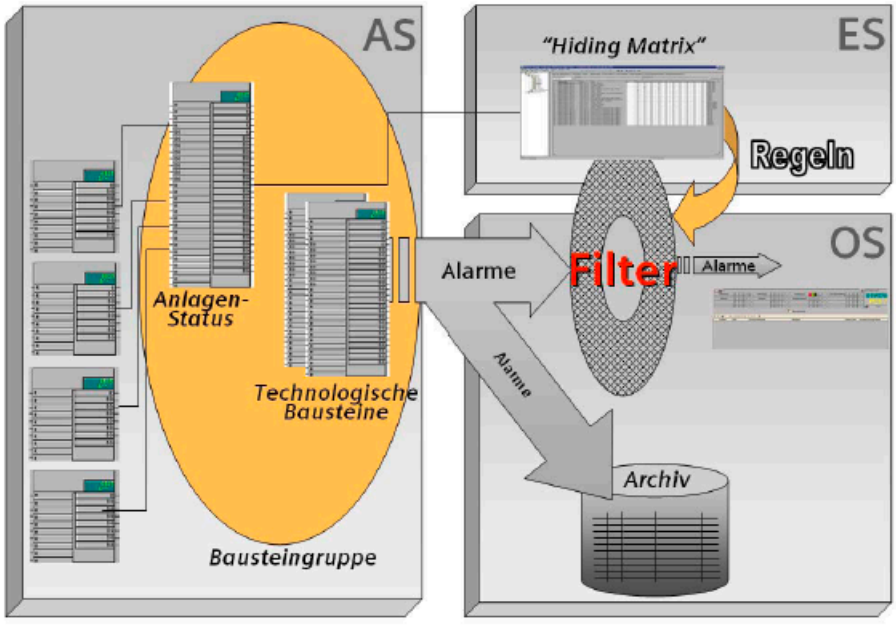
- Manuelles Ausblenden und Einblenden von Alarmen
- Automatisches Ein- und Ausblenden von Alarmen abhängig von Prozesszuständen

Manuelles Ausblenden der Alarme:

- Die Alarme werden nach definierter Zeit wieder eingeblendet.
- Manuell ausgeblendete Alarme werden automatisch quittiert.
- Manuelles Alarm Hiding gilt auf allen Clients des jeweiligen OS-Servers.
- Beim manuellen Aus- und Einblenden wird eine Bedienmeldung abgesetzt. Hierbei kann auch eine Begründung aus einer Auswahlliste angegeben werden.

Automatisches Ausblenden der Alarme:

Das automatische Alarm Hiding muss projektiert werden und wird grundsätzlich über Status-Bausteine im AS gesteuert, die in Verbindung mit einer Hiding-Matrix zustandsabhängig Alarme aus- oder einblenden. Die Zuordnung der technologischen (meldenden) Bausteine zu einem Status-Baustein erfolgt über die neue Baustein-Eigenschaft "Bausteingruppe".

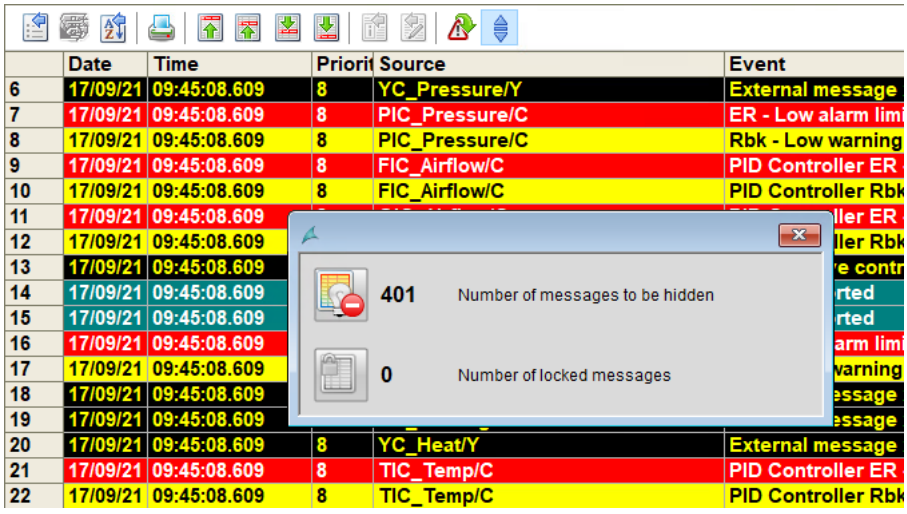


Hinweis

Der wesentliche Unterschied zwischen Meldeunterdrückung und Alarm Hiding besteht darin, dass unterdrückte (gesperrte) Meldungen an der jeweiligen Messstelle erst gar nicht erzeugt und somit nicht an das OS gesendet werden. Sie werden also auch nicht aufgezeichnet und archiviert.

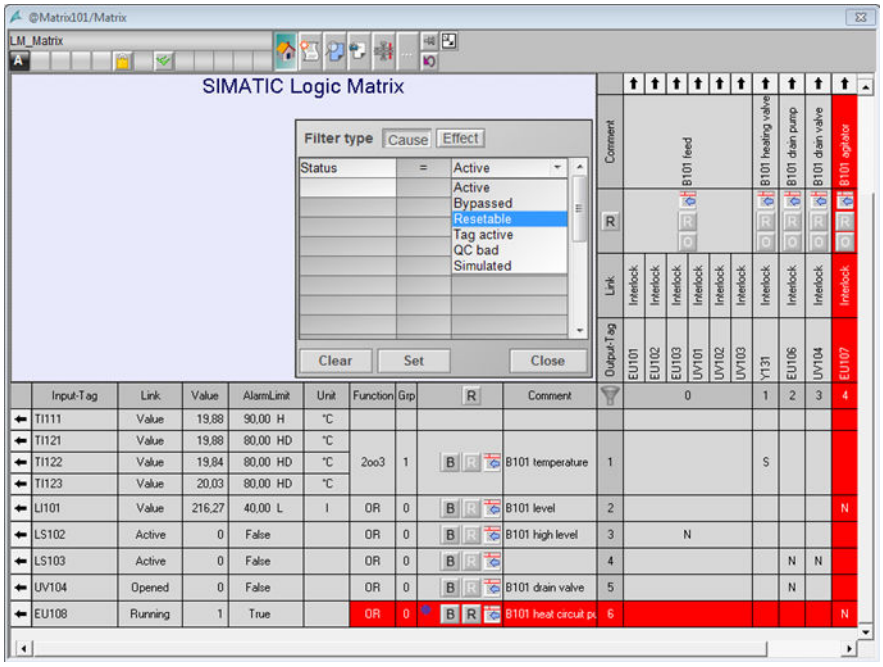
Das Alarm Hiding hingegen hat ausschließlich Auswirkung auf die Visualisierung.

Im Übersichtsbereich weist ein Symbol den Bediener auf vorhandene verriegelte oder ausgeblendete Alarme hin.



6.8.5 SIMATIC PCS 7 Logic Matrix

Die SIMATIC Logic Matrix vereinfacht die Projektierung von Verriegelungslogik. Der direkte Vorteil ist die Übersichtlichkeit, durch die zum einen Fehler in der Projektierung unwahrscheinlicher werden. Zum anderen erleichtert es die Überprüfung des Codes und damit auch die Validierung.



Die Abbildung zeigt die Oberfläche der SIMATIC Logic Matrix auf der Operator Station. Links unten sind die Eingänge dargestellt, rechts oben die Ausgänge. Man kann auf einen Blick die Ursache und die Wirkung erfassen.

Siehe auch

- Handbuch "SIMATIC PCS 7 Logic Matrix", Online-Support unter Beitrags-ID 109794041 (https://support.industry.siemens.com/cs/ww/de/view/109794041)

6.8.6 Überwachung von PCS 7 Komponenten – Lifebeat Monitoring

Das SIMATIC PCS 7 Lifebeat Monitoring ermöglicht die Überwachung der Automatisierungs- und Operator-Stationen auf Funktionstüchtigkeit. Hierzu müssen alle Automatisierungs- und Operator-Stationen in HW-Konfig konfiguriert und die OPC-Verbindungen zu den Operator Stationen angelegt sein.

Die Konfiguration der zu überwachenden Teilnehmer erfolgt im WinCC-Explorer unter dem Menübefehl *Editor > Lifebeat Monitoring > Öffnen*. Hier können alle zu überwachenden Teilnehmer sowie der Überwachungszyklus, in dem die Lebenszeichenüberwachung durchgeführt werden soll, eingerichtet werden. Sobald eine konfigurierte Station auf die Überwachungsanforderung nicht antwortet, wird eine Leittechnikmeldung ausgelöst.

Das Lifebeat Monitoring wird automatisch beim Anlauf der OS aktiviert.

Siehe auch

- Handbuch "PCS 7 Operator Station", Online-Support unter Beitrags-ID 109794374 (https://support.industry.siemens.com/cs/ww/de/view/109794374)

Hinweis

Alternativ können alle leittechnischen Einrichtungen auch über das PCS 7 Asset Management verwaltet werden. Das Asset Management erfordert keine zusätzliche Projektierung, siehe auch Kapitel "Asset Management (Seite 171)". Über eine Maintenance Station kann man sich einen Überblick über die Diagnose- und Serviceinformationen aller Einrichtungen verschaffen. Eine Lebenszeichenüberwachung mit "Lifebeat Monitoring" einer Anlage mit Maintenance Station ist jedoch nicht zulässig.

6.8.7 Überwachung von PCS 7 Komponenten – SMMC

Die SIMATIC Management Console (SMMC) ist ein Programmpaket, das die Überwachung, Dokumentation und Verwaltung der installierten Hard- und Software unterstützt. Zur Nutzung der SMMC ist das Softwarepaket auf einem Rechner zu installieren, hierbei sollte entweder ein separater Rechner oder die vorhandene ES verwendet werden. Zusätzlich ist auf allen zu verwaltenden Rechnern der "SIMATIC Management Agent" zu installieren.

Über die SMMC können nun detaillierte Berichte über die aktuell installierte Hard- und Software erstellt werden. Die hierfür erforderlichen Daten holt sich die SMMC direkt von den Rechnern und AS Systemen der Anlage. Die Dokumentation entspricht immer dem tatsächlichen "As Built" Zustand auf der Anlage.

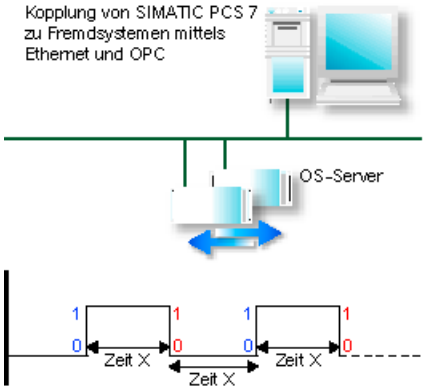
Die Berechtigungen für die SIMATIC Management Console müssen separat eingerichtet werden.

Siehe auch

- Handbuch "SIMATIC Management Console", Kapitel 4.1, Online-Support unter Beitrags-ID 109794443 (https://support.industry.siemens.com/cs/ww/de/view/109794443)

6.8.8 Überwachung angebundener Systeme

Das Lifebeat Monitoring zu angebundenen Systemen muss manuell konfiguriert werden. Es ist jeweils abhängig vom Kommunikationspartner. Stellt das angebundene System eine wichtige Schnittstelle zu SIMATIC PCS 7 dar, so ist ein Lifebeat Monitoring zwingend erforderlich.



Die Grafik zeigt ein Beispiel für eine Lösung des Lifebeat Monitoring zu einem Fremdsystem. SIMATIC PCS 7 setzt ein definiertes OPC-Variablen-Bit von logisch 0 auf 1. Nach einer definierten Zeit X muss das angebundene System das OPC-Variablen-Bit von logisch 1 nach 0 zurücksetzen.

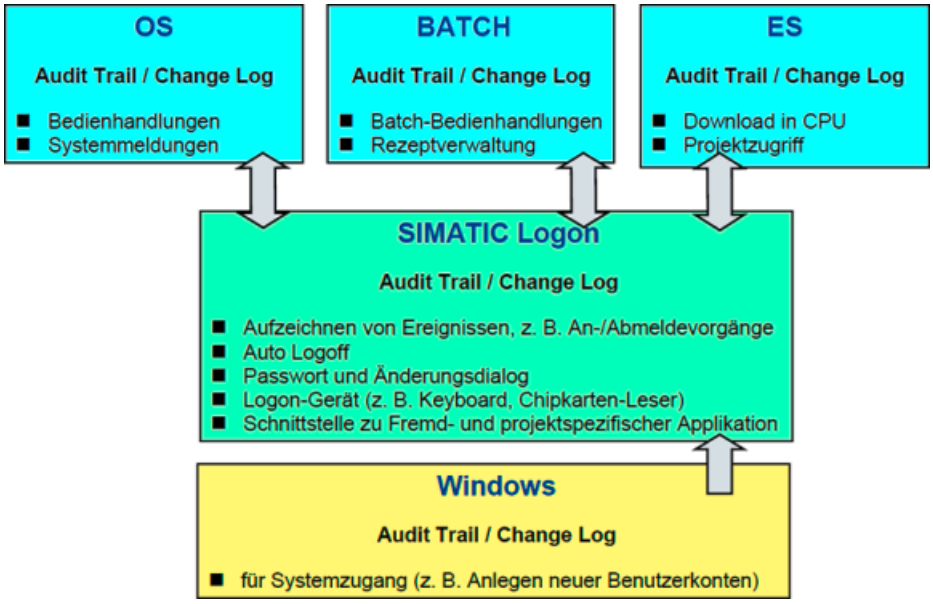
Dieser Vorgang wiederholt sich zyklisch. Wird ein Zustandswechsel in der spezifizierten Zeit vom angebundenen System nicht eingehalten, so wird eine Leittechnikmeldung am SIMATIC PCS 7 Prozessleitsystem erzeugt. Diese meldet dem Bediener, dass die Kommunikation zu dem angebundenen System gestört ist.

6.9 Audit Trail und Änderungskontrolle

Zur Nachverfolgbarkeit von Bedieneingriffen und kritischen Parameter- und Datenänderungen müssen diese unter Angabe des Bedieners gespeichert werden (Audit Trail). Anforderungen zu dieser Thematik definiert z. B. der 21 CFR Part 11 der US-amerikanischen Behörde FDA.

Änderungen z. B. an der Projektkonfiguration oder der Benutzerverwaltung unterliegen in einem regulierten Umfeld der Änderungskontrolle. Diese Änderungskontrolle wird durch die Aufzeichnung von Logdateien unterstützt.

In einem PCS 7-System wird das realisiert durch ein mehrschichtiges Konzept für die Themenkomplexe Audit Trail und Änderungskontrolle.



6.9.1 PCS 7 ES

Online-Änderungen auf der PCS 7 ES

Auf der Engineeringebene werden typischerweise Konfigurationsdaten bearbeitet, die nicht direkt den strengeren Anforderungen gemäß 21 CFR Part 11 unterliegen. Sehr wohl aber handelt es sich dabei meist um Systembestandteile, die validiert und kontrolliert werden müssen.

Mit der Möglichkeit der nachvollziehbaren Online-Parameteränderung könnte über die ES zwar auch direkt auf einige qualitätsrelevante Daten zugegriffen werden. Es ist allerdings sinnvoll und im regulierten Umfeld unbedingt zu empfehlen, solche Eingriffe ausschließlich auf der Bedienebene mit der entsprechenden Bedienberechtigung durchzuführen, wo die Änderungen im zentralen Audit Trail der OS protokolliert werden.

Hinweis

Parameteränderungen auf der OS-Oberfläche werden nicht automatisch in das Offline-Projekt übernommen. Hierzu muss die Funktion "Parameter zurücklesen" unter Auswahl der relevanten Parameter durchgeführt werden.

Während der Inbetriebnahmephase werden je nach Kunde kontrollierte Online-Parameteränderungen über die ES manchmal akzeptiert oder gar gewünscht. Im validierten Zustand einer Anlage sollten solche Parameteränderungen jedoch ausschließlich über die OS-Ebene oder per Änderungsantrag auf der ES erfolgen.

Siehe auch

- FAQ "Kennzeichnen von Parametern zum Rücklesen", Online-Support unter Beitrags-ID 23967880 (https://support.industry.siemens.com/cs/ww/de/view/23967880)

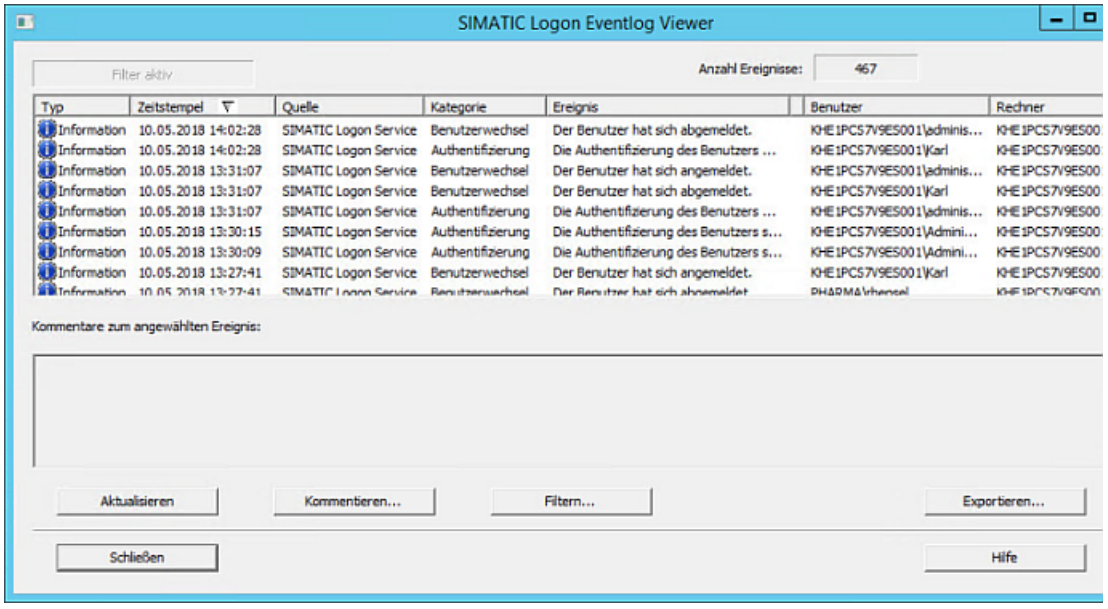
Änderungskontrolle der ES-/AS-Konfiguration

Zur Kontrolle der Offline-Konfiguration in der ES eignet sich neben einem definierten Änderungsprozess und einer entsprechenden Sicherungsstrategie der Projektdaten der Einsatz verschiedener Werkzeuge. Mit dem Version Cross Manager zum Beispiel können verschiedene Projektstände verglichen werden, siehe Kapitel "Versionsvergleich mit Version Cross Manager (VXM) (Seite 159)".

Des Weiteren kann der aktuelle Stand der Offline-/Online-Konfiguration durch das Aktivieren des "Testmodus" in der ES überprüft werden. Auch hier ist das Rücklesen von Parametern zu beachten, siehe vorheriger "Hinweis".

Projektzugriffe und Online-Änderungen auf der ES werden mit Hilfe des Änderungsprotokolls von SIMATIC Logon analog zu einem Audit Trail (wer hat wann was geändert) mitgeschrieben. Protokolliert werden dabei:

- Ereignisse des Zugriffsschutzes (Projekt öffnen, Zugriff auf das Projekt verweigert, Aktivieren / Deaktivieren des Zugriffsschutzes etc.)
- Ereignisse des Zielsystems (AS Konfiguration geladen, Software Applikation geladen, Onlinemodus aktiviert/deaktiviert)
- Ereignisse von Wertänderungen online (alter Wert, neuer Wert)
- Versionsänderungen (Archivierung von versionierten Projekten)



Änderungskontrolle bei AS-Download

Neben dem Zugriffsschutz auf die ES-Konfiguration über die Projekteinstellung "Zugriffsschutz aktivieren" kann das Laden in die CPU zusätzlich mit einem CPU-Passwort geschützt werden.

Ladevorgänge in die CPU werden allerdings ebenso wie online-Wertänderungen erst aufgezeichnet, wenn das Änderungslogfile aktiviert ist, siehe vorherigen Abschnitt "PCS 7 ES" zur ES-Änderungskontrolle.

Hinweis

Der Zeitpunkt der Aktivierung dieses Zugriffsschutzes sowie die Aktivierung des Änderungslogfile sollten frühzeitig mit dem Kunden definiert werden. Z. B. kann der Zugriffsschutz je nach Projektierungsumgebung schon in der Projektierungsphase sinnvoll sein, während das Änderungslogfile zu Beginn des FAT aktiviert wird.

Bei eingerichtetem Zugriffsschutz kann in Abstimmung mit dem Kunden oftmals auf das zusätzliche CPU-Passwort verzichtet werden.

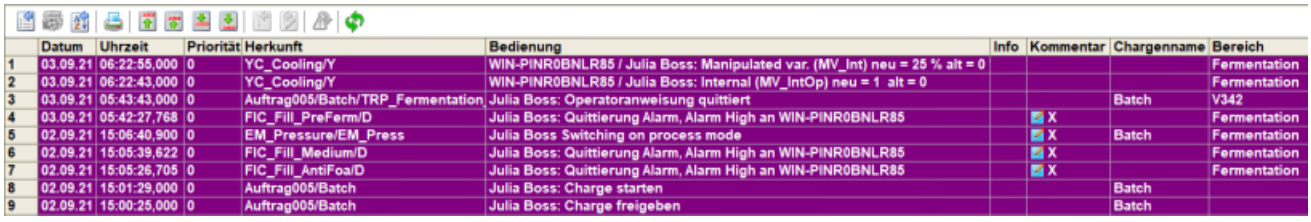
6.9.2 PCS 7 OS

Audit Trail in PCS 7 OS

SIMATIC PCS 7 zeichnet alle Bedienungen und Parameteränderungen im Prozessbetrieb mit der Meldeklasse "Bedienmeldungen" im Meldearchiv auf. Bei Parameteränderungen über Ein-/Ausgabefelder muss das Absetzen einer Meldung separat projektiert werden.

Quittierungen von Alarm-, Warn-, Systemmeldungen, etc. stehen in der "Chronikliste" des Prozessleitsystems zur Verfügung. Meldequittierungen können mit einem verpflichtenden Kommentar versehen werden.

Die nachfolgende Abbildung enthält einen Auszug der Bedienliste.



	Datum	Uhrzeit	Priorität	Herkunft	Bedienung	Info	Kommentar	Chargenname	Bereich
1	03.09.21	06:22:55,000	0	YC_Cooling/Y	WIN-PINR0BNLR85 / Julia Boss: Manipulated var. (MV_Int) neu = 25 % alt = 0				Fermentation
2	03.09.21	06:22:43,000	0	YC_Cooling/Y	WIN-PINR0BNLR85 / Julia Boss: Internal (MV_IntOp) neu = 1 alt = 0				Fermentation
3	03.09.21	05:43:43,000	0	Auftrag005/Batch/TRP_Fermentation	Julia Boss: Operatoranweisung quittiert			Batch	V342
4	03.09.21	05:42:27,768	0	FIC_Fill_PreFerm/D	Julia Boss: Quittierung Alarm, Alarm High an WIN-PINR0BNLR85		X		Fermentation
5	02.09.21	15:06:40,900	0	EM_Pressure/EM_Press	Julia Boss Switching on process mode		X	Batch	Fermentation
6	02.09.21	15:05:39,622	0	FIC_Fill_Medium/D	Julia Boss: Quittierung Alarm, Alarm High an WIN-PINR0BNLR85		X		Fermentation
7	02.09.21	15:05:26,705	0	FIC_Fill_AntiFoa/D	Julia Boss: Quittierung Alarm, Alarm High an WIN-PINR0BNLR85		X		Fermentation
8	02.09.21	15:01:29,000	0	Auftrag005/Batch	Julia Boss: Charge starten			Batch	
9	02.09.21	15:00:25,000	0	Auftrag005/Batch	Julia Boss: Charge freigeben			Batch	

Hinweis

Die Festplattenkapazität ist so zu wählen, dass das komplette Meldearchiv sicher bis zur nächsten Auslagerung zwischengespeichert werden kann.

Der eigentliche, gesetzlich geforderte Audit Trail beinhaltet nur die Änderungen an GMP relevanten Werten. Er ist somit eine Untermenge aus den aufgezeichneten Bedienhandlungen. Diese können zum Beispiel anhand einer separaten Meldepriorität herausgefiltert werden, siehe hierzu Kapitel "Prioritäten (Seite 113)". Alternativ können die relevanten Bedienmeldungen

auch mit Hilfe eines Add-ons realisiert werden, siehe Kapitel "OPD – Bedienerdialoge und elektronische Unterschriften (Seite 39)".

Hinweis

In einem verteilten System muss dem OS-Client ein Standard-Server zugewiesen werden, damit Meldungen und Alarme korrekt übermittelt werden. Dies ist im Handbuch "PCS 7 Kompendium Teil A" erläutert.

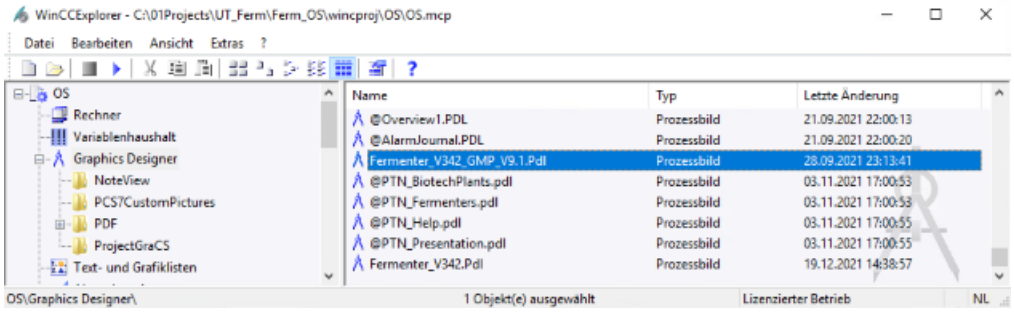
Siehe auch

- Handbuch "PCS 7 Kompendium Teil A", Kapitel 10.1.3 "Auswählen und Konfigurieren eines Standardservers", Online-Support unter Beitrags-ID 109809015 (https://support.industry.siemens.com/cs/ww/de/view/109809015)

Änderungskontrolle der OS-Konfiguration

Die OS-Konfiguration wie auch die Projektierung der OS-Elemente (Bilder, Skripte, etc.) wird mit dem Gesamtprojekt auf der ES versioniert (SIMATIC Version Trail) und archiviert. Die durchgeführten Änderungen können mit Hilfe von Screenshots dokumentiert und dem Änderungsantrag angehängt werden.

Geänderte Bedienbilder lassen sich über das Änderungsdatum im SIMATIC Manager in der Komponentensicht identifizieren. Zusätzlich können die Bedienbilder über den WinCC Explorer mit einem Passwort gegen Modifikation geschützt werden, siehe auch Kapitel "Schutz von Grafikbildern (Seite 164)".



Wer die Änderungen an Grafikbildern automatisiert im Detail nachverfolgen möchte, kann dieses mit Hilfe eines Add-ons realisieren, siehe Kapitel "versiondog – Versionierung und Konfigurationskontrolle (Seite 39)".

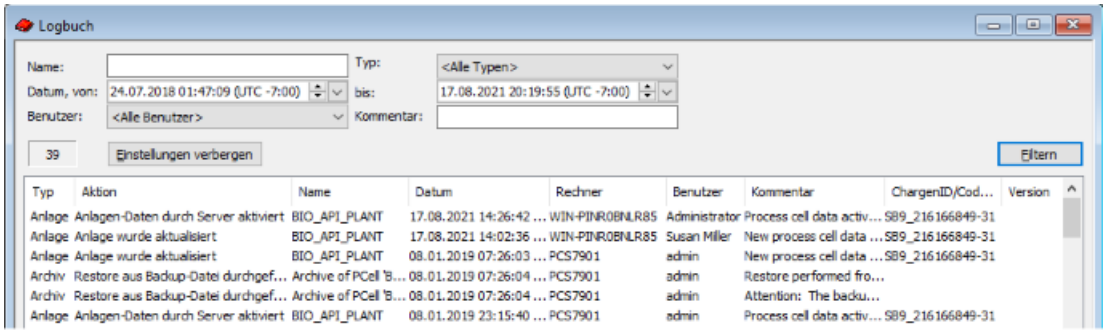
Änderungen an den einzelnen OS-Elementen müssen wie auch sonstige Änderungen ab ihrer ersten Freigabe mit dem geltenden Änderungsverfahren kontrolliert werden. Die eingesetzten Werkzeuge zur Dokumentation der Änderungen unterstützen hierbei lediglich.

6.9.3 SIMATIC BATCH

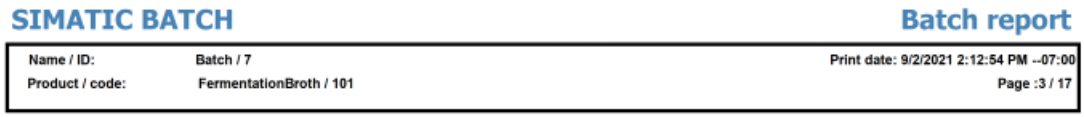
Audit Trail in SIMATIC BATCH

Bedienaktionen in SIMATIC BATCH werden im gleichen Meldearchiv wie OS-Bedienaktionen aufgezeichnet (s. o.).

Des Weiteren werden im SIMATIC BATCH Logbuch die Benutzeraktionen aufgezeichnet, die Sie im BatchCC durchführen.



In SIMATIC BATCH wird außerdem ein Chargenprotokoll erstellt, in dem die Informationen über die Aktionen des Bedieners (wer, wann, was) pro Charge protokolliert werden (Bearbeitungshistorie).



Editing history:

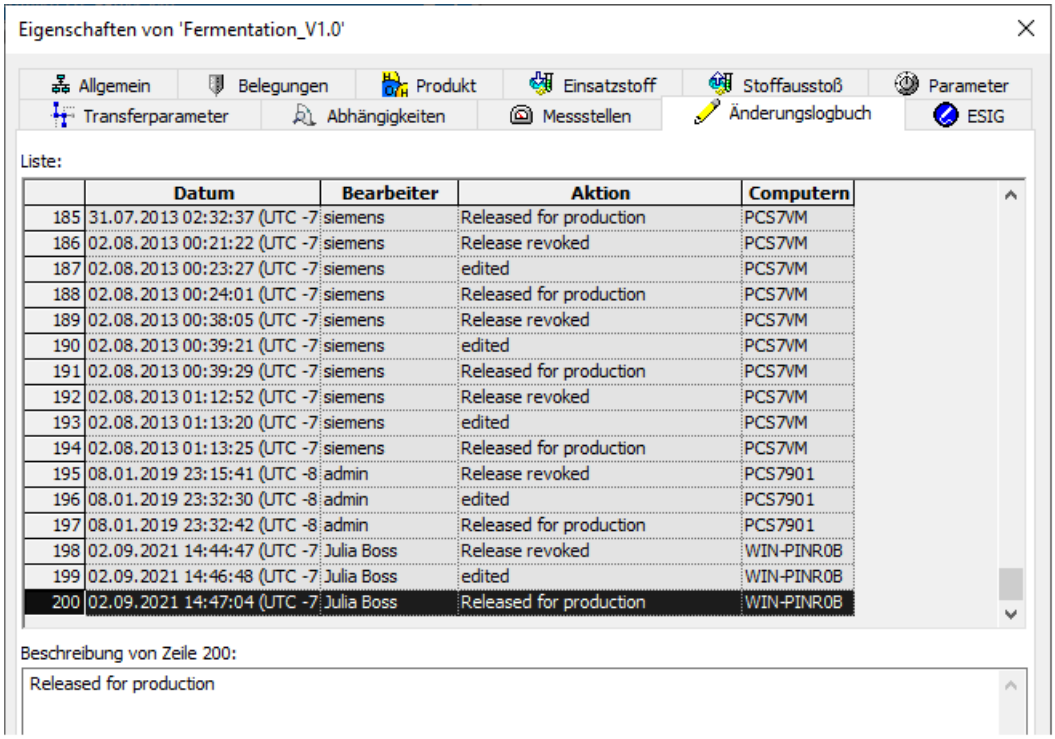
Date	Login	Processed by	Computer	Action
8/19/2021 7:41:38 AM -07:00	WIN-PINR0BNLR85\Julia Boss	Julia Boss	WIN-PINR0BNLR85	Batch created (ID: 7 / 1), Name: Batch
8/19/2021 7:42:05 AM -07:00	WIN-PINR0BNLR85\Julia Boss	Julia Boss	WIN-PINR0BNLR85	Scaling the control recipe
8/19/2021 7:42:05 AM -07:00	WIN-PINR0BNLR85\Julia Boss	Julia Boss	WIN-PINR0BNLR85	Batch release prepared
8/19/2021 7:42:05 AM -07:00	WIN-PINR0BNLR85\Julia Boss	Julia Boss	WIN-PINR0BNLR85	released
8/19/2021 7:42:14 AM -07:00	WIN-PINR0BNLR85\Julia Boss	Julia Boss	WIN-PINR0BNLR85	waiting
8/19/2021 7:42:15 AM -07:00	BCS	SIMATIC BATCH Control Server	WIN-PINR0BNLR85	Running
8/19/2021 8:20:21 AM -07:00	BCS	SIMATIC BATCH Control Server	WIN-PINR0BNLR85	Completed

Änderungskontrolle bei Rezepten und Batch-Objekten

Die Änderungskontrolle bei Rezepten wird unterstützt durch:

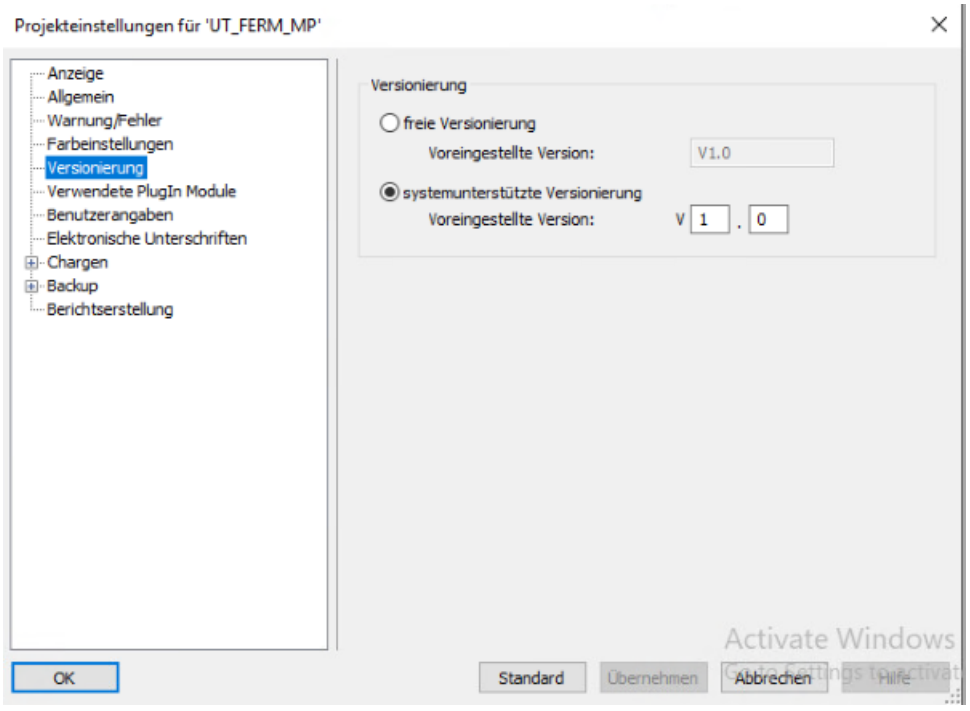
- Änderungslogbuch für wesentliche Bearbeitungsschritte
- Versionierung und Freigabe-Workflow einschließlich Unterschriften
- Berechtigungen und Projekteinstellungen
- Rezeptvergleicher

Im **Änderungslogbuch** werden Änderungen an Rezepten, Formula, Bibliotheken, Chargen und Stoffen dokumentiert. Es werden der Benutzer, die Uhrzeit und die Aktion eingetragen.



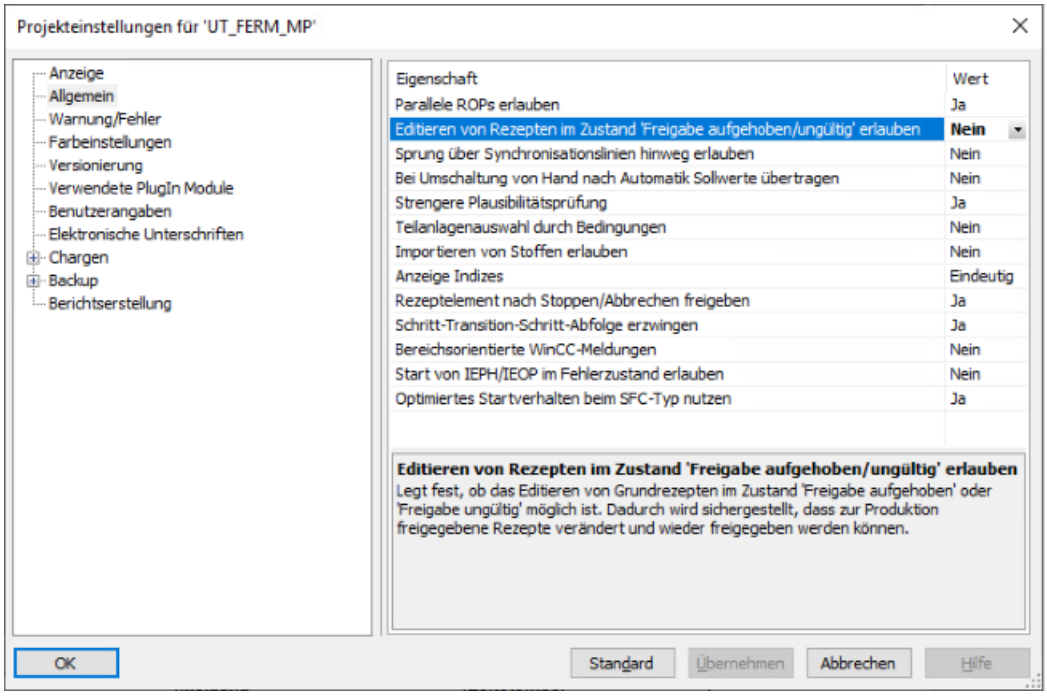
Für ein konsequentes **Versionsmanagement** sollte in den Projekteinstellungen

- die Option "systemunterstützte Versionierung" gewählt werden



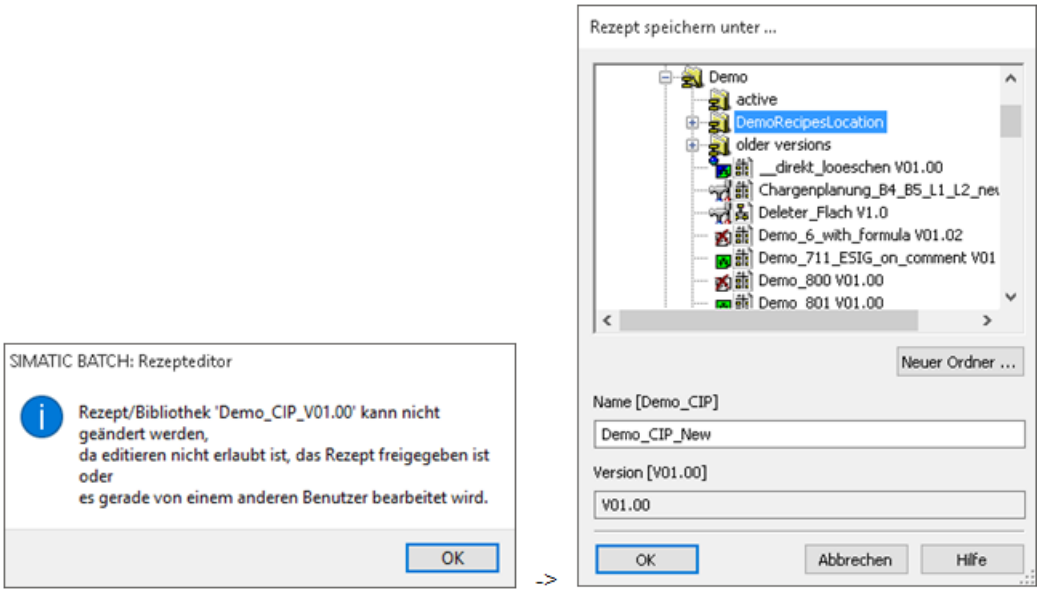
sowie

- die Eigenschaft "Editieren von Rezepten im Zustand 'Freigabe aufgehoben/ungültig' erlauben" **deaktiviert** sein (Default ist "Ja").



Sind diese Einstellungen gemacht, so kommt eine Meldung, wenn ein Rezept geändert werden soll.

Das Rezept kann dann nur nach "Speichern unter" bearbeitet werden:



Hinweis

Mit obiger Einstellung ist gewährleistet, dass ein einmal freigegebenes Rezept nicht nachträglich ohne Versions- oder Namensänderung bearbeitet werden kann.

Der **Vergleich von Rezeptobjekten** im BatchCC ermöglicht einen Vergleich verschiedener Versionen von Grundrezepten, Bibliotheken und Formulas.

Siehe auch

- FAQ "Speichern von Rezepten", Online-Support unter Beitrags-ID 23378328 (https://support.industry.siemens.com/cs/ww/de/view/23378328)
- Handbuch "SIMATIC BATCH", Kapitel 15.1.2.5 "Versionierung" sowie Kapitel 9.5.9 "Rezeptobjekte vergleichen", Online-Support unter Beitrags-ID 109794450 (https://support.industry.siemens.com/cs/ww/de/view/109794450)

6.10 Konfiguration für elektronische Unterschriften

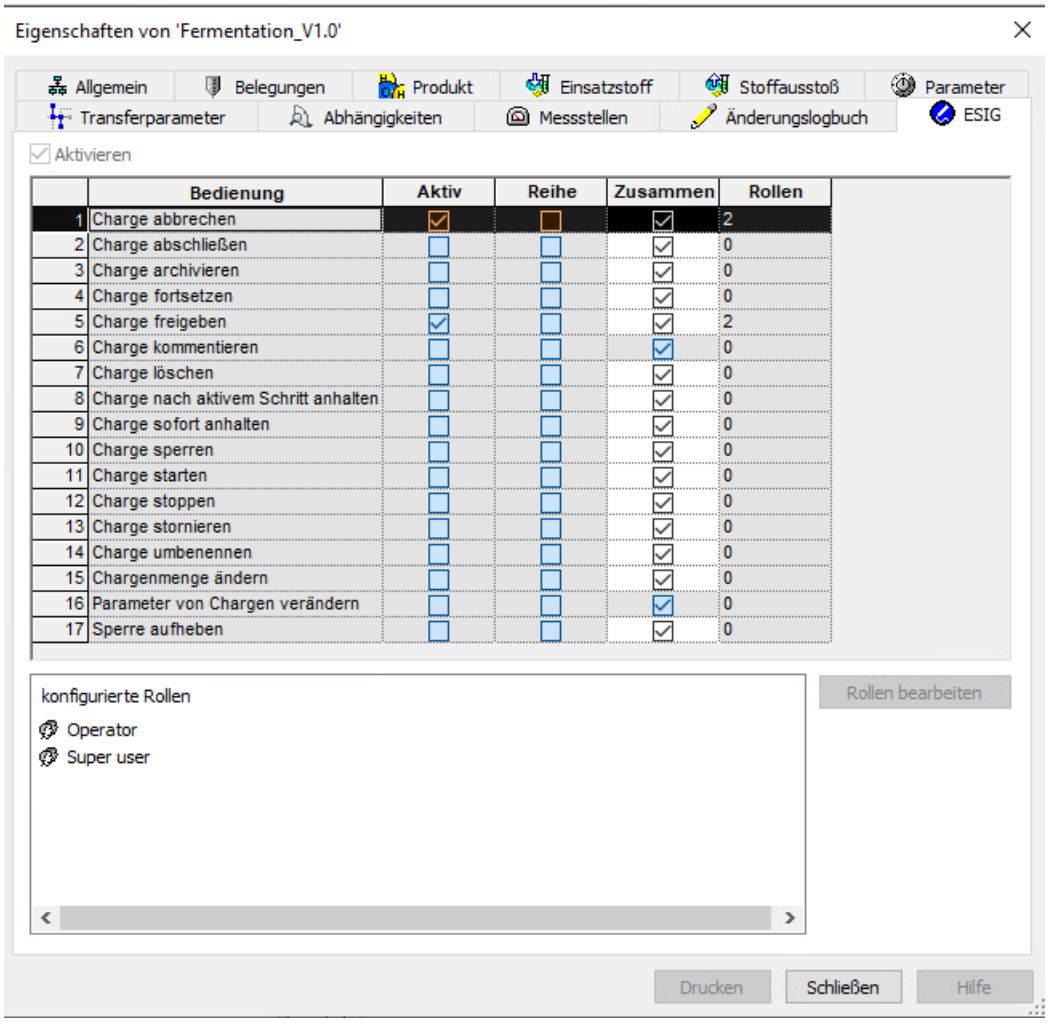
Um in einem Computer-System elektronische Unterschriften anstelle von handschriftlichen Unterschriften zu verwenden, müssen gesetzliche Vorschriften wie z. B. der 21 CFR Part 11 der US-amerikanischen Behörde FDA oder auch Annex 11 des EU GMP-Leitfadens erfüllt werden.

Für welche Aktionen Unterschriften erforderlich sind, wird durch weitere Gesetze und Vorschriften bzw. vom Prozesseigner definiert. Welche dieser Unterschriften auf elektronischem Wege geleistet werden, legt immer der Prozesseigner fest.

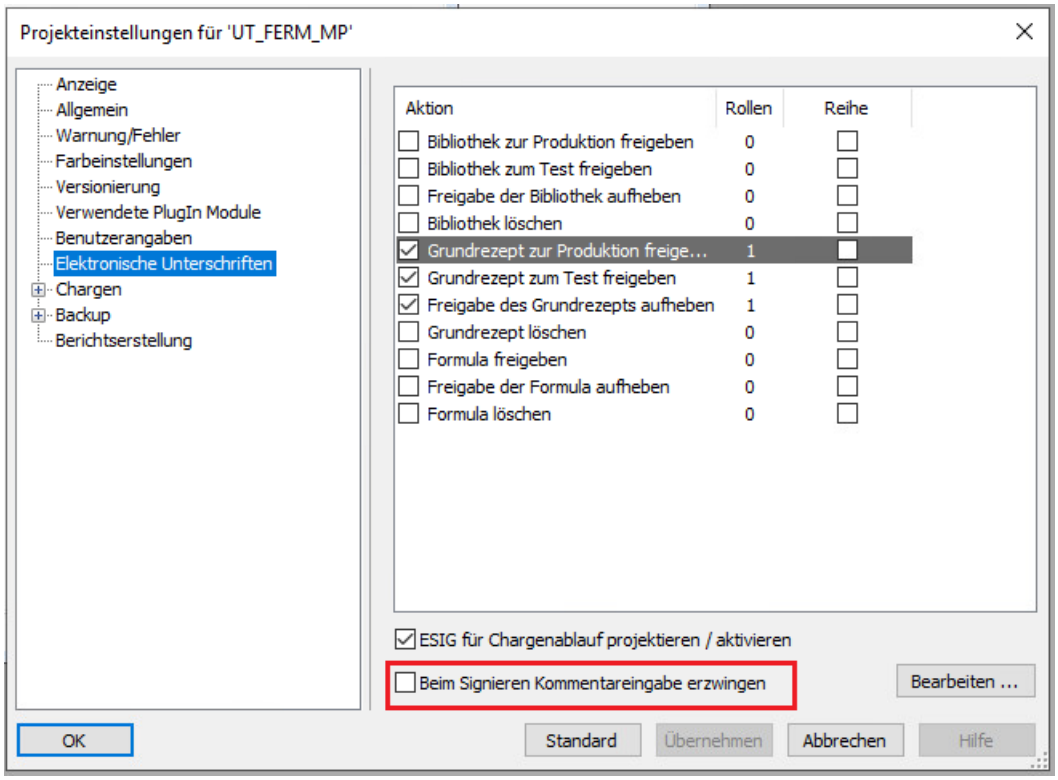
6.10.1 Elektronische Unterschrift in SIMATIC BATCH

Mit der Installation von SIMATIC Logon ist auch ein Paket für "Electronic Signature" verfügbar, dessen Standardfunktionalitäten in SIMATIC BATCH die Realisierung von elektronischen Unterschriften ermöglichen. Das nachfolgende Bild zeigt das Dialogfenster "Eigenschaften" für das Einrichten von elektronischen Unterschriften.

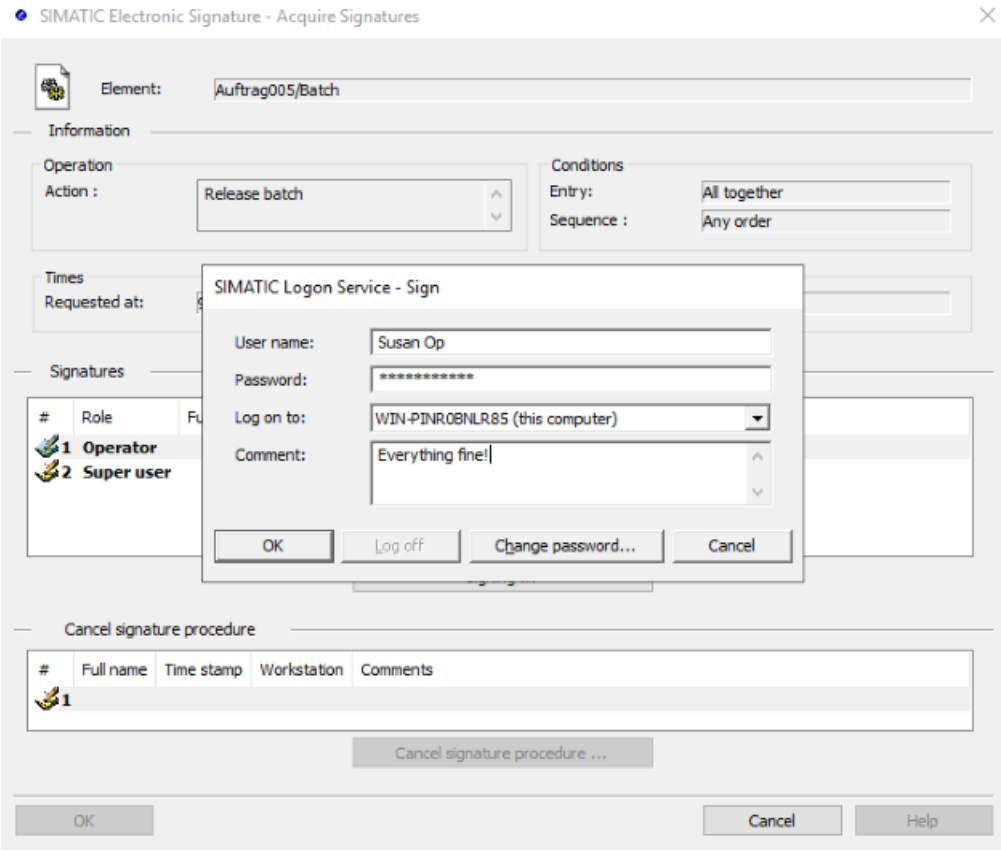
In dem Beispiel sind zwei elektronische Unterschriften nötig. Diese werden im SIMATIC BATCH Rezepteditor im Feld "konfigurierte Rollen" festgelegt.



Über die Projekteinstellungen kann auch eine elektronische Unterschrift z. B. für die Freigabe der Rezepte, der Parametersätze (Formula) und der Rezeptoperationen eingefordert werden.

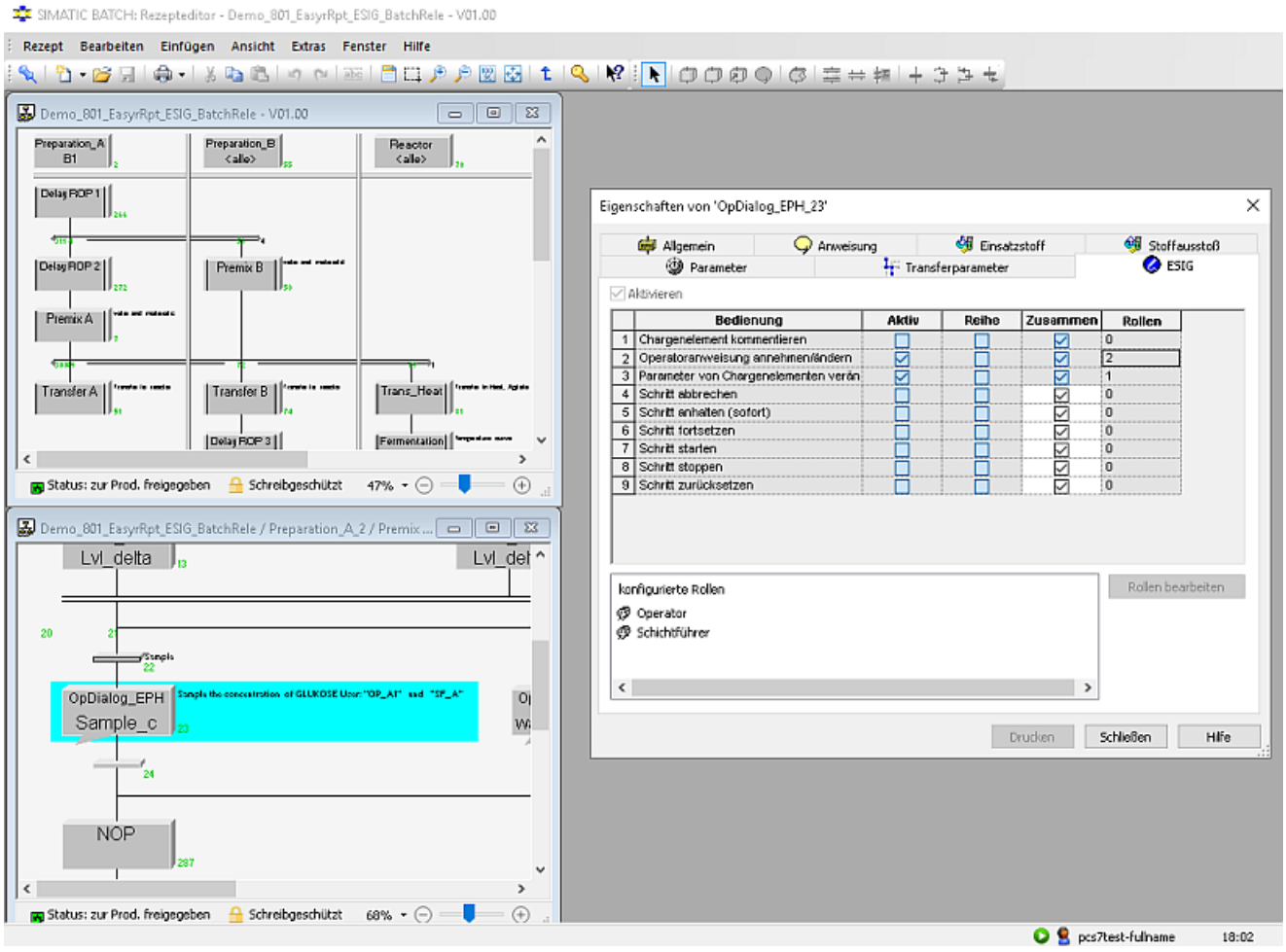


Zu jeder elektronischen Unterschrift kann auch ein Kommentar eingegeben werden; dieser Kommentar kann in oben abgebildeter Maske erzwungen werden.



Neben dieser projektweiten Regelung für elektronische Unterschriften gibt es auch die Möglichkeit für objektspezifische Unterschriftenregelungen. Die nachfolgende Abbildung zeigt hierzu ein Beispiel für die Unterschriftenregelung eines Rezepts.

Die Einstellungen werden in den Rezepteigenschaften durchgeführt.



Die geleisteten elektronischen Unterschriften werden im Änderungslogbuch von SIMATIC BATCH abgelegt und stehen im Report ebenfalls zur Verfügung.

Aktion:

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

Signaturen

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

Signaturen

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

6.10.2 Elektronische Unterschrift auf PCS 7 OS

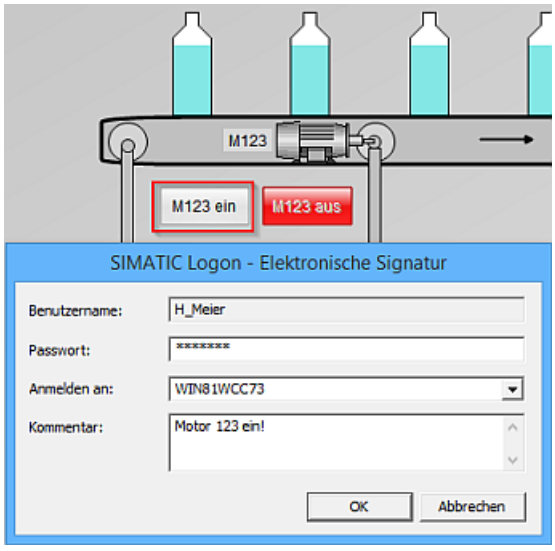
Es gibt verschiedene Wege, für die Bedienebene von PCS 7 OS eine elektronische Unterschrift zu projektieren. Diese sind im WinCC-Handbuch erläutert, siehe nachfolgender Link.

Siehe auch

- Handbuch "WinCC: Arbeiten mit WinCC", Kapitel 14.10 "Elektronische Signaturen", Online-Support unter Beitrags-ID 109792641 (https://support.industry.siemens.com/cs/ww/de/view/109792641)

Beispiel für eine einfache elektronische Unterschrift mit SIMATIC Logon Dialog

SIMATIC Logon bietet einen Dialog zur Angabe einer elektronischen Unterschrift. Dieser Dialog wird geöffnet, wenn die Funktion *Show Dialog* in einem VB- oder C-Skript aufgerufen wird.



Beispiel für eine mehrfache elektronische Unterschrift

Ein Anwendungsbeispiel zur Konfiguration mehrerer elektronischer Unterschriften für dieselbe Bedienaktion auf PCS 7 OS steht im Online Support zur Verfügung. Die Kompatibilität des Beispiels muss allerdings für aktuelle Systemversionen individuell geprüft werden.

Siehe auch

- Handbuch "SIMATIC Logon", Online-Support unter Beitrags-ID 109804727 (https://support.industry.siemens.com/cs/ww/de/view/109804727)
- Hinweise im "GMP Engineering Manual WinCC", Kapitel 6.4, Online-Support unter Beitrags-ID 109775436 (https://support.industry.siemens.com/cs/ww/de/view/109775436)
- Anwendungsbeispiel "Projektieren von Elektronischen Unterschriften", Online-Support unter Beitrags-ID 66926225 (https://support.industry.siemens.com/cs/ww/de/view/66926225)
- Kapitel "OPD – Bedienerdialoge und elektronische Unterschriften (Seite 39)"

6.10.3 Elektronische Unterschrift auf PCS 7 ES

Konfigurationsdaten im Engineering System unterliegen der Änderungskontrolle, und Änderungen müssen nachvollziehbar dokumentiert sein. Die Anforderungen des 21 CFR Part 11 an Audit Trail und elektronische Unterschriften kommen für Engineeringsysteme üblicherweise nicht zur Anwendung.

Sollten einzelne Daten bzw. deren Eingaben oder Änderungen qualitätsrelevant sein, so sollten sie ausschließlich über die Bedienebene (OS) eingegeben werden und falls erforderlich dort mit einer elektronischen Unterschrift versehen werden.

6.11 Elektronische Datenaufzeichnung und Archivierung

Besonders für Produktionsanlagen, die im GMP-Umfeld betrieben werden, ist es von großer Bedeutung, einen lückenlosen Qualitätsnachweis hinsichtlich der qualitätsrelevanten Produktionsdaten zu erbringen.

Zur elektronischen Aufzeichnung und Archivierung werden die folgenden Schritte durchgeführt:

- Ermitteln der zu archivierenden Daten, der Archivgrößen und der geeigneten Archivierungsstrategie, siehe Kapitel "Ermitteln der zu archivierenden Daten (Seite 133)"
- Einrichten von Prozesswertarchiven zur Onlinespeicherung der ausgewählten Prozesswerte, siehe Kapitel "Einrichten von Prozesswertarchiven (Seite 134)"
- Archivierung von Chargendaten, siehe Kapitel "Archivierung von Chargendaten (Seite 135)"
- Langzeitarchivierung, Definition der Parameter zum Auslagern auf den Archivserver (Zeitperiode bzw. belegter Speicherplatz), siehe Kapitel "Langzeitarchivierung auf einem zentralen Archivserver (Seite 136)"

6.11.1 Ermitteln der zu archivierenden Daten

Bei der Festlegung der Archivierungsstrategie und der Ermittlung des erforderlichen Speicherplatzbedarfs sind verschiedene Faktoren zu berücksichtigen, z. B.:

- Definition der zu archivierenden Daten unterschiedlicher Herkunft: Prozesswerte, Meldungen, Chargendaten und Batch-Reports, Audit Trail-Daten, Logfiles, etc.
- Definition der jeweiligen Aufzeichnungszyklen
- Festlegen der jeweiligen Aufbewahrungsdauer, online und offline
- Definition des Archivierungszyklus für externe Auslagerung

In PCS 7 werden diese in verschiedenen Archiven gespeichert:

- Prozesswertarchiv "Tag Logging fast" Archivierung von Prozesswerten <1 min
- Prozesswertarchiv "Tag Logging slow" Archivierung von Prozesswerten >1 min
- Meldearchiv "Alarm Logging"
- OS- und Batch-Reports

An weiteren Stellen des Systems werden Aktionen überwacht und in Log-Dateien oder Datenbanken mitgeschrieben:

- Änderungsprotokoll auf ES-Ebene für "Laden des Zielsystems" und Online-Parameteränderungen
- SIMATIC Logon Datenbank "EventLog.mdb"
- Ereignisanzeige im Windows-Computer Management (An- und Abmeldevorgänge, Kontenverwaltung, Filesystem-Rechteeinstellungen, etc. nach entsprechender Konfiguration)

Hinweis

Die Gesamtheit dieser erwähnten Dateien (und eventuell weiterer) muss beim Archivierungskonzept berücksichtigt werden.

6.11.2 Einrichten von Prozesswertarchiven

Die Projektierung eines Prozesswertarchivs gliedert sich in folgende Schritte:

- Erstellen des neuen Prozesswertarchivs und die Auswahl der Variablen, die im Umlaufarchiv gespeichert werden sollen.
- Konfigurieren des Prozesswertarchivs, indem z. B. die Berechtigungsstufen für den Zugriff oder der Speicherort festgelegt bzw. ausgewählt werden.

Bei dem Prozesswertarchiv werden messstellenbezogene Prozesswerte (Analog- und Binärwerte) in Form eines Umlaufarchivs in einer Datenbank festgehalten. Die Größe des Umlaufarchivs wird in der Spezifikation (URS, FS, DS) definiert.

Hinweis

Die Segmente im Umlaufarchiv müssen so angelegt werden, dass sie regelmäßig und rechtzeitig ausgelagert werden und somit keine Daten verloren gehen können.

Die im OS-Server gespeicherten Prozesswerte und Meldungen können auf ein externes Laufwerk exportiert oder zur Langzeitarchivierung an einen Archiv-Server übergeben werden.

Ebenso können angefallene Chargendaten und Reports vom BATCH-Server an den Archiv-Server weitergeleitet werden.

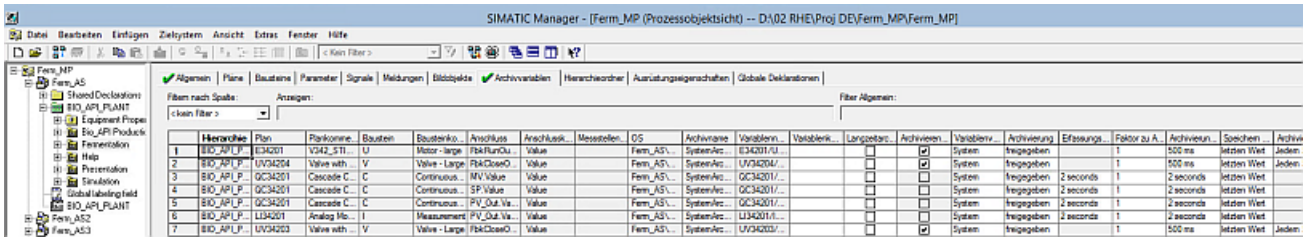
Hinweis

Wird die Verbindung zum Archiv-Server unterbrochen, so werden die Daten im Umlaufarchiv der jeweiligen Station gepuffert.

Die Größe der Datenbank wird durch die Anzahl der Prozesswertarchive und den darin befindlichen Prozessvariablen bestimmt. Die Größe jedes Prozesswertarchivs ist abhängig von der Messung mit dem kleinsten Erfassungszyklus. Die Zykluserfassung sollte innerhalb eines Prozesswertarchivs einheitlich erfolgen.

Es wird deswegen empfohlen, in einem Prozesswertarchiv immer Prozessvariablen mit gleichem Erfassungszyklus (z. B. 500 ms, 1 Sek., 10 Sek., 1 Min.) abzulegen. Dazu wird pro Erfassungszyklus jeweils ein Prozesswertarchiv konfiguriert.

Die Festlegung der Archivierungszyklen erfolgt in der Prozessobjektsicht.



In den Spezifikationsvorgaben (Messstellenliste, Entwurfsspezifikation, etc.) werden z. B. die nachfolgenden Parameter für Prozesswertarchive definiert.

- Klassifizierung in qualitäts- und nichtqualitätsrelevante Meldungen
- Erfassungsart zyklisch, zyklisch-kontinuierlich, bei Änderung, etc.
- Zykluszeit
- Art des Wertes (Momentanwert, Mittelwert, Maximalwert, etc.)

Siehe auch

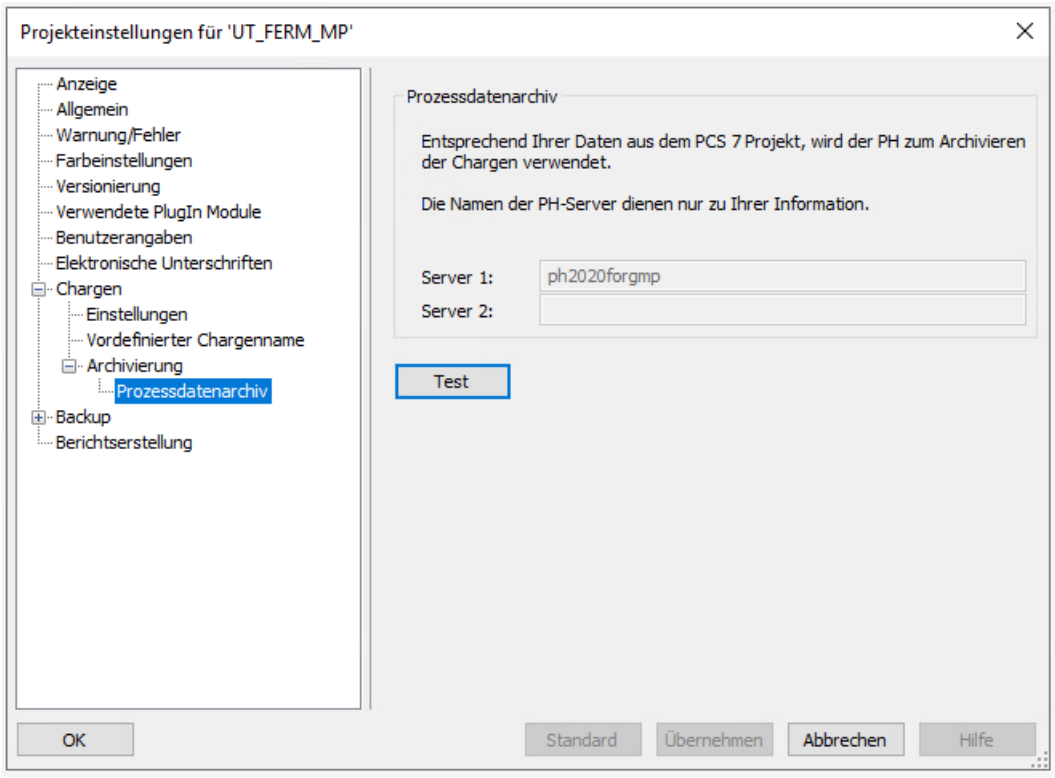
- Handbuch "WinCC: Arbeiten mit WinCC", Kapitel 6 "Archivieren von Prozesswerten", Online-Support unter Beitrags-ID 109792641 (https://support.industry.siemens.com/cs/ww/de/view/109792641)
- Handbuch "PCS 7 Kompendium Teil A", Kapitel 10.4.1 "Archivierung – Einleitung", Online-Support unter Beitrags-ID 109809015 (https://support.industry.siemens.com/cs/ww/de/view/109809015)

6.11.3 Archivierung von Chargendaten

Im BatchCC können Chargen in Langzeitarchive archiviert werden. Die Einstellungen für die Auswahl der gewünschten Archivierungstechnik und das Drucken von Chargenberichten erfolgt in den Projekteinstellungen.

Siehe auch

- Handbuch "SIMATIC BATCH", Kapitel 15.1.2.11, Online-Support unter Beitrags-ID 109794450 (https://support.industry.siemens.com/cs/ww/de/view/109794450)



In dem obigen Beispiel wurde ein SIMATIC Process Historian zur Archivierung konfiguriert. Falls stattdessen bei der Angabe des Archivierungspfades "Verzeichnis" gewählt wird, muss der Zugriff auf diesen Pfad über Windows Sicherheitsmechanismen geschützt werden und darf nur autorisierten Personen zugänglich sein.

6.11.4 Langzeitarchivierung auf einem zentralen Archivserver

Die Langzeitarchivierung erfolgt auf einem eigenständigen Server-PC, entweder in Form von einzelnen Segmenten oder auf dem SIMATIC Process Historian. Dies dient der Langzeitarchivierung von Meldungen, Prozesswerten und Reports.

Die aus den OS-Archiven ausgelagerten Prozesswerte und Meldungen sowie OS-Reports und Chargendaten von SIMATIC BATCH lassen sich am System visualisieren. Dabei verifiziert das System via Checksumme ("Signierung aktivieren"), dass die Daten nicht verfälscht wurden.

Die Daten eines Segments bleiben in der OS-Datenbank auch nach dem Archivieren zunächst erhalten. Das Segment Im Umlaufarchiv der OS wird erst gelöscht, wenn hierfür einer der Parameter "Zeitraum über alle Segmente" oder "Max. Größe über alle Segmente" überschritten wird.

Siehe auch

- Handbuch "PCS 7 Operator Station", Online-Support unter Beitrags-ID 109794374 (https://support.industry.siemens.com/cs/ww/de/view/109794374)
- Handbuch "PCS 7 Kompendium Teil A", Kapitel 10.4 "Archivierung", Online-Support unter Beitrags-ID 109809015 (https://support.industry.siemens.com/cs/ww/de/view/109809015)
- Linksammlung "Installation, Betrieb und Wartung PH/IS", Online-Support unter Beitrags-ID 66579062 (https://support.industry.siemens.com/cs/ww/de/view/66579062)

Netzwerksicherheit

Für Zugriffe aus einem anderen Netzwerksegment (Internet/Intranet) sind die Hinweise im Handbuch "Sicherheitskonzept PCS 7 und WinCC" zu beachten.

Einbindung in das Lifebeat Monitoring

Die Einbindung des Langzeitarchivservers erfolgt analog der Beschreibung in Kapitel "Überwachung von PCS 7 Komponenten (Seite 117)" zur Einbindung von SIMATIC PCS 7-Komponenten in das Lifebeat Monitoring. Es ist lediglich eine OPC-Verbindung einzurichten, über die das Lifebeat Monitoring erfolgt.

Audit Trail

Eine Änderung der archivierten Daten ist in aller Regel nicht erwünscht. Benutzer haben standardmäßig nur lesenden Zugriff auf archivierte Daten. Dementsprechend unterstützt der Langzeitarchivserver keinen Audit Trail im Sinne des 21 CFR Part 11. Sämtliche Ereignisse wie zum Beispiel Auslagerung von Daten auf externe Medien oder fehlgeschlagene Auslagerungen werden beim Process Historian dennoch in einem Logfile-Verzeichnis gespeichert.

6.12 Unterbrechungsfreie Stromversorgung (USV)

USV-Systeme sind notwendig, um bei Stromausfällen z. B. Prozess- und Audit Trail-Daten weiter aufzeichnen zu können. Die Auslegung der USV ist mit dem Systembetreiber abzustimmen und entsprechend zu spezifizieren. Hierbei sind folgende Punkte zu beachten:

- Energieverbrauch der zu versorgenden Systeme
- Leistungsfähigkeit der USV
- Gewünschte Dauer der USV-Pufferung

Der Energieverbrauch der zu puffernden Systeme bestimmt die Größe der USV. Ein weiteres Auswahlkriterium ist die Priorität der Systeme. Systeme mit hoher Priorität sind:

- Automatisierungssystem (AS)
- Archivierungsserver
- Operator-Station (OS) Server und Clients
- SIMATIC BATCH Server und Clients
- Netzwerkkomponenten

In jedem Fall ist es wichtig, die Systeme zur Protokollierung von Daten in die Pufferung mit einzubeziehen. In die Protokollierung sollte auch der Zeitpunkt des Spannungsausfalls mit aufgenommen werden.

Mit dem Einsatz von USV-Systemen ist auch die Installation und Konfiguration von Software verbunden. Zu beachten sind dabei

- Konfiguration der Alarmierung über den Stromausfall
- Festlegung des Zeitraumes bis zum Herunterfahren des PCs
- Festlegung des Zeitraumes der USV-Pufferung

Das Prozessleitsystem ist so zu programmieren, dass es bei einem Spannungsausfall nach einer einstellbaren Pufferzeit in einen sicheren Zustand gebracht wird.

6.12.1 Konfiguration einer USV

Die nachfolgende Tabelle beschreibt ein Beispiel für die Konfiguration einer unterbrechungsfreien Stromversorgung für eine Operator-Station eines Prozessleitsystems. Analog kann mit den Automatisierungsstationen verfahren werden.

Fall	Aktion	Reaktion
1	Spannungsausfall <10 Sekunden	Die Prozessleitsystemrechner werden durch die USV gepuffert. Ein Alarm unter Verwendung eines digitalen Eingangs im PLS dokumentiert den Spannungsausfall.
2	Spannungsausfall >20 Minuten. Nach 25 Minuten kehrt die Energie zurück	Die Prozessleitsystemrechner werden durch die USV gepuffert. Ein Alarm im PLS dokumentiert den Spannungsausfall und den Shutdown der Prozessleitsystemrechner nach 20 Minuten. Die USV beendet nach einer definierten Haltezeit die Spannungsversorgung, so dass ein eigenständiger Wiederanlauf der Prozessleitsystemrechner nach Spannungsrückkehr gewährleistet werden kann.
3	Spannungsausfall > 1 Stunde	Die Prozessleitsystemrechner werden durch die USV gepuffert. Ein Alarm im PLS dokumentiert den Spannungsausfall und den Shutdown der Prozessleitsystemrechner nach 20 Minuten. Die USV beendet nach einer definierten Haltezeit die Spannungsversorgung, so dass ein eigenständiger Wiederanlauf der Prozessleitsystemrechner nach Spannungsrückkehr gewährleistet werden kann.

6.12.2 USV Konfiguration über digitale Eingänge

Neben der Standardabsicherung durch USV-Geräte sollte die Möglichkeit der Überwachung der Versorgungsenergie genutzt werden. Hierbei wird über einen oder mehrere Digitaleingänge die Phase überwacht.

Der Ausfall der Versorgungsenergie kann über Alarmmeldungen registriert und während der Produktion in dem Chargenreport archiviert werden. Somit wird eine lückenlose Aufzeichnung von Anlagenproblemen gewährleistet.

USV-Pufferung Lastspannung

Die Automatisierungs-CPU wird durch das USV-Modul, z. B. 24V, während Spannungswischern als auch bei längeren Spannungsausfällen mit Energie versorgt. Durch das Phasenüberwachungsmodul wird die Zustandsänderung während eines Energieausfalls von einem digitalen Eingang überwacht, welcher als Failsafe-Eingangssignal ausgelegt sein sollte. Tritt ein Energieausfall auf, so kann zusätzlich eine Alarmierung erfolgen, wodurch der Bediener über den Energieausfall informiert wird (Alarmmeldung). Durch die Protokollierung im Meldesystem kann dieser Energieausfall zu späteren Recherchen genutzt werden.

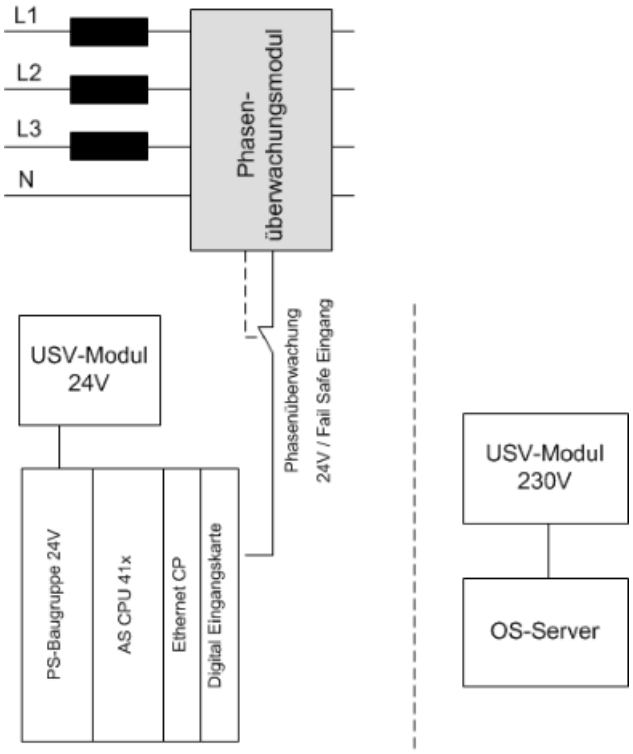
Zusätzlich können Sicherheitszustände durch Energieausfallkonzepte sofort oder nach Ablauf von Zeitgliedern realisiert werden (z. B. Equipment Phasen Halt, Herstellen des sicheren Anlagenzustands auch nach Rückkehr der Energie, etc.)

USV Pufferung Netzspannung

Parallel zur Phasenüberwachung wird der OS-Server über Standard-USV-Module z. B. 230V gepuffert. Hierdurch wird sichergestellt, dass der Server auch nach Energieausfall weiter in Betrieb ist.

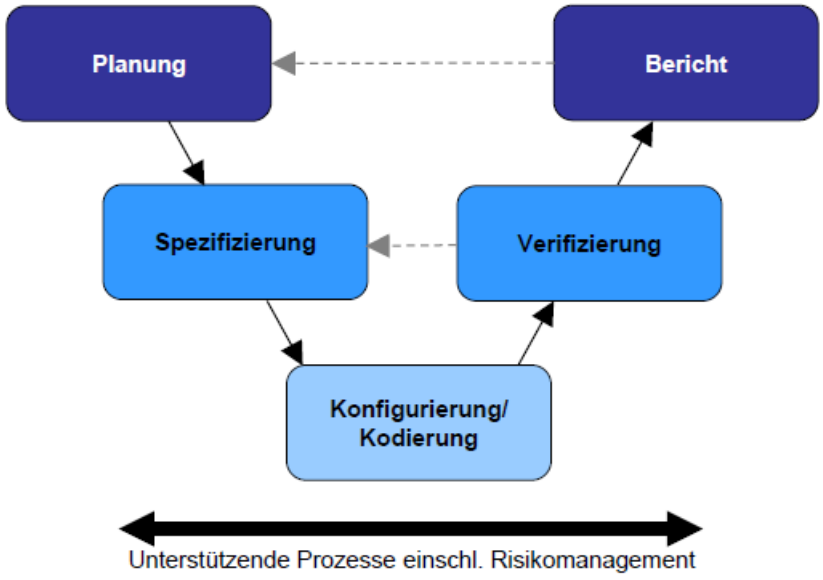
Der Bediener wird durch die USV-Pufferung auf den Energieausfall z. B. durch Alarmmeldungen hingewiesen. Sicherheitszustände können durch den Bediener oder durch automatisierte Konzepte eingeleitet werden.

Das sichere Herunterfahren des OS-Servers kann durch PCS 7 Alarmmeldungen angekündigt und ausgeführt werden, sofern die Energie nicht innerhalb einer spezifizierten Zeit zurückkommt. Durch diese Funktionalität wird die Verfügbarkeit des Systems nach Rückkehr der Energie erhöht.



Unterstützung bei der Verifizierung 7

Die folgende Grafik zeigt den allgemeinen Lebenszyklusansatz. Nach der Spezifizierung und der Systemerrichtung muss das System getestet werden. GAMP 5 nennt diese Phase die "Verifizierung". Ziel der Verifizierung ist der im Rahmen von Tests (z. B. FAT, SAT) dokumentierte Nachweis, dass das System die spezifizierten Anforderungen (URS, FS) erfüllt. Die Begriffe "Validierung" und "Qualifizierung" werden dadurch nicht ersetzt, sondern ergänzt. Was an Tests durch den Lieferanten abgedeckt und entsprechend dokumentiert wird, kann für die Validierungsaktivitäten des pharmazeutischen Unternehmens genutzt werden.



Quelle: Abbildung 3.3, GAMP 5 – Ein risikobasierter Ansatz für konforme GxP-computergestützte Systeme

Verschiedene Standardfunktionalitäten von SIMATIC PCS 7 können unterstützend bei dieser Verifizierung genutzt werden.

7.1 Testplanung

Mit der Definition eines Lebenszyklus für die Projektentwicklung werden verschiedene Testphasen bestimmt. Die grundlegenden Testaktivitäten (Verifizierung) werden dabei in einer sehr frühen Projektphase festgelegt und während der weiteren Spezifikationsphasen im Detail konkretisiert.

Zu Projektbeginn werden unter anderem festgelegt:

- Verantwortlichkeiten für Planung, Durchführung und Freigabe von Tests
- Testumfang in den einzelnen Testphasen
- Testumgebung (Testaufbau, Simulation)

Hinweis

Der Testaufwand sollte sowohl die Ergebnisse der Risikoanalyse als auch die Komplexität der zu testenden Komponente widerspiegeln.

Eine geeignete Testumgebung, ein geeigneter Testzeitpunkt sowie eine entsprechende Testdokumentation können dabei helfen, dass möglichst keine oder nur wenige Tests in nachfolgenden Testphasen wiederholt werden müssen.

Parallel zur Fertigstellung der Systemspezifikation (FS, DS) werden auch die einzelnen Tests detailliert geplant. Hierbei werden definiert:

- Testprozeduren für die einzelnen Tests
- Testmethoden, z. B. strukturell (Code-Review) bzw. funktional (Black-Box-Test)

7.2 Verifizierung von Hardware

Es wird geprüft, ob die installierten Komponenten und der gesamte Systemaufbau den Vorgaben aus der Designspezifikation entsprechen. Hierzu gehören Angaben wie Komponentenbezeichnung, Firmware- / Ausgabestand, Einbauort, eingesetzte Server und Clients, Schnittstellen, etc.

Hinweis

Ausdrucke und Screenshots können jeweils als Nachweis genutzt werden. Die Verwendung der SIMATIC Management Console ist hierbei sehr hilfreich.

Eine visuelle Überprüfung der Hardware kann zusätzlich erfolgen.

Verifizierung von Feldgeräten

Feldgeräte werden z. B. mit folgenden Angaben spezifiziert und geprüft:

- Hersteller und Typ-Bezeichnung
- Bestellnummer
- Funktion / Bestimmungsort
- Messstellenbezeichnung / Messbereich / Einheit
- Anschlussart
- Adressnummer

Hinweis

Das Asset Management von SIMATIC PCS 7 kann unterstützend genutzt werden.

Verifizierung der Automatisierungshardware

Automatisierungsstationen werden z. B. mit folgenden Angaben spezifiziert und geprüft:

- Hersteller und Typ-Bezeichnung
- Bestellnummer
- Anzahl an Baugruppenträgern
- Überprüfung der eingesetzten Hardwarekomponenten (CPU, CP, etc.)
- Anzahl an dezentralen Peripheriestationen
- Schnittstellen zu Fremdsystemen
- Adressnummer

Hinweis

Die Dokumentation wird durch Ausdrucke der HW Konfig bzw. auch mit der SIMATIC Management Console unterstützt.

Auch die Schaltschrankdokumentation muss damit übereinstimmen.

Verifizierung der Netzwerkstruktur

Bei der Verifizierung der Netzwerkstruktur werden z. B. die folgenden Angaben spezifiziert und geprüft:

- Namen von Station, PC, AS, Clients, etc.
- Kommunikationsbaugruppe, Art der Verbindung und Kommunikationspartner (Ethernet, PROFIBUS, Profinet, Seriell, etc.)
- MAC-Adresse (bei der Nutzung des ISO-Protokolls am Anlagenbus)
- TCP/IP-Adresse und Subnetmask (bei der Nutzung von Clients)
- PROFIBUS-Adressen
- Profinet Gerätenamen

Hinweis

Die SIMATIC NetPro Konfiguration kann ausgedruckt werden.

Verifizierung der eingesetzten PC-Hardware

Bei der Verifizierung der PC-Hardware werden z. B. die folgenden Angaben spezifiziert und geprüft:

- Hersteller / Typ-Bezeichnung / wesentliche Komponenten
- Zusätzlich installierte Hardwarekomponenten (zusätzliche Netzwerkkarte, Drucker, etc.)
- Überprüfung der konfigurierten Netzwerk-Adressen, Bildschirmauflösung, etc.

Hinweis

Hilfsprogramme können detaillierte Informationen über die Konfiguration des Rechners auslesen und dies als dokumentierten Nachweis ausdrucken. Mit Hilfe der SIMATIC Management Console kann dies von zentraler Stelle über die gesamte Anlage hinweg geschehen.

7.3 Verifizierung von Software

7.3.1 Software-Kategorisierung gemäß GAMP 5-Leitfaden

Nach dem GAMP 5-Leitfaden werden Hardware- und Softwarekomponenten eines Systems in Kategorien eingeteilt. Diese Zuordnung kann als ein Kriterium bei der Festlegung der geeigneten Lebenszyklusstrategie dienen. Die Grenzen zwischen den Kategorien 3 bis 5 sind hierbei als fließend und nicht starr zu verstehen.

In Bezug auf ein PCS 7-System bedeutet dies, dass die einzelnen Komponenten entsprechend ihrer Software-Kategorie bei Spezifikation und Test unterschiedlichen Aufwand verursachen. Allerdings können auch innerhalb jeder Kategorie Komponenten unterschiedlich komplex und/oder kritisch sein und müssen entsprechend behandelt werden.

Analog zu den weiter unten zitierten Literaturverweisen dienen die nachfolgenden Tabellen als Anleitung und Beispiele. Sie enthalten keine vollständige Auflistung.

Kategorie 1: Infrastruktur-Software **Testumfang:** **- Prüfen und dokumentieren der Versionsnummer** **- Prüfen und dokumentieren der korrekten Installation** **- Im Falle von Konfiguration auch entsprechende Prüfung**	
Betriebssystem	z. B. Microsoft Windows
Server, Clients	physisch oder virtuell, Kombination aus HW Kat. 1 und SW Kat. 1
Datenbank Manager	z. B. Backup-System
Programmiersprachen	z. B. CFC/SFC-Editor, Rezepteditor, Grafikeditor
DCS Entwicklungstools	z. B. Import-Export-Assistent
Konfigurationsmanagement-Tools	z. B. Version Trail, Version Cross Manager
Infrastruktur-Firmware	kann unterschiedlich komplex und konfigurierbar sein
Hypervisor	virtuelle Plattform, vergleichbar mit Betriebssystem
Netzwerk-Monitoring	
Sicherheits-Software	z. B. Antivirus-Programm, Kennwortverwaltung

Kategorie 3: Nicht-konfigurierte Produkte bzw. Standard-Funktionalität **Testumfang:** **- Prüfen und dokumentieren der Versionsnummer** **- Prüfen und dokumentieren der korrekten Installation** **- Funktionsprüfung**	
DCS Standard-Funktionalität	z. B. Alarmhistorie, SIMATIC Logon
Standardbausteine, Bibliotheken	z. B. APL Bibliothek einschließlich Standard-Faceplates
Parameter-Einstellungen	Netzwerk-Einstellungen, Backup-Pfad, Zugriffsrechte
PLC mit Firmware	z. B. S7-300/400
Firmware basierte Applikation	Gerät mit Standard-Funktionalität
Parameter für Geräte	z. B. I/O Range, PID Parameter, Alarmgrenzen
Smart Transmitter	
Electronic Chart Recorder	

Kategorie 4: Konfigurierte Produkte **Testumfang:** **- Prüfen und dokumentieren der Versionsnummer** **- Prüfen und dokumentieren der korrekten Installation und Konfiguration** **- Risikobasierter Test zum Nachweis der korrekten Arbeitsweise im Rahmen der Geschäftsprozesse**	
Funktionspläne (FBD)	CFC (Typ und Instanzen), FUP (Funktionsplan), KOP (Kontaktplan) basierend auf Bibliotheken
SFC Applikation	Konfiguration vergleichbar zu Verschaltungen in CFC, aber Testaufwand abhängig von Komplexität und Kritikalität
DCS Grafikbilder (mimic displays)	Konfiguration vorhandener Bausteinsymbole und Bildbausteine (Faceplates)
Rezeptbearbeitung	
Chargenplanung	
Route Control Engineering	Konfigurieren und Testen der Wege
OPC-Server/-Client, Open PCS 7	Einrichtung der Schnittstelle und enthaltene Daten prüfen
einfache Skripte	z. B. einzelne Zeile ST-Code zur Definition einer Aktion für einen Bedienbutton

Kategorie 5: Kundenspezifische Applikationen **Testumfang:** **- Prüfen und dokumentieren der Versionsnummer** **- Planen und freigeben des Entwurfs** **- Prüfen und dokumentieren der korrekten Installation, der Funktionen und des Quellcodes** **- Risikobasierter Test zum Nachweis der korrekten Arbeitsweise im Rahmen der Geschäftsprozesse**	
Bausteine erstellen	AWL (Anweisungsliste), SCL (Structured Control Language)
DCS/SCADA Skripte	z. B. VB und C++ -Skripte
kundenspezifische Applikationen	z. B. Tabellenkalkulationen (Makro), Berichtvorlagen mit Microsoft Reporting Services
BATCH API Schnittstelle	Applikative Schnittstelle zu SIMATIC BATCH

Während ein kundenspezifisch konfiguriertes PCS 7-System als Ganzes zwar einer Kategorie 4 oder manchmal sogar 5 zugeordnet werden müsste, kann man die einzelnen zu installierenden Standard-Bestandteile (ohne Konfiguration) jedoch analog einer Kategorie 3 bzw. 1 behandeln.

Der Konfigurationsanteil auf Basis installierter Produkte, Bibliotheken, Funktionsbausteine, etc. entspricht dann der Kategorie 4.

Wird darüber hinaus "freier Code" programmiert, entspricht dies einer Kategorie 5.

Siehe auch

- GAMP 5-Leitfaden, Anhang M4 "Hardware- und Software-Kategorien"
- GAMP Good Practice Guide “GxP Process Control Systems”, Anhang E1
- GAMP Good Practice Guide “IT Infrastructure Control and Compliance”, Kapitel 2.1

Vorgehensweise für Funktionen der Kategorie 5

Es ist ein entsprechend höherer Aufwand für Spezifikation und Test vorzusehen:

1. Erstellen einer Funktionsbeschreibung für die Software
2. Festlegen der verwendeten Funktionsbausteine
3. Festlegen der verwendeten Ein- und Ausgänge
4. Festlegen der Bedien- & Beobachtbarkeit
5. Softwareerstellung gemäß Spezifikation und Programmierrichtlinien
6. Strukturelles Testen auf Einhaltung von Programmierrichtlinien
7. Funktionelles Testen auf Übereinstimmung mit Funktionsbeschreibung
8. Freigabe vor Einsatz bzw. Vervielfältigung

7.3.2 Verifizierung der installierten Software

Bei der Verifizierung der eingesetzten "Standard"-Softwareprodukte wird geprüft, ob die installierte Software den Vorgaben aus der Spezifikation entspricht. Dies sind in der Regel Produkte, die nicht speziell für einen Kunden entwickelt werden und die am Markt frei verkäuflich sind, also z. B.:

- Betriebssystem
- SIMATIC PCS 7 Softwarepakete (OS-Server/-Client, Engineering System, etc.)
- SIMATIC Optionen wie SIMATIC BATCH, SIMATIC Route Control, etc.
- Standardbibliotheken
- Fremd-Software wie Acrobat Reader, Microsoft Office (Word, Excel), etc.

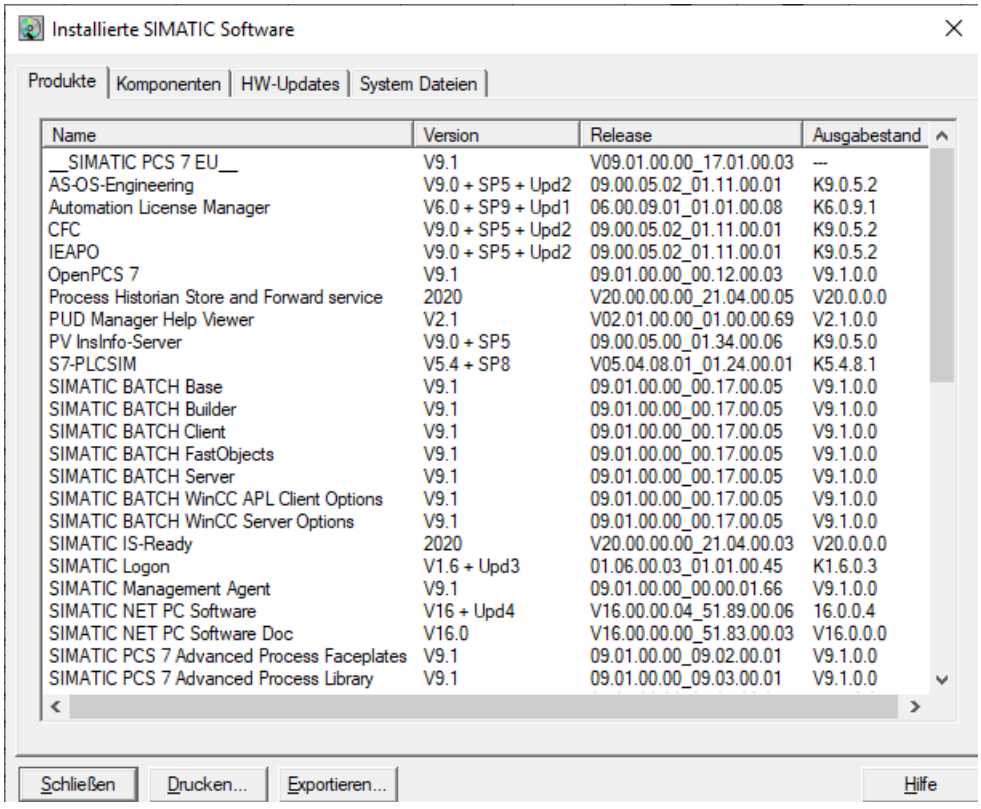
Betriebssystem und weitere Software-Pakete

Die Überprüfung von installierter Software kann durch Betriebssystem-Funktionen erfolgen. Die Informationen findet man in der Systemsteuerung > Software. Hier werden alle installierten Softwarekomponenten angezeigt.

Installierte SIMATIC Software

Die Überprüfung von installierter SIMATIC Software kann durch das Software-Tool "Installed SIMATIC Software" realisiert werden. Das Tool informiert über die aktuell installierte SIMATIC Software auf dem Rechner; die Auflistung kann auch gedruckt oder exportiert werden.

Unter Verwendung der SIMATIC Management Console kann die installierte Software aller verwalteten Rechner zentral erfasst werden. Der Aufwand zur Erstellung der Dokumentation kann hierdurch signifikant reduziert werden.



SIMATIC Software-Lizenzen

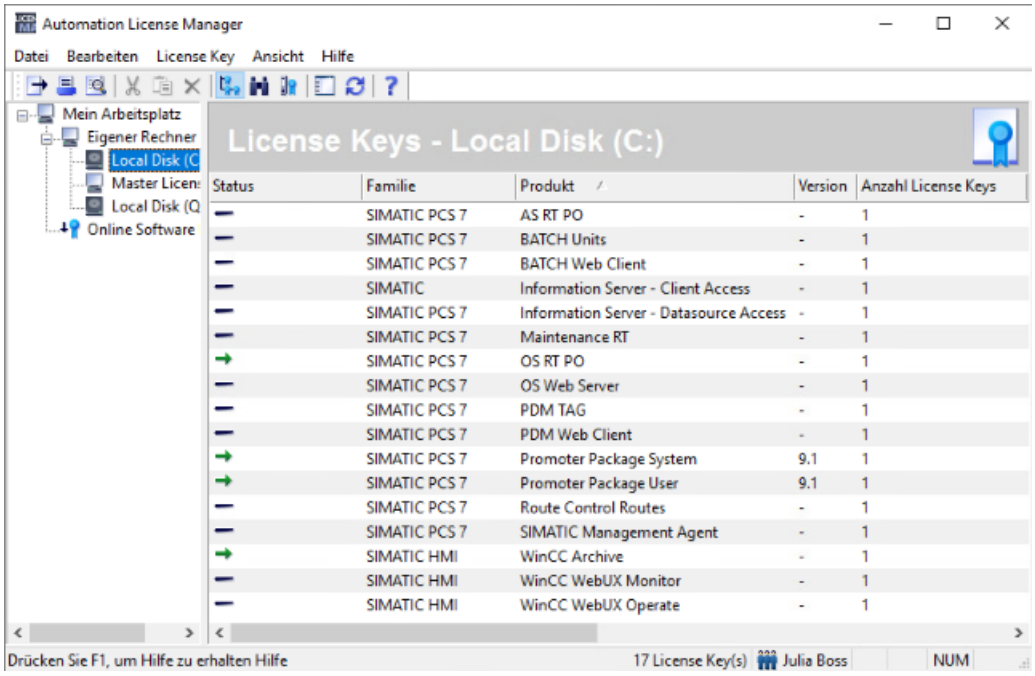
Das SIMATIC Tool "Automation License Manager" gibt Auskunft über aktuell installierte Lizenzen auf dem PC. Hierzu ist im Automation License Manager die Partition des PCs anzuwählen, auf der die Lizenzen installiert sind. In der rechten Seite des Fensters werden dann die verfügbaren Lizenzen des Systems angezeigt.

Über die SMMC ist auch hier eine zentraler Zugriff auf die Lizenzen der verwalteten Rechner möglich.

Das Handbuch "PCS 7 Kompendium Teil A" beinhaltet weitere Hinweise zur Dokumentation der Systeminstallation.

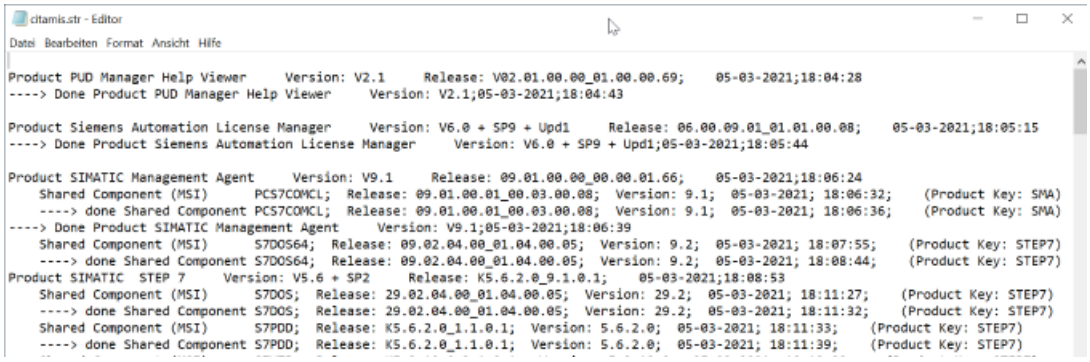
Siehe auch

- Handbuch "PCS 7 Kompendium Teil A", Kapitel 4.4.2 "Dokumentation und Inventarisierung", Online-Support unter
  Beitrags-ID 109809015 (https://support.industry.siemens.com/cs/ww/de/view/109809015)



SIMATIC PCS 7 Installationsprotokoll

Bei der Installation von SIMATIC PCS 7 wird der Istzustand der installierten Systemprogramme in der Datei "citamis.str" gespeichert. Nachinstallationen werden ebenfalls dokumentiert. Die Datei befindet sich im Verzeichnis "C:\ProgramData\Siemens\Automation\Logfiles\Setup".



7.3.3 Verifizierung der Applikationssoftware

Bei der Verifizierung der Applikationssoftware wird die erstellte Software gegen die Vorgaben aus der Spezifikation (FS/DS) geprüft. Es müssen Testbeschreibungen (z. B. für FAT/SAT) mit dem Betreiber abgestimmt und generiert werden. Diese müssen die Komplexität der Software und die Design-Vorgaben berücksichtigen.

Folgende Inhalte sind typische Bestandteile solcher Tests und können als Referenz für die Qualifizierung genutzt werden:

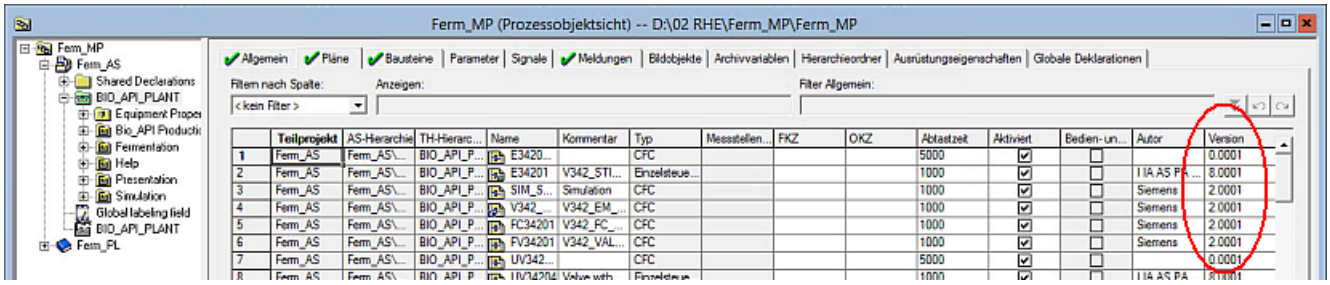
- Überprüfung des Namens der Applikationssoftware
- Überprüfung der Technologischen Hierarchie (Anlage, Teilanlage, technische Einrichtung, Einzelsteuerelement, etc.)
- Software-Modultest (Typical Test)
- Überprüfung der Kommunikation zu anderen Teilnehmern (Fremdsteuerungen, MES-Systeme, etc.)
- Überprüfung aller Ein- und Ausgänge
- Überprüfung aller Control Module (Einzelsteuerebene)
- Überprüfung aller Equipment Phasen und Equipment Operationen (Technische Funktionen)
- Überprüfung der Zusammenhänge von Betriebsarten (HAND/AUTOMATIK- Umschaltungen, Verriegelungen, Start, Läuft, Angehalten, Abbrechend, Beendet etc.)
- Überprüfung von Messstellenbezeichnungen
- Überprüfung der Visualisierungsstruktur (R&I Darstellung)
- Überprüfung der Bedienphilosophie (Zugangskontrolle, Gruppenrechte, Benutzerrechte)
- Überprüfung der Archivierungskonzepte (Umlaufarchive, Langzeitarchive)
- Überprüfung des Meldekonzepts
- Überprüfung der Trends, Kurven
- Überprüfung der Uhrzeitsynchronisation
- Überprüfung von Redundanzumschaltungen

Hinweis

Werden neben den PCS 7 Standard-Bibliotheken zusätzliche Bausteine zur Projektierung spezieller Prozesse oder Funktionen benötigt, so sind wenn möglich Bausteinbibliotheken (FB, FC, DB) des PCS 7 Add-on-Katalogs zu verwenden.

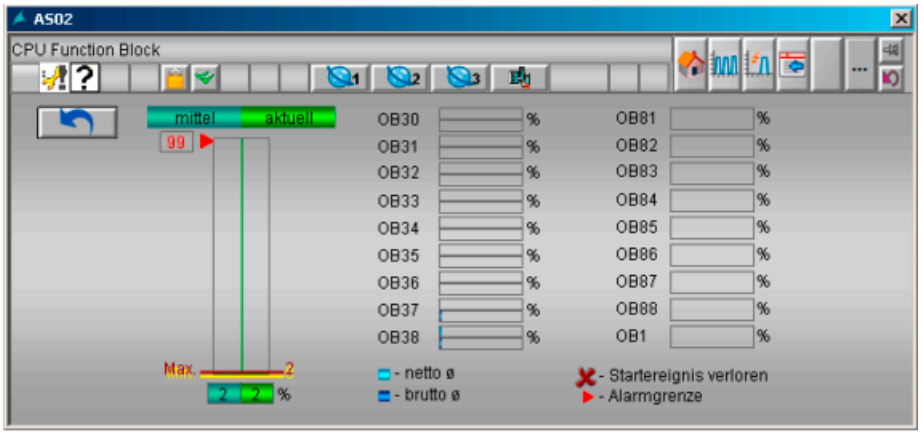
Bei selbst erstellten Bausteinen muss ein deutlich höherer Aufwand für Spezifikation, Erstellung und Verifizierung berücksichtigt werden.

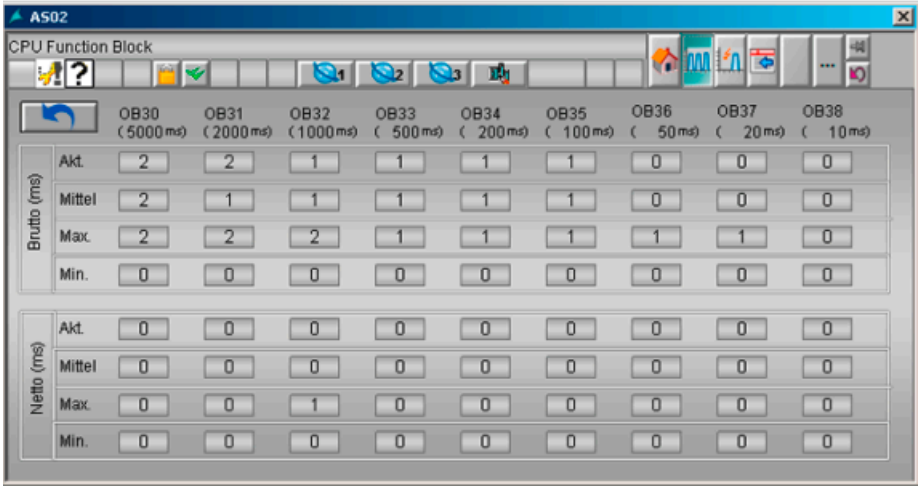
Zur Prüfung von Versionsständen bei der Verifizierung kann die Prozessobjektsicht genutzt werden. Dort ist auch eine Anpassung der Software-Versionen möglich (siehe Abbildung).



CPU-Lastanalyse

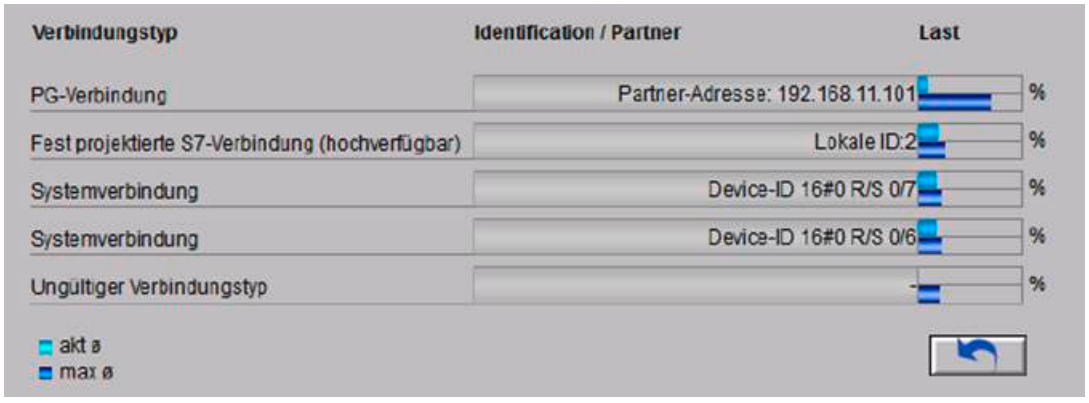
Mit Hilfe des Asset Managements kann die Auslastung von CPUs analysiert und dokumentiert werden.





CPU-Verbindungsauslastung

Mit Hilfe des Asset Managements kann ebenfalls die Verbindungsauslastung von CPUs analysiert und dokumentiert werden. Dies kann insbesondere dann relevant werden, wenn mit dem Kunden z. B. bestimmte Reserven vereinbart wurden.



DOCPRO

Mit DOCPRO steht ein Werkzeug zum Erstellen und Verwalten von Anlagendokumentation zur Verfügung. SIMATIC PCS 7 V9.1 unterstützt DOCPRO allerdings nicht mehr. Die Kompatibilität mit früheren Versionen von DOCPRO muss projektspezifisch geprüft werden.

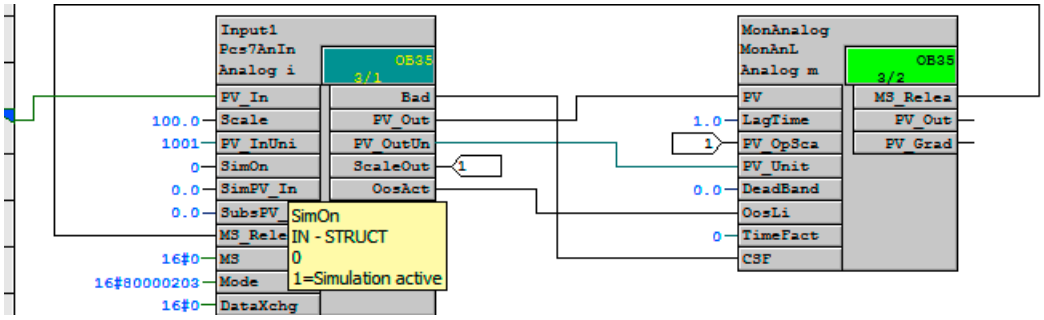
7.3.4 Simulation für Testbetrieb

SIMATIC PCS 7 bietet die Möglichkeit, Eingangs- und Ausgangsgrößen von verschiedenen Bausteinen zu simulieren. Die Simulation ist für Testzwecke, z. B. im Rahmen des FAT, von großer Bedeutung, da sie dem Projektierer ermöglicht, digitale und analoge Ein- und Ausgänge so zu beeinflussen, dass komplexe Funktionen (z. B. Temperaturregelung) nachgestellt und überprüft werden können.

Aktivierung der Simulation

Das Aktivieren der Simulation für Testzwecke kann an den Kanaleingangstreiber- oder Kanalausgangstreiberbausteinen erfolgen.

Bei einem Ventil wird z. B. an den Eingängen SimOn die Simulation eingeschaltet, und an dem Eingang SIMPV_In kann der Eingang simuliert werden.



Simulation deaktivieren

Die aktivierten Simulationen sollten gemäß Guter Praxis notiert werden. Nach Abschluss des Tests müssen alle Simulationen wieder deaktiviert werden, bevor die Anlage für den Betrieb freigegeben wird.

Eine Übersicht der APL Bausteine mit aktiver Simulation kann auch über den Messstellenbrowser auf der OS angezeigt werden.

Hinweis

Wenn möglich können teilanlagenspezifisch zentrale Schalter zur Simulation Ein/Aus projektiert werden, die mit allen Eingangstreibern verschaltet sind. Nach Abschluss der Tests kann dieser zentrale Schalter gelöscht oder deaktiviert werden, wodurch die Simulation zentral abgeschaltet wird.

Forcen von Variablen

Im SIMATIC Manager kann man mithilfe einer Variablentabelle Ein- bzw. Ausgänge zusammenstellen und über das Menü einen Wert vorgeben (Variable -> Forcen). Wichtig ist auch hier, nach der Testdurchführung für ALLE Variablen das Forcen wieder zu deaktivieren.

Simulationssoftware SIMIT

SIMIT ermöglicht einen Software-Test über eine Simulationsplattform, ohne dass man die entsprechenden Feldgeräte benötigt. SIMIT simuliert Feldgeräte und ermöglicht eine vielfältige Anwendung von einfachen Signaltests per Knopfdruck bis hin zu komplexen Funktionstests (z. B. Temperaturreglung).

Zusammen mit der SPS-Simulationssoftware S7-PLCSIM oder SIMIT Virtual Controller (VC) zur Emulation der CPU eines Automatisierungssystems lassen sich so Software-Tests ohne Automatisierungsstation und Feldgeräte durchführen, was z. B. für den Akzeptanztest (FAT) beim Software-Ersteller genutzt wird.

Anwendung von SIMIT:

- I/O Simulation
- Prozesssimulation

- Virtuelle Abnahmetests und Inbetriebnahmeunterstützung
- Bedienerschulung

Hinweis

SIMIT eignet sich auch hervorragend für den Einsatz auf einer Test- bzw. Simulationsanlage. Nahezu alle designspezifischen und funktionalen Fehler können frühzeitig erkannt und noch vor der realen Inbetriebnahme behoben werden. Im Produktivbetrieb können darüber hinaus z. B. validierungspflichtige Änderungen vorab simuliert und getestet werden.

Siehe auch

- Handbuch "SIMIT", Online-Support unter Beitrags-ID 109801804 (https://support.industry.siemens.com/cs/ww/de/view/109801804)

Simulationshardware Simulation Unit (SU)

Die Simulation Unit ermöglicht in Verbindung mit der Software SIMIT ebenfalls einen Software-Test, ohne die Feldgeräte zu benötigen. Die SU stellt quasi ein Hardware-Interface für SIMIT zur Verfügung.

Die SU verfügt über Profibus und Profinet Schnittstellen, die wie Profibus bzw. Profinet Segmente an die AS angeschlossen werden und die Hardware simulieren. Der Vorteil hierbei ist, dass direkt die reale Hardware-Schnittstelle der AS angesprochen wird, was den Test noch realitätsnäher macht. Dies erhöht die Wahrscheinlichkeit, Fehler bereits vor der Inbetriebnahme zu entdecken und letztere damit zu verkürzen.

Die SU ist kein direkter Nachfolger der SIMBA Box, löst diese jedoch technisch ab..

7.4 Kontrolle der Konfiguration

7.4.1 Versionieren von Projekten mit Version Trail

Mit SIMATIC PCS 7 Version Trail können Multiprojekte, Einzelprojekte und projektspezifische Bibliotheken mit einer eindeutigen Versionskennzeichnung gespeichert und archiviert werden. Dies erfolgt nach dem Archivierungsverfahren von PCS 7. Projektspezifische Bibliotheken werden bei der Archivierung eines Multiprojektes mitgesichert und bleiben somit dem entsprechenden Multiprojekt zugeordnet.

Eine lückenlose Hochzählung der Versionen nach Validierungsgesichtspunkten wird von SIMATIC PCS 7 Version Trail gewährleistet. Eine abgeschlossene Version kann nicht mehr verändert werden. Jedoch kann jede archivierte Version mittels Version Trail oder im SIMATIC Manager ins System zurückgeladen werden.

Durch das ohnehin im GMP-Umfeld erforderliche Arbeiten mit SIMATIC Logon werden alle relevanten Aktionen unter dem angemeldeten Benutzer gespeichert.

Hinweis

Vor der Archivierung eines Multiprojektes muss überprüft werden, dass keine dem Multiprojekt zugehörigen Projekte oder Bibliotheken ausgehängt sind. Denn es werden lediglich Projekte und Bibliotheken archiviert, die zum Zeitpunkt der Archivierung im Multiprojekt enthalten sind.

Die zu archivierenden Projekte dürfen im SIMATIC Manager nicht geöffnet sein.

In einer validierten Anlage ist ein Rücklesen (Dearchivieren) älterer Projektversionen nur in Ausnahmefällen und in gemeinsamer Planung mit dem Anlagenbetreiber durchzuführen.

Siehe auch

- Handbuch "PCS 7 Engineering System", Kapitel 15.5.3, Online-Support unter Beitrags-ID 109800500 (https://support.industry.siemens.com/cs/ww/de/view/109800500)
- Online-Hilfe von SIMATIC PCS 7, Thema "Version Trail"

Hinweis

Die Projektstruktur wird nur einmalig beim Anlegen eines Archivs übernommen. Spätere Änderungen im eigentlichen Projekt werden von Version Trail nicht nachgezogen, sondern müssen händisch erfolgen.

Die Darstellung in Version Trail hat keinen Einfluss auf die eigentliche Archivierung. Jedoch können nur von den sichtbaren Elementen automatische Archivierungen erstellt werden.

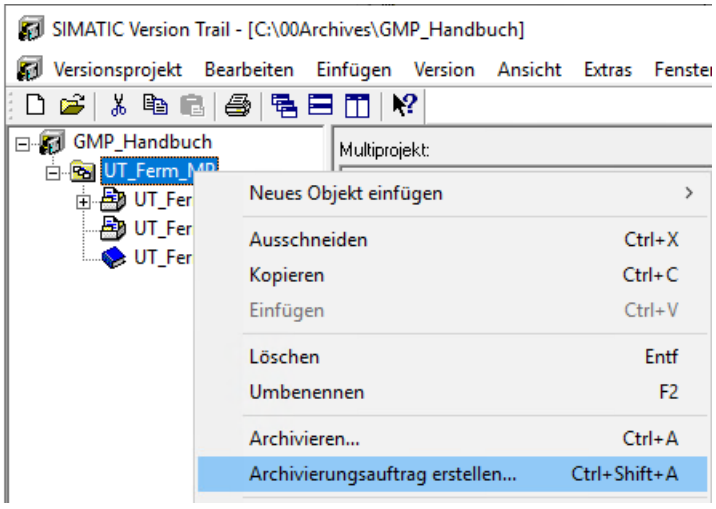
Automatisches Archivieren nach Download

Mit der Funktion "Projekt nach erfolgreichem Laden archivieren" wird unter Verwendung von SIMATIC Version Trail nach dem erfolgreichen Laden eine Projektsicherung der aktuell geladenen Softwareversion erzeugt.

Automatisches Archivieren zeitgesteuert

Auch ein automatisches Archivieren und Versionieren von Multiprojekten, Projekten und Bibliotheken zu definierten Zeiten ist möglich, inklusive dem zeitgesteuerten Rücklesen von Bausteinparametern. Die Windows Aufgabenplanung stößt dabei die Ausführung der jeweiligen Aufträge an.

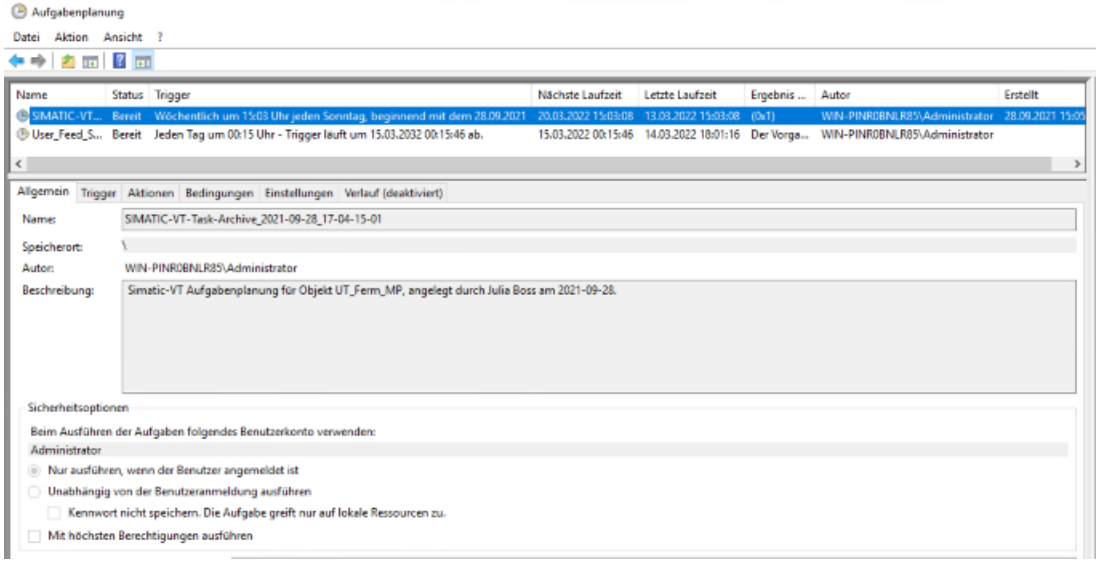
Dazu ist im Kontextmenü des gewünschten Objektes (Multiprojekt, Projekt, Bibliothek) "Archivierungsauftrag erstellen..." auszuwählen.



Für jedes Objekt kann dabei nur ein einziger Archivierungsauftrag erstellt werden. Besteht zu einem Objekt bereits ein Archivierungsauftrag, kann dieser über diesen Weg angepasst werden.

In dem sich öffnenden Dialogfenster gelangt man über den Button "Archivierungsauftrag erstellen / bearbeiten..." zur Windows Aufgabenplanung. Diese dient zum Anpassen der Parameter und stößt die Ausführung der erstellten Aufträge an.

In der Windows Aufgabenplanung ist im Ordner "Simatic VT" mit einem Doppelklick der entsprechende Auftrag auszuwählen. Es öffnen sich dessen Eigenschaften.



In den Registerkarten "Allgemein" und "Trigger" sind entsprechende Einstellungen vorzunehmen. Dabei ist besonders in der Registerkarte "Allgemein" auf die Sicherheitsoptionen bezüglich des Benutzerkontos zu achten. Denn an dieser Stelle kann eingestellt werden, ob die Archivierung benutzerabhängig oder unabhängig ablaufen soll und mit welchen Privilegien sie

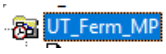
ausgeführt wird. Der Benutzer, unter dem dann die Archivierung stattgefunden hat, erscheint auch in der Versionstabelle in Version Trail.

Hinweis

In der Registerkarte "Allgemein" sollten unter "Beschreibung" aussagekräftige Informationen zur Aufgabe hinterlegt werden. Dazu zählen unter anderem der Name der Aktion, der Name des zu archivierenden Versionsobjekts, der Ersteller des Auftrags sowie das Datum der Erstellung / Modifikation.

Nun muss nur noch im Dialogfenster "Archivierungsauftrag erstellen" von Version Trail der Archivierungsauftrag aktiviert werden. An dieser Stelle kann außerdem eingestellt werden, ob die CPUs vor dem Archivieren zurückgelesen werden.

Das Symbol einer Uhr neben dem Archivierungsauftrag zeigt an, dass dieser auch aktiviert ist.



20 Sekunden vor dem Ausführen eines automatischen Auftrags erscheint ein Hinweis auf dem Bildschirm. So lange kann dieser noch abgebrochen werden.

Hinweis

Version Trail darf zum Zeitpunkt des Ausführens eines Auftrages **nicht** geöffnet sein, da dieser sonst nicht ausgeführt werden kann.

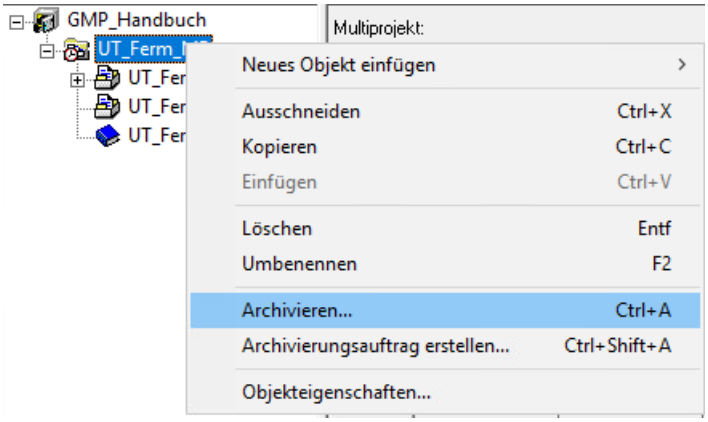
Automatisches Rücklesen

Die Windows Aufgabenplanung stößt auch das automatische Rücklesen der Online-Parameter an, wenn ein entsprechender Rückleseauftrag vorliegt. Über das Kontextmenü einer CPU kann dieser erstellt werden.

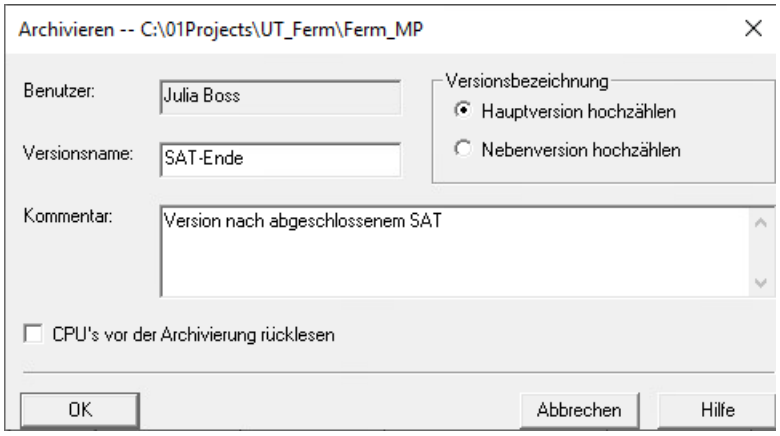
Beim Erstellen eines Rückleseauftrags gilt dieselbe Vorgehensweise wie bei einem Archivierungsauftrag. Einzig die Auswahl des Rückleseumfangs unterscheidet sich von dem eines Archivierungsauftrags. Hier kann zwischen allen Parametern, bedien- und beobachtbaren Parametern oder gekennzeichneten Parametern ausgewählt werden.

Manuelles Archivieren und Rücklesen

Version Trail bietet auch die Möglichkeit, ein manuelles Archivieren und/oder Rücklesen durchzuführen. Dazu ist im Kontextmenü des gewünschten Objektes "Archivieren..." bzw. "Rücklesen..." auszuwählen.



Daraufhin öffnet sich das jeweilige Dialogfenster. Auch beim manuellen Archivieren kann ausgewählt werden, ob vorher die CPUs zurückgelesen werden sollen oder nicht. Ein sinnvoller Kommentar ist hilfreich.



Beim manuellen Archivieren kann beim Hochzählen zwischen Hauptversion und Nebenversion gewählt werden.

Dearchivieren

Archivierte Objekte (Multiprojekte, Projekte, Bibliotheken) können jederzeit wieder dearchiviert werden, siehe allerdings den Hinweis zu Beginn dieses Abschnitts "Versionieren von Projekten mit Version Trail".

Der entsprechende Eintrag im Versionsprojektfenster von Version Trail ist zu markieren und im Kontextmenü der Punkt "Dearchivieren..." auszuwählen.

Löschen

Archivierte Objekte können auf dieselbe Art und Weise wie sie dearchiviert werden auch gelöscht werden. Dazu ist im Kontextmenü des ausgewählten Eintrags der Punkt "Löschen" auszuwählen. Es wird nur der ausgewählte Eintrag gelöscht.

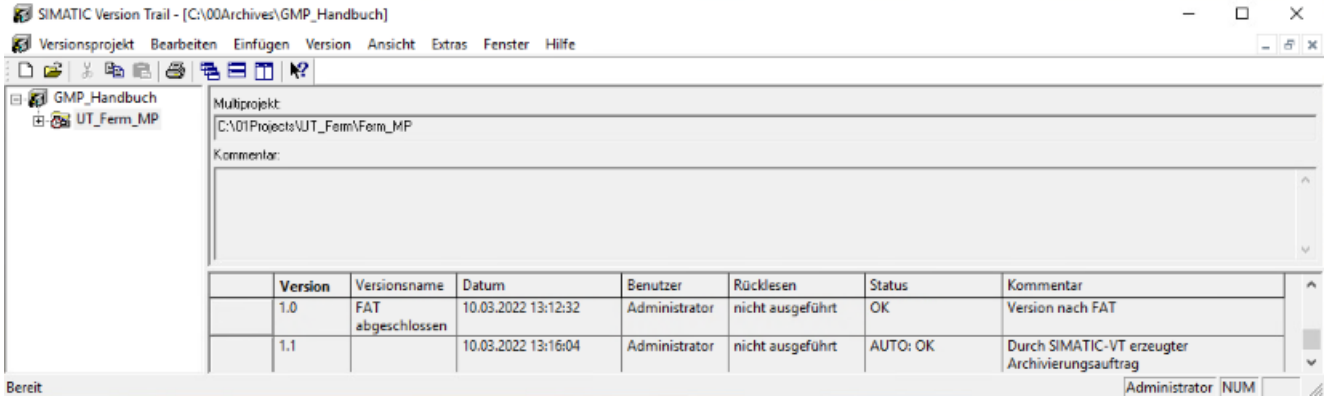
Um alle Einträge eines Versionsarchivs zu löschen, muss direkt in der Baumstruktur das entsprechende Element ausgewählt und im Kontextmenü der Punkt "Löschen" gewählt werden.

Vergleich der archivierten Projekte

Aus der Oberfläche in Version Trail heraus können archivierte Projekte untereinander oder auch mit der Online-Version verglichen werden. Version Trail bedient sich hierbei der Funktion des Version Cross Manager, ruft diesen auf und zeigt die Unterschiede an, siehe hierzu Kapitel "Versionsvergleich mit Version Cross Manager (VXM) (Seite 159)".

Versionshistorie

SIMATIC PCS 7 Version Trail verwaltet sämtliche Aktionen wie z. B. Anlegen, Archivieren, Löschen von Versionsständen, etc. eines Versionsprojektes in der Versionshistorie. Die Versionshistorie kann über das Menu **Extras > Version Trail** aufgerufen werden. Hier werden alle Aktionen bezüglich des Archivierens von Projekten sowie auch das Löschen von Versionsständen mitgeloggt. Das nachfolgende Bild zeigt die Versionshistorie vom Anlegen des Versionsprojektes bis zur Archivierung von verschiedenen Versionsständen.



Bei kontinuierlicher Archivierung über SIMATIC PCS 7 Version Trail bietet die Versionshistorie eine gute Möglichkeit zur Dokumentation von verschiedenen Softwareständen während des Lebenszyklus eines Automatisierungssystems.

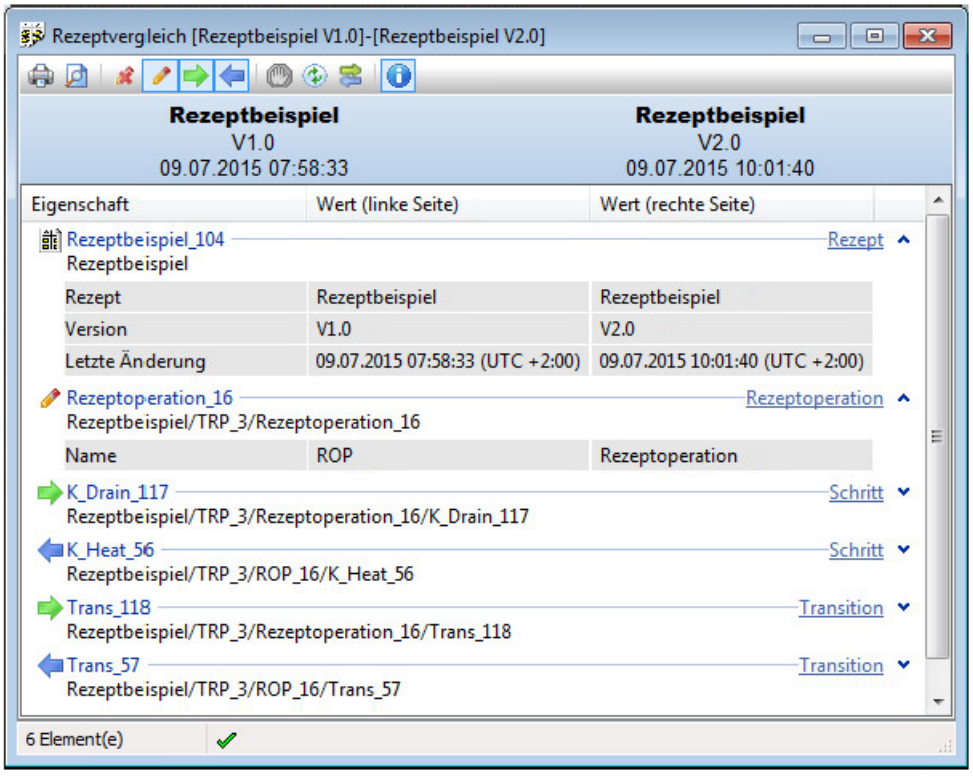
Es werden sämtliche Softwarestände mit Archivierungsdatum und Version in chronologischer Reihenfolge aufgelistet. Somit kann bei Verlust der Anwendersoftware der aktuelle Softwarestand sicher zurückgespielt werden.

7.4.2 Rezeptvergleich

Der **Vergleich von Rezeptobjekten** ermöglicht einen Vergleich verschiedener Versionen von Grundrezepten, Bibliotheken und Formulas.

Siehe auch

- Handbuch "SIMATIC BATCH", Kapitel 9.5.9, Online-Support unter Beitrags-ID 109794450 (https://support.industry.siemens.com/cs/ww/de/view/109794450)



7.4.3 Versionsvergleich mit Version Cross Manager (VXM)

Der Version Cross Manager vergleicht in Projekten u. a. folgende Objekte:

- Bibliothek
- HW Konfiguration
- CFC/SFC Engineeringdaten, z. B. Pläne, Typen, Planordner, Bausteinordner
- S7-Programm, S7-Bausteine, S7-Symbole
- Globale Deklarationen
- Meldungen

Die zu vergleichenden Projekte werden synchron abgearbeitet, d. h. die Objektbäume der zu vergleichenden Softwarestrukturen werden Attribut für Attribut verglichen. In einem Ergebnisbaum wird der Veränderungsvergleich farblich dargestellt.

Projektunterschiede speichern oder drucken

Die durch den Vergleich ermittelten Projektunterschiede können in einer CSV-Datei gespeichert oder auf einem Drucker ausgegeben werden. Die früher vorhandene Berichtsfunktion des VXM kann auch in neueren Versionen von PCS 7 noch genutzt werden, siehe Support-Beitrag.

Die nachfolgenden Informationen werden dargestellt:

- Zusätzlich enthaltene Objekte in Projekt A
- Zusätzlich enthaltene Objekte in Projekt B
- Unterschiede zwischen Projekt A und Projekt B

Hinweise zur betrieblichen Änderungskontrolle siehe Kapitel "Betriebliche Änderungskontrolle (Seite 170)".

Siehe auch

- FAQ "Verwenden der Berichtsfunktion in VXM", Online-Support unter Beitrags-ID 109755393 (https://support.industry.siemens.com/cs/ww/de/view/109755393)

7.4.4 Konfigurationskontrolle mit "versiondog"

Das PCS 7 Add-on "versiondog" kombiniert die Funktionalitäten von SIMATIC Version Trail und Version Cross Manager und geht im Funktionsumfang noch darüber hinaus. Es kann als zentrales Werkzeug für Datensicherung, Änderungskontrolle und Software-Versionierung eingesetzt werden.

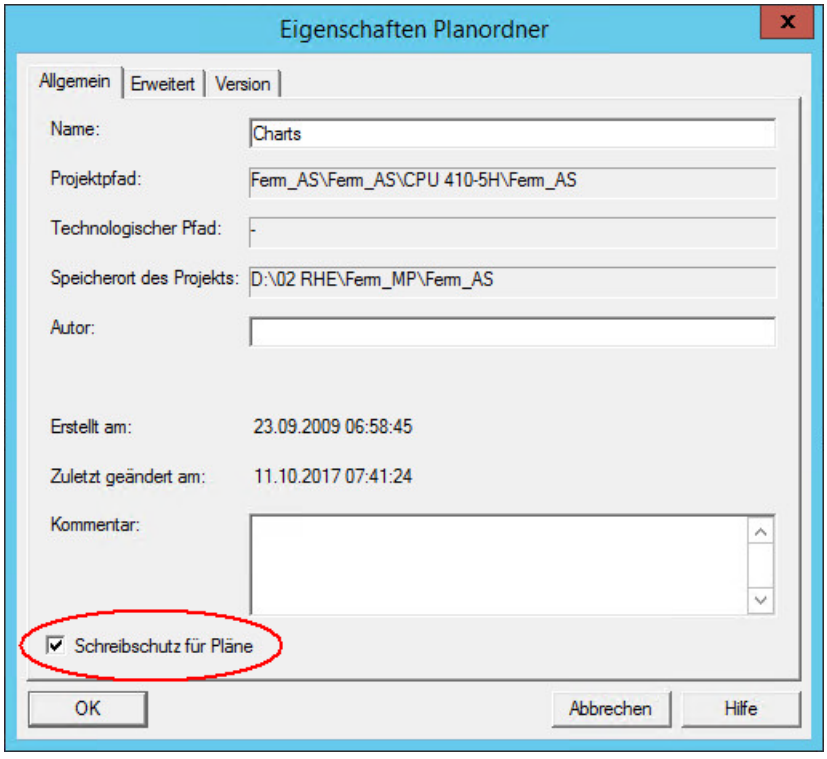
Weitere Hinweise beinhaltet das Kapitel "versiondog – Versionierung und Konfigurationskontrolle (Seite 39)" sowie der PCS 7 Add-on-Katalog.

7.5 Schreibschutz

7.5.1 Schreibschutz von CFC/SFC-Plänen und SFC-Typen

Zum sicheren Betreiben der Anlage nach der Inbetriebsetzung bzw. nach der Verifizierung gibt es die Möglichkeit, CFC/SFC-Pläne und SFC-Typen mit einem Schreibschutz zu versehen. Ist der Schreibschutz aktiviert, so kann das Betriebs- und Wartungspersonal lediglich CFC/SFC-Pläne oder SFC-Typen öffnen und Prozesswerte online beobachten, jedoch keine beabsichtigten oder auch unbeabsichtigten Änderungen an Plänen und Typen durchführen.

Zur Aktivierung des Schreibschutzes kann in den Eigenschaften des Planordners der Schreibschutz für jede Automatisierungsstation markiert werden.



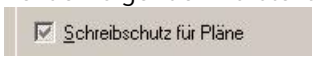
Der Projektmitarbeiter hat auch die Möglichkeit, den Schreibschutz von einzelnen Plänen oder SFC-Typen zu aktivieren oder zu deaktivieren.

Das Optionskästchen "Schreibschutz für Pläne" kann hierbei in zwei unterschiedlichen Darstellungen angezeigt werden.

Bei der folgenden Darstellung ist der Schreibschutz für alle Pläne aktiviert

Hintergrund weiß und Haken schwarz:

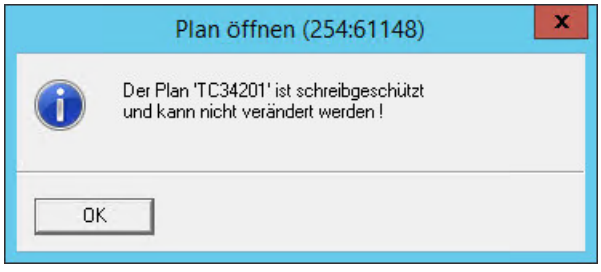
Bei der folgenden Darstellung ist nur ein Teil der Pläne oder SFC-Typen schreibgeschützt.



Hintergrund schraffiert und Haken grau:

Ist der Schreibschutz nicht für alle Pläne aktiviert, so kann durch einmaliges Deaktivieren und Aktivieren am Ordner "Pläne" der Schreibschutz für alle CFC/SFC-Pläne und SFC-Typen der jeweiligen Automatisierungsstation aktiviert werden.

Wird der Plan eines CFC/SFC oder SFC-Typs geöffnet, so bekommt man bei schreibgeschützten Plänen folgenden Hinweis:



Hinweis

In der Prozessobjektsicht können auch dann Änderungen vorgenommen werden, wenn die Planordner schreibgeschützt sind.

Siehe auch

- Handbuch "PCS 7 Engineering System", Kapitel 4.3.4, Online-Support unter Beitrags-ID 109800500 (https://support.industry.siemens.com/cs/ww/de/view/109800500)

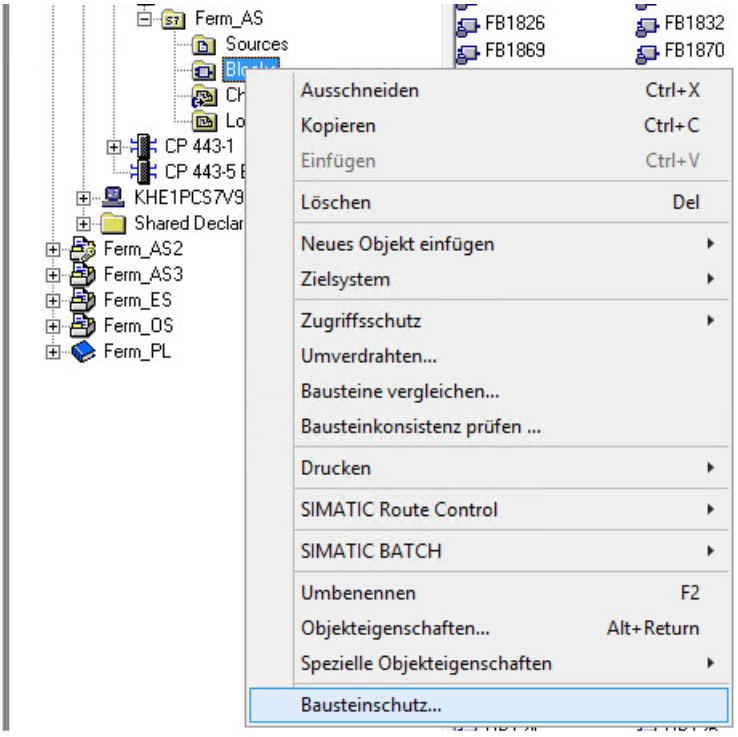
7.5.2 Bausteinverschlüsselung mit "S7-Block Privacy"

Mit Hilfe des Erweiterungspakets "S7-Block Privacy" können Funktionsbausteine (FB) und Funktionen (FC) ver- und entschlüsselt werden. Es ist nicht möglich andere Bausteine, wie Organisationsbausteine (OB), fehlersichere Bausteine oder Bausteine mit "Know-How-Protection" zu verschlüsseln. Die Verschlüsselung erfolgt direkt in der Datenbank eines Projektes. Alle FBs und FCs, welche verschlüsselt wurden und in die AS geladen sind, haben den Status "S7-Block- Privacy".

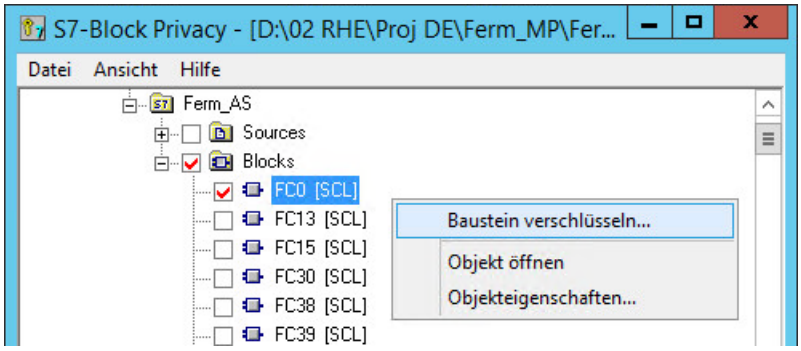
"S7-Block Privacy" bietet eine höhere Sicherheit als der KNOW-HOW Schutz eines Bausteins und sollte deshalb besonders für sensible Bereiche bevorzugt verwendet werden.

Vorgehensweise

Zum Verschlüsseln ist im Kontextmenü eines Bausteinordners "Bausteinschutz" auszuwählen.



In der sich öffnenden Baumstruktur des Verschlüsselungstools werden die im Projekt vorhandenen Bausteine und SCL-Quellen aufgelistet. Die mit einem Häkchen markierte Auswahl kann mit der Auswahl "Baustein verschlüsseln..." im Kontextmenü verschlüsselt werden. Daraufhin öffnet sich ein Dialog, dessen Anweisungen zu befolgen sind.



SCL-Quellen

SCL-Quellen, die im Projekt enthalten sind und deren Bausteine verschlüsselt worden sind, sollten vor Übergabe des Projektes an Dritte gelöscht werden. Dies kann ebenfalls in der Applikation "S7-Block Privacy" vorgenommen werden. Dazu ist im Kontextmenü der Quelle die Funktion "Quelle löschen" auszuwählen.

Hinweis

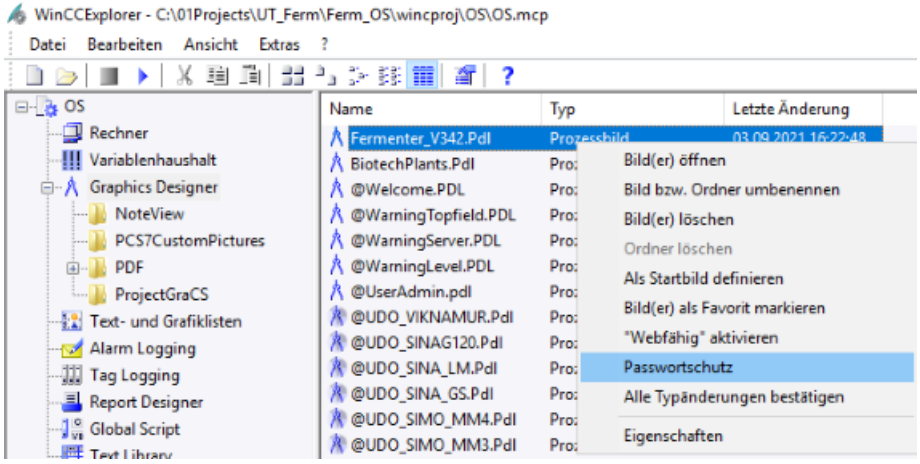
Nachdem die Quellen gelöscht wurden und aus der Baumstruktur entfernt sind, muss der Quellordner noch reorganisiert werden. Denn erst durch die Reorganisation werden die Quellen tatsächlich gelöscht. Zuvor wurden sie nur für das Löschen vorgemerkt und aus dem SIMATIC Manager entfernt. Am eigentlichen Speicherort des Projektes sind sie aber noch vorhanden.

Entschlüsseln

Zum Entschlüsseln ist dieselbe Vorgehensweise wie beim Verschlüsseln zu wählen. Jedoch sind hierzu der richtige Schlüssel und die Rückübersetzungsinformation notwendig.

7.5.3 Schutz von Grafikbildern

Bedienbilder können mit einem Passwort gegen Modifikation geschützt werden. Dies erfolgt im WinCC Explorer per Markierung eines oder mehrerer Bilder im Kontextmenü.



7.6 Hinweise für die Systemübergabe

Für die Systemübergabe sollten folgende Aspekte frühzeitig geklärt sein:

- Welche Dokumente in welchem Format übergeben werden.
- Schulung von Bedien- und Wartungspersonal
- Hinweise für Systembetrieb, z. B. Archivierung, Backup, Kalibrierung
- Rücksetzen von Simulationen, etc.

Hinweis

Bei Übergabe des Systems müssen zwingend alle Testaccounts gelöscht und Standard-Passwörter geändert werden!

Datensicherung

8

Regelmäßige Datensicherungen müssen nicht nur während der Projektierungsphase erstellt werden, um Datenverluste zu vermeiden.

Auch in der Betriebsphase sind verschiedene Datensicherungen notwendig, um eine reibungslose Systemwiederherstellung im Falle von Datenverlusten oder Systemausfällen zu garantieren. Dazu bedarf es auch eines Notfallplanes.

Neben der Sicherung der Systeminstallation sollten auch die Projektierungsdaten regelmäßig gesichert werden, um z. B. nach einem Hardwaredefekt oder Datenverlust auf die zuletzt aktuelle Systemkonfiguration zurückgreifen zu können.

Folgende Datensicherungen sollten betrachtet werden:

- Sicherungen der Systeminstallation, siehe Kapitel "Sicherung der Systeminstallation (Seite 165)"
- Sicherung der Installation einschließlich aller Projektdateien (Image) nach Systemaktualisierungen und größeren Projekt-Änderungen sowie periodisch, z. B. alle 12 Monate
- Änderungsgetrieben Sicherung der Projektdaten vor / nach jeder Änderung
- Periodisches Sichern bzw. "Umkopieren" aller archivierten Daten zur Sicherstellung der Lesbarkeit der Daten, z. B. alle 3-5 Jahre

Hinweis

Die Sicherungen der Anwender-Software und die Sicherung der Systempartition mit und ohne SIMATIC PCS 7 sollten auf externen Speichermedien aufbewahrt werden (z. B. CD, DVD, Netzwerksicherung).

Siehe auch

- Kapitel "Systemwiederherstellung (Seite 173)"

8.1 Sicherung der Systeminstallation

Die Sicherung des Betriebssystems und der PCS 7- Installation sollte mit Festplatten-Images durchgeführt werden. Mit diesen Images kann der Ursprungszustand der PCs wieder hergestellt werden.

Welche Images sind sinnvoll?

- Erstellung eines Images der Betriebssysteminstallation mit allen Treibern sowie sämtlichen Einstellungen bzgl. Netzwerk, Benutzerverwaltung, etc., aber ohne SIMATIC PCS 7
- Erstellung eines Images der installierten PCs mit SIMATIC PCS 7
- Erstellung eines Images der installierten PCs mit SIMATIC PCS 7 einschließlich aller Projekte

Hinweis

Ein Image kann immer nur auf einem PC mit identischer Hardware eingespielt werden. Aus diesem Grund ist die hardwareseitige Konfiguration der PCs geeignet zu dokumentieren, z. B. mit Hilfe der SIMATIC Management Console.

Images von einzelnen Partitionen können nur zwischen imagekompatiblen PCs ausgetauscht werden, da sich verschiedene Einstellungen, z. B. in der Registry, auf den PCs unterscheiden.

8.2 Datensicherung der Applikationssoftware

Es wird empfohlen, regelmäßige Datensicherungen der Projektdaten zu erstellen. In einem Speicherkonzept wird z. B. festgelegt, dass nach jeder Änderung das Projekt gesichert wird. Diese Projektsicherung kann auf verschiedene Weise durchgeführt werden.

Siehe auch

- Handbuch "PCS 7 Serviceunterstützung und Diagnose", Kapitel 3.2 "Datensicherung", Online-Support unter Beitrags-ID 109794378 (https://support.industry.siemens.com/cs/ww/de/view/109794378)

Sicherung der Anwender-Software im Engineering System

Hierfür sollte die Systemfunktion "Projekt archivieren" im SIMATIC Manager oder das Optionspaket "Version Trail" für eine versionsbasierte Archivierung genutzt werden.

Ab V9.1 SP1 können die archivierten Projekte mit einem Hash gesichert werden, sodass eine Manipulation des Projekts erkannt wird.

Mit der Option SIMATIC Version Trail kann das Projekt manuell oder zeitgesteuert gesichert und gleichzeitig die Versionen kontrolliert werden. Es kann über die Oberfläche auch eine ältere Version zurückgespielt werden.

Siehe auch

- Kapitel "Versionieren von Projekten mit Version Trail (Seite 153)"

Hinweis

Bei Datensicherungen im Betrieb der Anlage sollte berücksichtigt werden, ob und welche Online-Parameter zuvor zurück zu lesen sind.

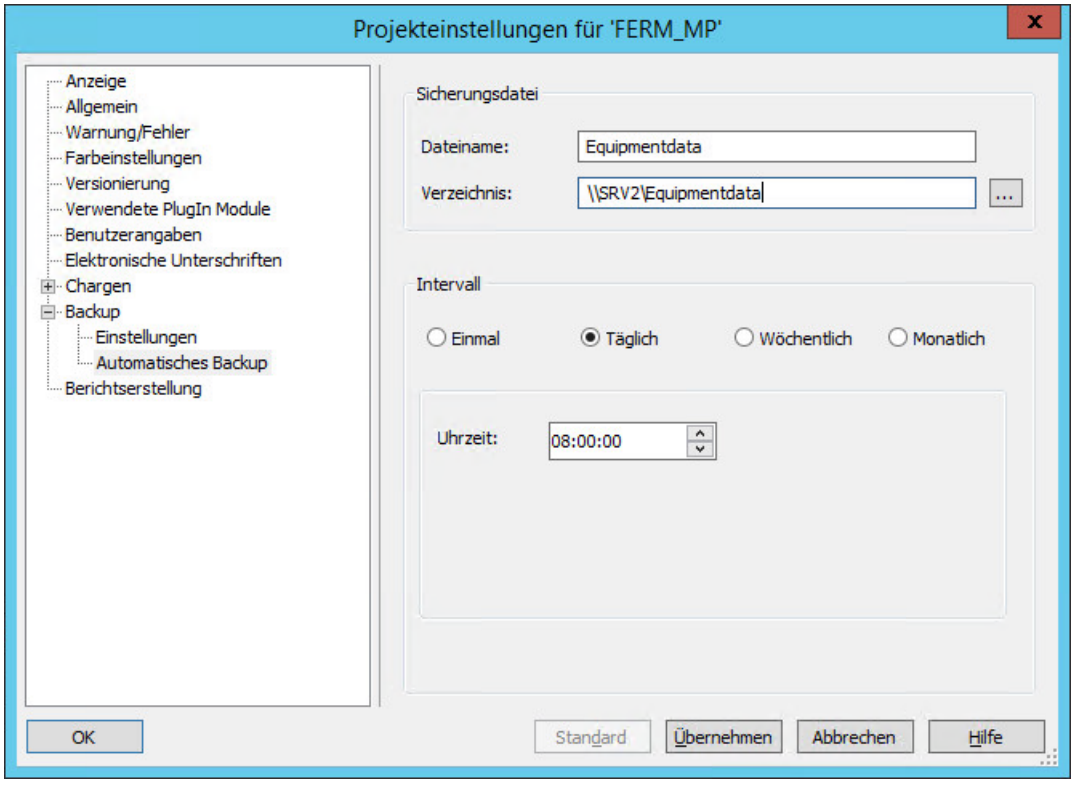
Nicht zurückgelesene Parameteränderungen gehen im Falle einer System- bzw. Projektwiederherstellung verloren.

Sicherung der Rezeptdaten in SIMATIC BATCH

Neben der Projektkonfiguration in PCS 7 müssen auch die Anwenderdaten in SIMATIC BATCH (Bibliotheken, Grundrezepte, Stoffe, Benutzerrechte, usw.) gesichert werden. Dies erfolgt aus dem SIMATC BATCH Control Center.

SIMATIC BATCH unterstützt ein automatisches und zeitgesteuertes Sichern der BATCH-Projektdaten. Dies beinhaltet z. B.:

- Anlageneinstellungen
- Projekteinstellungen
- Bibliotheken
- Formulas
- Grundrezepte
- Materialien



Mit dem Befehl "Restore" können die Backup-Daten zurückgespielt werden.

Sicherung der Konfiguration von SIMATIC Route Control

Beim Laden der Projektierung in SIMATIC RouteControl werden ab SIMATIC PCS 7 V9.1 SP1 alle für die CSV-Schnittstelle beschriebenen Route Control Engineering-Daten und die Materialkonfigurationsdaten automatisch exportiert.

Betrieb, Wartung und Instandhaltung

9

9.1 Betrieb und Überwachung

9.1.1 Prozessvisualisierung

SIMATIC PCS 7 bietet eine umfangreiche Prozessvisualisierung. Für jeden Einsatzzweck lassen sich individuell projektierte Bedienoberflächen erstellen – zur sicheren Prozessführung und zur Optimierung der gesamten Produktion.

Runtime-Daten können anhand von Protokollen vom System ausgegeben werden.

9.1.2 Benutzerdokumentation

Ab SIMATIC PCS 7 V9.0 steht der PUD (Plant and User Documentation) Manager Help Viewer zur Offline-Anzeige der Dokumentation zur Verfügung. Er ist ein Bestandteil des SIMATIC PCS 7 Software-Pakets. Durch Hinzufügen von Dokumentationspaketen erweitern und aktualisieren Sie individuell den Umfang Ihrer Benutzerdokumentation.

Mit der Installation von SIMATIC PCS 7 beinhaltet der PUD Manager Help Viewer folgende Dokumentation:

- SIMATIC PCS 7 Help Center
- OS-Prozessführung

Siehe auch

- PUD Manager Erläuterung und Download, Online Support unter Beitrags-ID 109748882 (https://support.industry.siemens.com/cs/ww/de/view/109748882)

9.1.3 Audit Trail Review

Im regulierten Umfeld muss nicht nur ein Audit Trail für Änderungen an GMP-kritischen Daten geführt werden, sondern dieser Audit Trail muss auch regelmäßig geprüft werden. Dies kann zum einen durch die regelmäßige Überprüfung der Funktionalität bei gleichzeitiger Einarbeitung der relevanten Audit Trails in entsprechende Produktionsberichte erfolgen. Zum anderen können aber z. B. auch Auswertungen über kritische Alarme, Bedienereingaben und Häufigkeitsanalysen von Meldungen dem Ziel dienen, den Prozess zu verbessern.

Hilfsmittel für den Audit Trail Review können sein:

- Mögliche Inhalte eines Audit Trails, siehe Kapitel "Audit Trail und Änderungskontrolle (Seite 119)"
- Meldeklassen und Prioritäten, siehe Kapitel "Alarm Management (Seite 112)"

- Optionen zur Protokollierung, siehe Kapitel "Protokollierung (Seite 36)" sowie "Erstellen von Protokollen in SIMATIC BATCH (Seite 110)"
- Umfangreiche Analyse von Meldungen verschiedenster Quellen mit Hilfe des WinCC Add-ons PM-ANALYZE (https://www.siemens.de/industrysolutions/de/en/wincc/products/pm-analyze/Pages/Default.aspx)

9.2 Betriebliche Änderungskontrolle

Änderungen an validierten Anlagen müssen unbedingt in Abstimmung mit dem Anlagenbetreiber geplant, dokumentiert und erst nach Freigabe durchgeführt und getestet werden.

Nachfolgend wird beispielhaft die Vorgehensweise bei Änderungen beschrieben:

1. Initiative, Beschreibung und Freigabe der geplanten Änderung durch den Anlagenbetreiber
2. Überprüfung und Sicherung der aktuellen Version der Applikationssoftware (Projektdaten)
3. Anpassen der Systemspezifikation
4. Durchführung der Änderung inkl. Dokumentation der durchgeführten Änderung (evtl. Unterstützung durch Tool-Vergleich)
5. Test der Änderung inkl. Testdokumentation in geeigneter Form
6. Sicherung des geänderten Projektes mit neuer Versionskennzeichnung

Die Auswirkungen der Änderung auf andere Teile der Applikation und die daraus resultierenden Tests sind risikobasiert festzulegen und zu dokumentieren.

Dabei kann es sinnvoll sein, verschiedene Tätigkeiten zu kategorisieren und den Änderungsaufwand am Risiko zu bemessen. Bei einem 1:1 Austausch einer Hardware-Komponente zum Beispiel dürfte das Risiko geringer sein als bei einem ungleichen Austausch.

Des Weiteren kann bei Software-Updates eine Abwägung erforderlich sein zwischen Systemsicherheit und Vorschriftenkonformität, siehe auch "Aktualisierung der Systemsoftware (Seite 176)".

Siehe auch

- GAMP 5-Leitfaden, Anhang O6
- GAMP Good Practice Guide "Operation of GxP Computerized Systems", Kapitel 10

9.3 Wartung und Instandhaltung

Zugänge und Berechtigungen für Wartungspersonal müssen kontrolliert und dokumentiert sein. Sie müssen im Berechtigungskonzept ebenso berücksichtigt sein wie die betrieblichen Rechte und diejenigen für Administratoren.

Auch Wartungsaktivitäten sind Änderungen am validierten Gesamtsystem. Oft existieren für wiederkehrende Tätigkeiten standardisierte Vorgehensweisen auf Betreiberseite, so dass nicht für jede einzelne Aktion ein Änderungsantrag erforderlich ist. Die Tätigkeiten müssen aber zeitlich koordiniert und auf alle Fälle gemäß Vorschrift dokumentiert werden.

9.3.1 Besonderheiten bei der Fernwartung

Für Fernzugriffe gibt es verschiedene technische Möglichkeiten. Je nach Programm muss zur Einwahl auf eine fremde PC-Station neben der vorhandenen Zugangsberechtigung (Benutzername und Passwort) auch der Remote-Zugang an sich freigeschaltet werden. Dies sollte allerdings im Rahmen des Gesamtsystems geplant und dokumentiert werden, da der Zugriff kontrolliert sein muss. Siehe dazu auch die Kapitel 3.2 (Seite 28) sowie Kapitel 4.6 (Seite 55).

Hinweis

Die Einrichtung einer Fernwartungsmöglichkeit ist mit dem Anlagenbetreiber abzustimmen. Auch jeder einzelne Verbindungsaufbau (Anmeldung) mit dem System bedarf oft der ausdrücklichen Zustimmung des Anlagenverantwortlichen. Auch per Fernzugriff durchgeführte Änderungen müssen gemäß Betreibervorschrift dokumentiert werden.

Siehe auch

- Liesmich PCS 7 V9.1, Kapitel 3.4.14; Online-Support unter Beitrags-ID 109780270 (https://support.industry.siemens.com/cs/ww/de/view/109780270)

Eine sinnvolle Variante ist z. B., neben der Vergabe der logischen Zugriffsberechtigung eine physische Verbindung nur im Bedarfsfall und nur unter Anwesenheit des Vorort-Wartungspersonals herzustellen.

9.3.2 Asset Management

Asset Management hat in der Prozesstechnik das Ziel, durch geeignete Maßnahmen eine möglichst hohe Verfügbarkeit einer Produktionsanlage bei möglichst geringen Betriebskosten zu gewährleisten. Die effizienteste Strategie ist unbestritten die zustandsorientierte Instandhaltung mit einer möglichst kontinuierlichen Zustandserkennung als notwendige Voraussetzung. Das möglichst genaue Wissen um den aktuellen Zustand der Anlage ist Basis des Asset Managements, sodass die richtigen Instandhaltungsmaßnahmen am richtigen Ort zum richtigen Zeitpunkt abgeleitet werden können.

Realisierung in PCS 7

Zur Instandhaltung von Anlagen wird in SIMATIC PCS 7 das integrierte Asset Management verwendet. Zusätzliche Hardware oder Software-Werkzeuge entfallen. Anlagenfahrer und Instandhalter nutzen dieselben SIMATIC PCS 7-Werkzeuge und Bedienoberflächen mit für den jeweiligen Aufgabenbereich gefilterten und aufbereiteten Informationen. Während der Anlagenfahrer über die PCS 7 Operator-Station (OS) den Prozess bedient und beobachtet, kontrolliert der Instandhalter per Maintenance-Station (MS) die Hardwarestruktur der Produktionsanlage, um Diagnose- und Wartungsanforderungen bearbeiten zu können.

Mit den in SIMATIC PCS 7 integrierten Diagnose- und Instandhaltungsfunktionen können die verschiedenen Komponenten einer PCS 7-Anlage überwacht werden.

PCS 7 Maintenance Station (MS) ist in den Ausprägungen Basis, Standard und PDM erhältlich.

Hinweis

In Verbindung mit PDM kann von jedem MS-Client aus die erweiterte Diagnose der Feldgeräte geöffnet werden. Über einen Maintenance Client können die Geräteparameter von Feldgeräten ausgelesen und bearbeitet werden.

Dokumentation hierzu siehe

- Handbuch "PCS 7 Maintenance Station", Online-Support unter Beitrags-ID 109794384 (https://support.industry.siemens.com/cs/ww/de/view/109794384)
- Handbuch "PCS 7 Serviceunterstützung und Diagnose", Online-Support unter Beitrags-ID 109794378 (https://support.industry.siemens.com/cs/ww/de/view/109794378)
- Handbuch "PCS 7 Hilfe zu PDM", Online-Support unter Beitrags-ID 109794428 (https://support.industry.siemens.com/cs/ww/de/view/109794428)

Der Instandhalter hat ausgehend von einer Übersichtsdarstellung (Anlagensicht) im Bedarfsfall Zugriff auf alle Details der Komponenten und Geräte. Die Übersichtsdarstellung visualisiert mit Symbolen den Zustand einer Komponente selbst und als Sammelinformation die Zustände aller Geräte der unterlagerten Hierarchien.

Auf der obersten Ebene gibt es 4 Bereiche:

- IPC Bereich (IPC's, Server, Clients, ES, PH)
- Netzwerk-Bereich (Netzwerkswitche)
- AS Bereich, welcher wiederum in zwei Sub-Bereiche unterteilt ist
  - CPU Bereich
  - Feldgeräte-Bereich
- Benutzerbereich (Überwachung von Anlagenteilen aufgrund von Projektierten Kenngrößen wie z. B. Betriebsstunden oder Schaltzyklen)

Die Sammelzustandsmeldung zeigt nach Art einer Ampel den Gutzustand bzw. die Schwere des Problems gemäß NE107 an.

Über das Diagnose-Faceplate einer überwachten Komponente können Instandhaltungsarbeiten direkt angefordert werden. Die Anforderung ist dann vom Anlagenfahrer (OS) über das Standard-Faceplate freizugeben, bevor der Instandhalter mit dem angeforderten Service beginnen kann.

Über das gleiche Interface kann der Status der Arbeit angegeben und überwacht werden. Dies wird als Bedienmeldung protokolliert und in den Symbolen signalisiert. Zu jeder Arbeitsanforderung kann eine Arbeitsanweisungsnummer und ein Kommentar eingegeben werden. Ebenfalls können Servicetermine bzw. Intervalle festgelegt werden. Nach Ablauf des eingestellten Intervalls wird automatisch eine Systemmeldung erzeugt, die auf den erforderlichen Service, z. B. eine notwendige Kalibrierung, hinweist.

Zu jeder Komponente kann ein Protokoll erstellt und ausgedruckt werden. Nützlich kann die Erstellung von Protokollen für ganze Gerätegruppen sein. Hierbei ist es möglich, Geräte nach deren Priorität zu filtern. Voraussetzung dafür ist die entsprechende Kennzeichnung der Geräte, die im SIMATIC Manager vorgenommen wird. Aktuell ist eine Kennzeichnung der Geräte als "wichtig" oder "SIF" (Safety relevant) möglich.

Condition Monitoring

Oft ist es erforderlich, bestimmte verfahrenstechnische, chemische und mechanische Zustände im Wartungskonzept einer Anlage zu berücksichtigen. Das sogenannte Condition Monitoring (z. B. Arbeitspunkte von Pumpen, Lagerüberwachung von Motoren) wird hierbei hauptsächlich vorbeugend eingesetzt. Bevor es zu kritischen Zuständen kommt, wird der Anwender automatisch darüber informiert.

Asset Management in PCS 7 bietet die Möglichkeit, anwenderspezifische wartungsrelevante Prozess- oder Kenngrößen, z. B. Betriebsstunden oder Schaltzyklen, in die bestehende Diagnosestruktur einzubinden. PCS 7 stellt dafür die entsprechenden Schnittstellen, einen Funktionsbaustein auf der AS und ein Faceplate auf der OS zur Verfügung.

9.4 Systemwiederherstellung

Mit Hilfe von Datensicherungen wird das System nach einem Ausfall wiederhergestellt. Die Sicherungsdaten müssen mit allen zur Wiederherstellung notwendigen Materialien (Grundsystem, Einspielsoftware, Dokumentation) an definierter Stelle hinterlegt werden.

Ein Systemausfall (auch Desaster genannt) kann z. B. folgende Ursachen haben:

- Beschädigung des Betriebssystems oder installierter Programme
- Beschädigung der Systemkonfigurations- / Projektierungsdaten
- Verlust oder Beschädigung der Runtime-Daten
- Beschädigung oder Ausfall der Hardware

Es muss ein Desaster Recovery Plan vorliegen und regelmäßig geprüft werden.

Wiederherstellung des Betriebssystems und der installierten Software

Die Wiederherstellung des Betriebssystems und der installierten Software wird mit dem Einspielen des entsprechenden Images durchgeführt (siehe Kapitel "Datensicherung (Seite 165)"). Dabei ist die Anleitung des jeweiligen Softwarelieferanten für die Datensicherungsapplikation zu beachten.

Falls kein PC mit baugleicher Hardware-Konfiguration zur Verfügung steht, muss die Installation komplett neu durchgeführt werden. Dazu kann die Dokumentation zur Qualifizierung der Software herangezogen werden, in der die installierte Software mit den zusätzlich installierten Updates, Upgrades und Hotfixes beschrieben ist.

Wiederherstellung der Applikationssoftware

Abhängig von der Art der Sicherung wird das Wiederherstellen der Applikationssoftware durchgeführt.

Folgende Schritte können dabei relevant sein:

- Zurücklesen der Daten über die Software Version Trail
  Version Trail listet alle Sicherungsstände mit Haupt- und Nebenversion auf. Über die Schaltfläche Dearchivieren wird der ausgewählte Sicherungsstand zurückgelesen.
- Zurücklesen der Daten aus einem manuell erzeugten Sicherungsstand

- Zurücklesen der Rezepte
- Zurücklesen von Archiven
  Dies betrifft je nach Systemkonfiguration und Umfang der Störung: Prozessdaten, Meldungen, Chargendaten, Log-Dateien, etc.

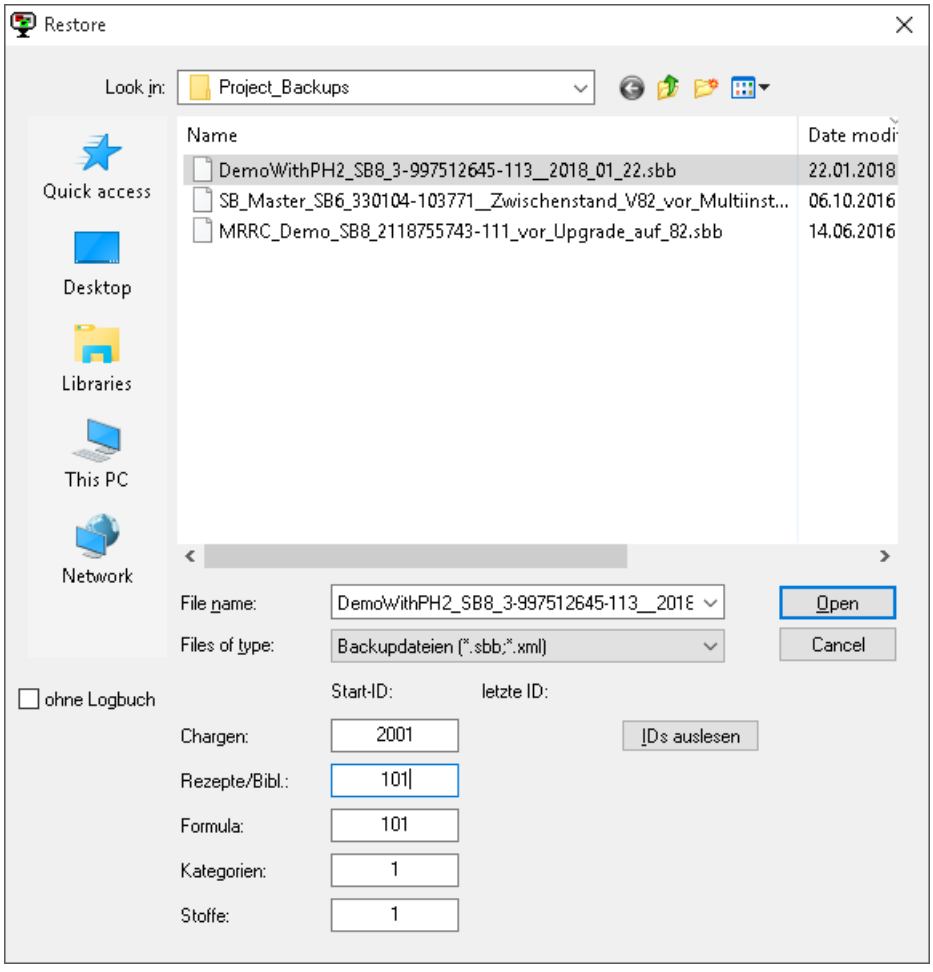
Projektspezifische Anpassungen

Projektspezifische Anpassungen am System, die nicht mit der Projektdatei gespeichert werden, müssen wiederhergestellt werden.

Backup/Restore der SIMATIC BATCH Datenbank

Beim Rücklesen einer Datensicherung der SIMATIC BATCH Datenbank kann eine Start-Chargen-ID vergeben werden, um doppelt vergebene Chargen-IDs zu vermeiden.

Außerdem wird in diesem Dialogfenster der Import des zugehörigen Logbuchs festgelegt.



System Updates und Migration 10

10.1 Allgemeine Vorgehensweise

Eine Aktualisierung der Systemsoftware an einer validierten Anlage muss unbedingt mit dem Betreiber abgestimmt bzw. von ihm initiiert sein. Es handelt sich um eine Systemänderung, die nach dem gültigen Änderungsverfahren zu planen und zu bearbeiten ist. Analog zu der Beschreibung im Kapitel "Betriebliche Änderungskontrolle (Seite 170)" bedeutet dies in etwa die folgenden Schritte:

- Beschreibung der geplanten Änderung
- Auswirkung auf Funktionen / Anlagenteile / Dokumentation, bei System-Updates z. B. unter Berücksichtigung der Systembeschreibung der neuen und geänderten Funktionen in Liesmich-Datei / Release-Notes
- Auswirkung auf Lesbarkeit und Verfügbarkeit archivierter Daten
- Bewertung der Risiken für den Gesamtprozess und den validierten Zustand
- Definition der durchzuführenden Tests zum Erhalt des validierten Zustandes auf Basis der Risikobewertung
- Genehmigung / Ablehnung der Änderung (gemäß definierter Verantwortlichkeiten)
- Aktualisierung der existierenden Systembeschreibung und Vorbereiten der Testdokumente
- Datensicherung vor Update durchführen
- Durchführung der Änderung (nach Freigabe der Anlage)
- Begleitende Dokumentation der durchgeführten Aktivitäten
- Durchführung und Dokumentation der erforderlichen Tests (Verifikation)
- Neue Datensicherung durchführen, eventuell mit System-Image

Bei der Betrachtung der möglichen Einflüsse auf die Applikation können z. B. relevant sein:

- Module und Bibliotheken, Typen und Instanzen
- Prozessbilder, Grafikeinstellungen, Objekte, skriptbasierte Dynamisierung
- Alarmsystem und Prozesswertarchivierung in Funktion und Darstellung
- Bedienberechtigungen
- Schnittstellen
- Auswirkungen beim Laden
- Performance des Systems
- Dokumentation (Spezifikation)
- Zu wiederholende bzw. neue Verifikationstests

10.2 Aktualisierung der Systemsoftware

Aktualisierungen der Systemsoftware können z. B. sein:

- SIMATIC PCS 7 Updates, Service Packs und neue Versionen
- Aktualisierungen von Standardsoftware wie z. B. Microsoft Office oder Virenscanner
- Betriebssystem Updates

Neben der Verbesserung von Sicherheitsaspekten und Fehlerbereinigungen kann dabei der Funktionsumfang erweitert bzw. verbessert werden.

Bei einer Aktualisierung der Systemsoftware kann es erforderlich sein, dass die Konfigurationsdaten des Projekts der älteren Version migriert oder konvertiert werden müssen, siehe dazu Kapitel "Migration der Applikationssoftware (Seite 176)".

Bei einem größeren Versionssprung ist es zudem möglich, dass zunächst auf eine Zwischenversion und erst danach auf die Zielversion hochgerüstet werden muss.

Siehe auch

- FAQ "Informationen zur PCS 7 Software-Aktualisierung", Online-Support unter Beitrags-ID 39980937 (https://support.industry.siemens.com/cs/ww/de/view/39980937)
- Handbuch "PCS 7 Kompendium Teil D", Kapitel 3, Online-Support unter Beitrags-ID 109808463 (https://support.industry.siemens.com/cs/ww/de/view/109808463)
- FAQ "Microsoft Sicherheits-Updates", Online-Support unter Beitrags-ID 18490004 (https://support.industry.siemens.com/cs/ww/de/view/18490004)
- GAMP 5-Leitfaden, Anhang S4 "Patch- und Aktualisierungs-Management"
- GAMP Good Practice Guide "IT Infrastructure" 2nd Edition, Kapitel 13

Hinweis

Unterstützung beim Software-Update und der Projektmigration leistet der SIMATIC Industry Support (http://support.industry.siemens.com).

10.3 Migration der Applikationssoftware

Über die Systemsoftware hinaus kann bei einer Aktualisierung wie oben bereits angedeutet auch die Applikationssoftware betroffen sein. Der Umfang kann hierbei von einer reinen Migration von Daten, Dateiformaten oder Speichermedien über die Migration von Datenbanken und Projektierungsdaten bis hin zu komplexen Systemmigrationen einschließlich Wechsel von Hardware und Betriebssystem reichen. Dabei versteht man unter Migration den Übergang zu einer technischen Nachfolgegeneration.

Siemens bietet **optimierte Migrationslösungen** für den Übergang zu SIMATIC PCS 7 an.

Die Anwender bisheriger Siemens-Leitsysteme wie auch fremder Leitsysteme können somit die Vorteile von Totally Integrated Automation für ihre Prozesse nutzen, siehe "Migration zu PCS 7" im Internet (http://w3.siemens.com/mcms/process-control-systems/de/simatic-pcs7-migration/Pages/simatic-pcs7-migration.aspx).

Auf Grundlage einer Systemanalyse, Risikoanalyse sowie der jeweiligen Rahmenbedingungen (vorhandene installierte Basis, vorgegebene Anlagenstillstandszeiten, etc.) wird eine individuell abgestimmte Migrations-Strategie unter Berücksichtigung der erforderlichen Qualifizierungsmaßnahmen konzipiert. Dabei sind auch die im Kapitel "Allgemeine Vorgehensweise (Seite 175)" beschriebenen Aktivitäten zur Systemaktualisierung zu berücksichtigen.

Das technische Verständnis der einzelnen Schritte, ob manuell oder automatisiert, sowie die Betrachtung möglicher Fehlerfälle sind die Grundvoraussetzung für eine erfolgreiche und effiziente Validierungsstrategie. Daher ist es besonders wichtig, die entsprechend kompetenten Fachkräfte in die Planung zu involvieren.

Siehe auch

- GAMP 5-Leitfaden, Anhang D7 "Datenmigration"
- GAMP Good Practice Guide "Operation of GxP Computerized Systems", Kapitel 17 "Datenmigration"

10.4 Validierungsaufwand bei der Migration

Systemaktualisierungen und Migrationen müssen geplant, kontrolliert und dokumentiert werden. Der Validierungsaufwand ist in Abstimmung mit dem Anlagenbetreiber festzulegen. Die technische Expertise kommt dabei aber in der Regel vom Systemlieferanten.

Je nach Umfang entstehen bei der Aktualisierung folgende Dokumente:

- Änderungsantrag des Betreibers,
  siehe Kapitel "Betriebliche Änderungskontrolle (Seite 170)"
- Migrationsplan bzw. Update-Plan
- Checkliste für die Installation / Migration
- Testspezifikation zur Sicherstellung der Funktionalität nach Aktualisierung
- Testergebnisse nebst Anhängen und Abweichungen
- Abschlussbericht

Prüfpunkte in der Verifizierung

Zur Verifizierung der durchgeführten Änderungen können in der Testspezifikation folgende Prüfpunkte relevant sein:

- Vorschriftsmäßige Installation der erforderlichen Software-Komponenten
- Neue oder geänderte Systemfunktionen dieser Version
- Grundlegenden Funktionalitäten des Systems, aus technischer und aus Anwendersicht
- GMP-kritische Funktionen und Parameter, Archivierung und Reports, auch die Rücklesbarkeit archivierter Daten

- Stichprobentests bei automatisierter Migration
  (Die vom System zur Verfügung gestellte Migrationsfunktionalität selbst ist eine Produkteigenschaft, die in der Projektanwendung nicht detailliert getestet werden muss.)
- Manuelle Anpassungen, die zusätzlich zur automatischen Migration durchgeführt werden, müssen separat beschrieben, ihre Durchführung dokumentiert und angemessen getestet werden.

Die Schritte gemäß Kapitel "Allgemeine Vorgehensweise (Seite 175)" sind zu berücksichtigen.

Hinweis

Faustregel: Je höher der manuelle Engineering-Aufwand bei einer Migration/Aktualisierung ist, umso höher ist auch der zugehörige Validierungsaufwand in der Vorbereitung, dem anschließenden Test und der Dokumentation.

Abkürzungen

A

Abkürzung	Beschreibung
AS	Automatisierungsstation
CFC	Continuous Function Chart (Funktionsplan)
CFR	Code of Federal Regulations (USA)
CM	Control Module (Einzelsteuereinheit)
CMT	Control Module Type
CSV	ein Dateiformat; aber auch verwendet für Computerized System Validation
DCS	Distributed Control System (Prozessleitsystem)
DS	Designspezifikation
EM	Equipment Module (Technische Einrichtung)
EMT	Equipment Module Type
EPH	Equipment Phase (Technische Funktion)
EPHT	Equipment Phase Type
ES	Engineering Station
FAQ	Frequently Asked Question
FAT	Factory Acceptance Test (Teil des Abnahmetests)
FDA	Food and Drug Administration
FS	Funktionsspezifikation
GAMP	Good Automated Manufacturing Practice
GMP	Good Manufacturing Practice (Gute Herstellpraxis)
HDS	Hardware Design Spezifikation
HMI	Human Machine Interface (Bediener-Schnittstelle)
IEA	Import-Export Assistent
IQ	Installation Qualification
OLE	Object Linking and Embedding
OPC	Open Platform Communications
OS	Operator Station (Bedienstation)
PAA	Plant Automation Accelerator
R&I	Rohr- und Instrumentierungsschema
SAT	Site Acceptance Test (Teil des Abnahmetests)
SDS	Software Designspezifikation
SFC	Sequential Function Chart (Ablaufsteuerung)
SMDS	Softwaremodul Designspezifikation
SMMC	SIMATIC Management Console
SOP	Standard Operating Procedure (Arbeitsanweisung)
SSC	SIMATIC Security Control
URS	User Requirements Specification (Kundenanforderungsspezifikation)
USV	Unterbrechungsfreie Stromversorgung

Abkürzung	Beschreibung
UTC	Universal Time Coordinated
VPN	Virtuelles privates Netzwerk
VXM	Version Cross Manager

Index

K

L

M

O

P

R

S

T

U

V

W

Z

Weitere Informationen

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

PDF (A5E42888172-AB)
Produced in Germany