Spezifikation
für ein
Prozessautomatisierungssystem

Inhalt

1 Einführung

1.1 Zweck

Diese Spezifikation legt die Anforderungen für ein Prozessautomatisierungssystem incl. zugehöriger Software und die zugehörigen Support-Dienstleistungen fest.

Feldgeräte sind nicht Gegenstand dieser Spezifikation.

1.2 Projektziele

Ziel ist die Installation eines Prozessautomatisierungssystems das eine hohe Verfügbarkeit, Zuverlässigkeit und Sicherheit aufweist und zudem kosteneffektiv ist. Mit dem System soll ein effektiver kontinuierlicher Anlagenbetrieb bei maximaler Produktion während seiner gesamten Lebensdauer möglich sein. Das System muss auf allen Ebenen robust und für diese industrielle Anwendung niedrige Komponentenausfallraten ausweisen.

Es muss anlagenweite Disziplinen unterstützen (kontinuierliche und diskrete Prozesse).

Das System muss sich nahtlos in die übrigen Systeme der Anlage integrieren lassen (Stromversorgungs-, Hilfs-, mechanisches, ziviles, Management-, Wartungssystem usw.) und insgesamt betrachtet die wirtschaftlichste Lösung bieten. Das System muss standardisierte Lösungen für die digitale Integration von Hilfssystemen wie Motor Control Center (MCC), Antrieben, Transmitter, Package Units, Wägesysteme usw. bieten.

Es muss skalierbar sein, was durch die Nutzung einer einzigen Plattform mit skalierbarer integrierter oder separater Failsafe Funktion einschließlich einer Safetymatrix für Engineering und Betrieb erreicht wird. Das System muss eine hohe Controller-Leistung und -Kapazität mit Hot Swappable-, Standard-, Remote-, Eigensicheren und SIL2/3-konformen Failsafeeingängen/-ausgängen (E/A), optionale Redundanz auf allen Ebenen einschließlich Ein- und Ausgängen sowie Teilnehmerredundanz bereitstellen.

Es muss über ein integriertes Sicherheitskonzept verfügen, das sich auf die gesamte Anlage, unternehmensweite und externe Intranet-/Internet-/Kommunikationssysteme erstreckt. Das Sicherheitskonzept soll als integriertes Konzept entwickelt werden und Hardware, Firmware und Anwendungssysteme über alle Lebenszyklusphasen des Prozessautomatisierungssystems hinweg abdecken.

Das Prozessautomatisierungssystem muss den in diesem Dokument aufgeführten internationalen technischen Normen und Vorschriften entsprechen.

Das System muss aufgrund seiner Bauweise und Standardisierung sicherstellen, dass die für die Projektausführung und die Implementierung vorgesehene Zeit eingehalten bzw. unterboten wird. Aufgrund der Verfügbarkeit fortschrittlicher Engineering-Tools muss das Prozessautomatisierungssystem-Engineering auf Basis einer Projektierung erfolgen, statt dafür einen speziellen Software-Code zu entwickeln.

Das System muss ein schnelles Engineering sowie eine schnelle und zuverlässige Inbetriebnahme und integrierte Funktionen wie Batch-, Material-Management-, Wegesteuerungs- und modellprädiktive Regelfunktionen bieten. Standardisierte, vollständig getestete Objekte (Funktionsbausteine und Bildbausteine) für Sensoren,

Motoren, Ventile in veröffentlichten Bibliotheken einschließlich spezieller Prozessgrafikvorlagen müssen verfügbar sein.

Das Assetmanagement muss die Überwachung großer Aggregate wie Pumpen, Motoren, Wärmetauschern usw. unterstützen.

Das System muss unter Berücksichtigung eines maximalen ergonomischen Bedienkomforts mit fortschrittlichen Alarm-Management-Technologien gestaltet werden, die die Reduzierung von Alarmen und der Arbeitsbelastung des Bedieners auf strukturierte und sichere Weise unterstützen. Intuitive Ansichten sollen zu einer besseren Lageerkennung und Entscheidungsfindung beitragen.

Das System muss zur konstanten und intensiven Nutzung der Anlageninformationen durch Produktionsexperten beitragen, sodass Bediener, Produktionsleiter, Wartungs- und Entwicklungstechniker, die allesamt auf dasselbe Ziel hinarbeiten, die besten Ergebnisse erzielen.

Als modernes System mit angemessenem Support zeichnet sich das Prozessautomatisierungssystem durch seinen bewährten Aufbau aus und verfügt zudem über eine umfassende Referenzliste mit etablierten und installierten Projekten. Das System muss für ähnliche Anwendungen in einer vergleichbaren Umgebung zuvor installiert worden sein. Das Prozessautomatisierungssystem muss von einem angesehenen Hersteller mit ausreichend Erfahrungen im jeweiligen Anwendungsgebiet stammen. Ein solider Support für den vorgesehenen Lebenszyklus der Anlage sowie für künftige Erweiterungen und Upgrades ist nachzuweisen.

Das System muss in erheblichem Maße zu betrieblichen Produktion-Spitzenleistungen (Operational Excellence), einem maximalen Durchsatz, zur Verfügbarkeit und Produktqualität beitragen und gleichzeitig Betriebs- und Wartungskosten, den Energie- und Rohstoffverbrauch, nicht spezifikationsgerechte Produkte, Emissionen und Sicherheitsrisiken minimieren.

Der Anbieter muss eine öffentlich zugängliche Preisliste für Hardware, System-Software und Anwendungspakete besitzen, die auch über ein unterstütztes Partnernetzwerk bezogen werden können. Erweiterungen, Änderungen bzw. Modifikationen müssen auch von geschulten und zertifizierten Fremdunternehmen vorgenommen werden können.

2 Allgemein

2.1 Für alle Lösungen

Das Prozessautomatisierungssystem soll als Prozessleitsystem (PLS) zur Steuerung, Überwachung und Verwaltung von Alarmen sowie zur Speicherung von Prozessdaten einschließlich der homogenen Integration von speicherprogrammierbaren Steuerungen und Sicherheitssystemen ausgelegt werden.

Hardware und Software müssen weitgehend skalierbar sein, um die breitgefächerten Anforderungen zu erfüllen.

Das System muss auf Grundlage verschiedener Protokolle mit anderen Systemen kommunizieren und eine nahtlose horizontale und vertikale Integration ermöglichen.

Das System soll eine Client-Server Architektur bereitstellen.

Das System muss eine gemeinsame Hardware und Entwicklungswerkzeuge für unterschiedliche Lösungen bereitstellen.

Das System muss für PLS-, Sicherheits- und SPS-(speicherprogrammierbare Steuerungen)-Anwendungen entworfen sein und auch Hochgeschwindigkeitsanforderungen erfüllen können.

Das System muss integrierte Fehlersicherheit (Failsafe) in Runtime und Engineering anbieten.

Das System muss Änderbarkeit im laufenden Betrieb unterstützen.

Das System muss Feldbusgeräte beliebiger Hersteller ohne zusätzliche Zertifizierung unterstützen.

Das Anbietersystem muss ein eigenes leistungsfähiges ABK-(HMI, Human Machine Interface)-Produkt enthalten, das Besitz des Anbieters ist und von diesem entwickelt, hergestellt und getestet wurde.

Das Anbietersystem muss bei Bedarf auch eine Trennung zwischen Terminal- und Systembus unterstützen.

Das Anbietersystem muss im Feldbusbetrieb mittels PROFINET als minimal Anforderung die Systemredundanz als auch Medienredundanz unterstützen.

Die Controller des Systems müssen lüfterlosen Betrieb ermöglichen.

2.2 Kombination von PLS, SPS, Chargen- und Sicherheitssystem

Das Prozessautomatisierungssystem muss Funktionen aufweisen, die bisher sowohl mit einer speicherprogrammierbaren Steuerung als auch mit einem verteilten I/O Steuerungssystem (DCS) in Verbindung gebracht werden, z.B. Automatisierung von kontinuierlichen und komplexen Prozessen, hoch entwickelte Operator-Funktionen und skalierbare Redundanz auf allen Ebenen.
Alle Funktionen müssen ohne Verwendung besonderer Gateways oder Schnittstellen nahtlos in einer einheitlichen Automatisierungslösung bereitgestellt werden.
Darüber hinaus muss das System die nahtlose Integration von kontinuierlicher Steuerung, Chargensteuerung und Sicherheitsschutzsteuerung einschließlich einheitlicher Software-Tools vorsehen.

2.3 Horizontale Integration

Das System muss neben Prozessleitaufgaben auch vorgeschaltete (Upstream) und nachgeschaltete (Downstream) diskrete Steuer- und Regelaufgaben wie z.B. Handling und Verpackung von Rohmaterialien integrieren. Darüber hinaus muss das System auch die wirtschaftliche anlagenweite Integration aller Betriebsvorgänge in jeder Fertigungs- und Prozessumgebung unterstützen.

2.4 Vertikale Integration

Das System muss die vertikale Integration durch Verwendung einheitlicher Datenkommunikationsstrukturen für die vollständige Integration ab der Enterprise Resource Planning (ERP)-, Manufacturing Execution Systems (MES)-, Controller- und Feldebene unterstützen.

2.5 Offene Systeme

Das System muss auf unterstützten offenen/herkömmlichen kommerziellen Systemen und Technologien basieren, einschließlich u.a. Personalcomputer-(PC)-Plattformen mit Microsoft Windows-Betriebssystem, Ethernet-Kommunikation, TCP/IP, OPC für die Verbindung verschiedener Systeme verschiedener Anbieter, feldmontierbarem Leitsystem, Remote-I/O-Subsystemen und busgestützte Kommunikation mit Feldgeräten über PROFIBUS DP/PA-,PROFINET, Foundation Fieldbus H1-, HART-, AS-I- und Modbus-Netzen.

2.6 Dezentralisierte Architektur

Das System muss eine dezentrale flache und Client/Server-Architektur mit umfassender Skalierbarkeit aufweisen. Es muss erweiterungsfähig sein und bis zu zwanzig Engineering-Workstations, 40 Operator-Bildschirmstationen – jede Station mit Zugriff auf die gesamte Anlage –, achtzehn redundante Server und 128.000 PLT-Stellen unterstützen.

2.7 Skalierbarkeit

Das System muss ohne die Bereitstellung von Reservekapazitäten von hundert bis hunderttausend I/Os skalierbar sein. Es muss ein abgestuftes Sortiment an Controllern verfügbar sein, die eine skalierbare Leistung für verschiedene Prozess-Anforderungen bereitstellen.

Controller und I/O müssen austauschbar sein und den Tausch von Controllern zur Erfüllung von Performance-Anforderungen ermöglichen.

Die Skalierbarkeit des Systems muss sowohl Software-Lizenzierung als auch Hardware-Konfigurierung beinhalten.

Die Funktionalität des Systems muss skalierbar sein und die Erfüllung von wechselnden Anforderungen ohne den Tausch von Controllern ermöglichen:

- Kommunikationsanforderungen (z.B. Telecontrol)
- Operator Interfacing (z.B. Lokale Display-Units-)
- Integration von neuen Datensets (z.B. Asset Management oder Power Control Systeme)

2.8 Redundanz

Das System muss zur Gewährleistung hoher Verfügbarkeit optionale Redundanz auf allen Ebenen bieten. Operator-Stationen, Server (einschließlich Chargensteuerung), Historian, Terminal- und Systembus, Controller, Feldbusse und Eingabe-/Ausgabebaugruppen oder Kanäle müssen bei Bedarf redundant auslegbar sein. Redundanz ist durch die ereignisgesteuerte Synchronisation zu erreichen, die im Störfall eine schnelle und stoßfreie Umschaltung zur Zentraleinheit (CPU) gewährleistet.

Ein einzelner Fehler irgendwo im System darf keinen Ausfall der Regelung bei mehr Regelkreisen als denjenigen nach sich ziehen, bei dem der Fehler aufgetreten ist. Der Ausfall eines einzelnen Geräts darf sich nicht auf die Fähigkeit des Systems auswirken, mit anderen Geräten im System zu kommunizieren. Die Umschaltung im redundanten Fall darf keine Systemfunktionen unterbrechen.

Redundante Geräte und Software müssen kontinuierlich auf Fehler überwacht werden. Alle Baugruppen müssen online diagnostiziert werden. Fehler müssen mit Fehlermeldungen angezeigt werden, die kennzeichnen, welche Baugruppe gestört ist.

Zur Maximierung der Datenverfügbarkeit und -integrität muss die OS die Möglichkeit der Konfigurierung von Systemredundanz bieten. Diese darf die Nutzung der Client/Server-Konfiguration und/oder Architektur in keiner Weise begrenzen oder beschränken.

Clients müssen im Fehlerfall automatisch auf den Reserve- oder redundanten Server umschalten. Dieser Vorgang darf keine Anwendungsprogrammierung oder Rekonfiguration erfordern.

Systemredundanz muss auf *"Server-by-Server"*-Basis bis zu einem Profil von maximal achtzehn redundanten Servern konfigurierbar sein.

Client-Stationen müssen die Festlegung verschiedener primärer Server unterstützen, sodass es möglich ist, die Netzbelastung zu verteilen und sicherzustellen, dass im Fehlerfall nicht für alle Clients eine Umschaltung erfolgt.

Sobald ein gestörter Server wieder verfügbar wird, muss der aktive Server fehlende Daten auf dem ausgefallenen Server prüfen und wiederherstellen. Die Datenwiederherstellung muss im Hintergrund ablaufen und darf den Betrieb des Online-Servers nicht beeinträchtigen.

Die Redundanz muss auf allen Ebenen (Feld-E/A, Controller, Kommunikation, Server und Operator) flexibel gemäß den Anforderungen konfiguriert werden. Die physikalische Trennung redundanter Paare muss möglich sein.

Redundante Feldbusarchitektur erlaubt Mehrfachfehler ohne Unterbrechung. Es sollte zur Erhöhung der Verfügbarkeit ein ringförmiger Feldbus eingesetzt werden können.

Die I/O-Redundanz ist nicht abhängig von der CPU-Redundanz.

Es muss möglich sein, zwei PLT-Stellen unter derselben Bezeichnung anzulegen und integrierte Redundanzfunktionalitäten anzuwenden (ohne Neuprogrammierung). Ferner muss es möglich sein, redundante PLT-Stellen an verschiedene I/O-Racks anzuschließen.

2.9 Verfügbarkeit

Das System muss eine hohe Ausfallsicherheit der Geräte gewährleisten. Die hohe Ausfallsicherheit muss basierend auf praxiserprobten Designs und unter ähnlichen Umgebungsbedingungen nachweisbar sein. Die Mean Time Between Failure (MTBF) von Geräten muss verfügbar sein.

Die Ausfallsicherheit muss nachweisbar sein für:

- Hardware-, Firmware- und Software-Komponenten (Controller, Server, etc.)
- Kommunikationskomponenten
- I/O
- Peripherie (Operator Systeme, Bedienelemente)
- Hilfskomponenten (System-Uhr, etc.)

Um Abnormal Shutdown Time (AST) zu reduzieren, müssen Instandhaltungsarbeiten auf dem einfachen Austausch von defekten Geräten, die vom System selbst als defekt erkannt werden, beruhen. Das System muss eine nachweisbar niedrige Mean Repair Time besitzen (entsprechend AST). Umfangreiche Selbst-Diagnose-Einrichtungen müssen die Identifizierung von fehlerhaften Geräten und einfache Alarme an den Operator unterstützen.

Das System muss zertifiziert sein und relevante Sicherheitsanforderungen und die anwendbaren nationalen und internationalen Standards erfüllen:

- IEC 61508 (bis SIL 3) Funktionale Sicherheit in der Industrie
- IEC 61511 7 ANSI / ISA-84 für die Prozessindustrie
- IEC 62061 / IEC 60204-1 / ISO 13849-1 für die Maschinenindustrie

Das Design von Prozessleitsystemen muss so beschaffen sein, dass der Ausfall einer Komponente des Systems minimale Auswirkungen auf den Prozess hat. Die Komponenten müssen eine nachweisbar hohe Integrität besitzen, sowie robust und physikalisch kompakt sein.

Das Prozessleitsystem muss mithilfe einer eingebauten Redundanz sowohl für Hardware als auch für Software für eine 99,99 (bis 99,9999) prozentige Verfügbarkeit geeignet sein. Dies muss redundante Prozessoren, redundante I/O Cards, redundante Daten-Highways und eine redundante Stromversorgung mit automatischem Wechsel zur spannungsführenden Standby-Einheit bei Erkennung eines Defekts oder Ausfalls der aktiven Einheit beinhalten. Jeder Controller in einer redundanten Konfiguration muss mit beiden Daten-Highways kommunizieren.

Verfügbarkeit wird wie folgt definiert:

$$\%\ \text{Verfügbarkeit} = \frac{100 \times \text{MTBF}}{\text{MTBF} + \text{MTTR}} \quad \text{oder} \quad \frac{100 \times (\text{OPT} - \text{AST})}{\text{OPT}}$$

Wobei:

OPT = Operating Period Time (h) (Beinhaltet shutdown Zeit)

AST = Abnormal Shutdown Time (h)

2.10 Online-Änderungen

Das System muss die Möglichkeit bieten, folgende Änderungen online ohne Betriebsunterbrechung vorzunehmen:

- Ändern der Parameter eines E/A-Kanals
- Hinzufügen oder Entfernen einer E/A-Baugruppe
- Hinzufügen oder Entfernen eines E/A-Baugruppenträgers
- Hinzufügen oder Entfernen eines PROFIBUS-DP-Slave
- Hinzufügen oder Entfernen eines PROFIBUS-PA-Feldgeräts
- Hinzufügen neuer Verbindungen zu Industrial-Ethernet-Netzen
- Ändern des Bereichs eines analogen Punkts
- Ändern einer Prozessgrafik
- Hinzufügen einer neuen Variable zur Archivdatenbank

Hinzufügen eines neuen Regelkreises zur Projektierung

2.11 Lizenzierung

Software-Lizenzen für Engineering-Workstations und für Operator-Schnittstellenkonsolen müssen unabhängig von der Art und Kombination der verwendeten Eingänge/Ausgänge (analog vs. diskret, Eingabe vs. Ausgabe) sein.

Die Software-Lizenzen (für den Betrieb wie auch für das Engineering) müssen portierbar sein und dem Benutzer die Übertragung von Lizenzen zwischen unterschiedlichen PCs ohne Zuhilfenahme des Anbieters ermöglichen.

Lizenzmodell

Der Anbieter muss ein überschaubares, fein abgestuftes Lizenzmodell anbieten.

Der Anbieter muss ein Lizenzverfahren anbieten, das sich an der Anzahl von Prozessobjekten (PO) für die Operator-Station (OS) und Controller in der Lösung orientiert.

Das Engineering-System muss die verwendeten Lizenzen und die Reservekapazität zeigen.

2.12 Verwendung von Standardprodukten

Das System muss aus der standardisierten Hardware, System-Software und Firmware des Herstellers bestehen, die entsprechend den angegebenen Anforderungen konfiguriert werden können und für die der Hersteller einen langfristigen Support bieten und Qualität garantieren. Die vom Anbieter standardisierte Software oder Firmware darf nicht eigens modifiziert werden, um die Anforderungen des Benutzers zu erfüllen.

Die Anwendungs-Software muss anhand des standardmäßigen Prozessautomatisierungssystems implementiert werden, ohne dass dafür eine Änderung der System-Software oder der Betriebssysteme erforderlich ist.

Der ursprüngliche Hersteller der im Angebot genannten jeweiligen Komponententypen ist aufzuführen.

2.13 Reservekapazität und Erweiterung

Das System muss mit XX% Reservekapazität für jeden E/A-Typ im Basissystem bereitgestellt werden. Als Basissystem wird die Hardware-Menge definiert, die zur Erfüllung der Projektanforderungen benötigt wird.

Kommunikationsnetze müssen so ausgelegt sein, dass ein Systemwachstum von mindestens XX% auf Grundlage der Anzahl nicht genutzter Knotenadressen möglich ist. Die Systemerweiterung muss ohne Abschaltung der Controller möglich sein, die nicht direkt von der Erweiterung betroffen sind.

System-Runtime- und Engineering-Software muss durch den Erwerb zusätzlicher Lizenzierungseinheiten erweitert werden können.

2.14 Spezielle Anwendungen

PC-basierte Controller müssen für spezielle Anwendungen (z.B. für Package Units, Laborautomatisierung, weit verbreitete Automatisierungsaufgaben) verfügbar sein. Der Controller muss ein Windows-Betriebssystem mit Echtzeiterweiterungen (RTX, Real Time Extensions) bieten. Es muss die Möglichkeit bestehen, viele Controller für größere Anwendungen zu vernetzen und zu integrieren.

Der Controller muss gemäß dem Prozessautomatisierungssystem ohne Lüfter oder sonstige rotierende Komponenten aufgebaut sein und denselben Konstruktionstemperaturen und Vibrationsstandards entsprechen, wie sie für einen 24-stündigen kontinuierlichen Betrieb in einer industriellen Umgebung infrage kommen. Der Controller muss die E/A-Baugruppen eines Standard-Prozessautomatisierungssystems nutzen.

Der Controller muss sich in das Prozessautomatisierungssystem integrieren lassen, das mit Ethernet PROFIBUS- und PROFINET-Schnittstellen sowie mit Standard-USB-Schnittstellen für die lokale Anbindung von Peripheriegeräten ausgestattet ist.

Der Controller muss für den unabhängigen Standalone-Betrieb (z.B. Tanklager, Anwendungen der Wasserversorgungsbranche mit dezentralen Automatisierungsaufgaben) geeignet sein oder sich vollständig in das Prozessautomatisierungssystem integrieren lassen (wie es z.B. bei Package Units üblich ist).

3 Umgebungsbedingungen

3.1 Installation in Innenräumen

Geräte, die in Räumen installiert werden, müssen für den Betrieb unter den folgenden Umgebungsbedingungen ausgelegt sein:

- Temperaturbereich: 0 °C bis 50 °C[1]
- Relative Feuchtigkeit: 5% bis 95%

3.2 Außenumgebung

Geräte, die im Außenbereich installiert werden, müssen für den Betrieb unter den folgenden Umgebungsbedingungen ausgelegt sein:

- Temperaturbereich: -40 °C bis 70 °C[2] (keine direkte Sonneneinstrahlung)
- Relative Feuchtigkeit: 5% bis 95

3.3 Umgebungsbedingungen für Komponentenaufbau

Komponenten, die in Bedieneinheiten installiert werden, müssen für den Betrieb unter den folgenden Bedingungen ausgelegt sein:

CPUs

- Temperaturbereich: 0 °C bis +70 °C[3]
- Conformal Coating industrial standards (ISA-S71.04 severity level G1; G2; G3)
- Relative Feuchte 0% bis 95% (ohne Kondensation)

Stromversorgungseinheit (PSU, Power Supply Unit)

- Temperaturbereich: 0 °C bis +70 °C[4]
- Conformal Coating industrial standards (ISA-S71.04 severity level G1; G2; G3)
- Relative Feuchte 0% bis 95% (ohne Kondensation)

Peripheriegeräte

- Temperaturbereich: -40 °C bis +70 °C[5]
- Conformal Coating industrial standards (ISA-S71.04 severity level G1; G2; G3)
- Relative Feuchte 5% bis 95% (ohne Kondensation)

Netzwerkgeräte

[1] An Anforderungen anzupassen
[2] An Anforderungen anzupassen
[3] An Anforderungen anzupassen
[4] An Anforderungen anzupassen
[5] An Anforderungen anzupassen

- Temperaturbereich: -40 °C bis +70 °C[6]
- Relative Feuchte 0% bis 95% (ohne Kondensation)

IPC Server/Clients

- Temperaturbereich: +5 °C bis 50 °C[7] geprüft nach IEC 60068-2-2, IEC 60068-2-1, IEC 60068-2-14
- Relative Feuchtigkeit: 5% bis 95% (ohne Kondensation)

Der Komponentenaufbau muss eine Projektierung von Steuereinrichtungen ohne Lüfter oder Klimatisierung ermöglichen.

3.4 Anforderungen für explosionsgefährdete Bereiche

Geräte in explosionsgefährdeten Bereichen müssen gemäß der ATEX-Richtlinie 99/92/EG über explosive Atmosphären und dem National Electric Code NFPA 70 Artikel 500/505 ausgelegt und installiert werden.

Elektroräume und Leitstände, sowie Prozessbereiche im Allgemeinen, werden als sichere Bereiche eingestuft, sofern diese nicht in einen speziellen Gefahrenbereich eingeordnet sind.

3.5 Lagerumgebung

Es muss möglich sein, die Geräte vor der Installation bis zu 6 Monate unter folgenden Bedingungen zu lagern:

- Die Geräte müssen in feuchtigkeitsbeständige Behälter verpackt werden.
- Lagertemperatur: -40 °C bis 70 °C (keine direkte Sonneneinstrahlung)
- Relative Feuchtigkeit (außerhalb des feuchtigkeitsbeständigen Behälters): 5% bis 95%

3.6 Geräteschutz[8]

Der Schutzgrad elektrischer Umhüllungen und Einrichtungen gegen Staub und Eindringen von Wasser muss der Norm IEC 60529 entsprechen:

- Leitstände IP20
- Prozessbereiche IP54
- Außenbereiche (natürlich belüftete und Wash-Down-Bereiche) IP55

[6] An Anforderungen anzupassen

[7] An Anforderungen anzupassen[7]

[8] Gemäß Anforderungen anzupassen

4 Elektrische Anforderungen

4.1 Spannungsversorgung des Systems

Die Spannungsversorgung ist wie folgt auszulegen:

- Spannung: 100/110/120/230/240 V AC oder 5/24/48/60 V DC
- Frequenz: 50/60 Hz

4.2 Elektromagnetische Verträglichkeit

Die Geräte müssen alle Vorschriften zur Elektromagnetischen Verträglichkeit entsprechend den IEC-Normen 61000-4-2, 61000-4-3 und 61000-4-4 erfüllen.

4.3 Verdrahtung und Verkabelung

PROFIBUS-, Industrial Ethernet- und andere Kommunikationskabel müssen in mindestens 75 mm Abstand von Wechselstromkabeln geführt werden. Lichtwellenleiterkabel sind von dieser Bestimmung ausgeschlossen.

Der Anbieter muss die Kabel so installieren, dass die für die Wartung problemlos abgenommen werden können. Kabel dürfen zu keinem Hindernis werden bei der Entfernung von Leiterplatten.

Steckverbindungen und Baugruppen müssen mechanisch so verlegt werden, dass es beim Einstecken oder einer Verbindungsherstellung nicht zu Kurzschlüssen oder einer falschen Polarität kommt.

4.4 Erdung von Schränken und Arbeitsplätzen

Die Wechselstrom-Schutzerdung und die Erdung von Instrumentenschaltungen (Instrumentation Circuit Ground) müssen der IEC 61131-2 (oder NEC, Artikel 250) entsprechen.

4.5 Leiterplatten

Der Austausch einer Steuerbaugruppe oder einer Eingabe-/Ausgabebaugruppe muss ohne Entfernung der Leistungs- oder Feldverdrahtung möglich sein.

5 Controller

5.1 Mehrzweck-Controller

Erforderlich ist eine Mehrzwecksteuerung bzw. ein Mehrzweck-Controller, der schnelle Programme des SPS-Typs (diskret) wie auch Anwendungen des DCS-Typs (Regelung) ausführen kann und die Integration von Prozess- und Maschinensteuerung in einem Gerät ermöglicht. Es müssen sowohl extrem kurze Anweisungsverarbeitungszeiten bis zu 10 ms, die für die speicherprogrammierbare Steuerung erforderlich sind, als auch langsamere Verarbeitungszeiten, die für die Prozesssteuerung benötigt werden, verfügbar sein. Mindestens 9 unabhängige Anwendungszyklusraten müssen angeboten werden, um die Ausführungszeit eines Anwendungsprogrammes optimieren zu können.

Der Controller muss alle im Kapitel 7 „Feldbus“ erwähnten Anbindungen und Anforderungen/Normen unterstützen.

In Bezug auf die PROFINET-Normen muss der Controller die Medienredundanz (MRP) unterstützen.

5.2 Hochleistungs-Controller

Der Controller muss mindestens 1000 Standard-PID-Regelkreise mit einer Zykluszeit von 500 ms ausführen können, um die Notwendigkeit einer Verteilung des Benutzer-Anwendungsprogramms zu verringern.

Ein Controller der oberen Leistungsklasse muss folgende Leistungsdaten bieten:

Ausführungszeiten für die Anweisungsverarbeitung: 18 ns

Arbeitsspeicher: 30 MB

Es muss die Möglichkeit bestehen, Controller mit E/A von 100 bis 4.000 Punkten zu konfigurieren.

Ein Kaltstart muss auch ohne Engineering-Workstation möglich sein.

Das Prozessautomatisierungssystem muss ermöglichen, dass Anwendungsprogramme dokumentiert und kommentiert werden, ohne Einbuße der CPU-Leistung oder des Controller-Arbeitsspeichers.

Der Controller muss über PROFIBUS-Anschlüsse und mindestens zwei PROFINET-Anschlüsse verfügen. Der Betrieb von 500 PROFINET Geräten an einem Controller muss gewährleistet sein.

5.3 Redundante Controller

Für Anwendungen mit hoher Verfügbarkeit muss folgendes vorhanden sein: Redundante Controller, - Stromversorgungen, - Ethernet-Verbindungen, - Baugruppenträger (Racks), - PROFIBUS- und - PROFINET-Netze.

In Bezug auf die PROFINET-Norm muss der redundante Controller, die Systemredundanz S2 und redundante PROFINET Konfiguration R1 unterstützen.

Redundante Controller müssen die Änderbarkeit im laufenden Betrieb unter-stützen.

Bei redundanten Systemen im laufenden Betrieb müssen Firmware-Updates möglich sein.

Physikalische Trennung redundanter Controller

Bei Bedarf muss die Möglichkeit bestehen, redundante Controller in separaten Bedieneinheiten/Räumen/Gebäuden unterzubringen, um das Gefahrenpotenzial zu mindern, das aufgrund von Mehrfachausfällen (z.B. Brände) besteht.. Eine räumliche Trennung von >1.000 m ist erforderlich.

Umschaltzeit bei redundanten Systemen

Bei einem redundanten System müssen Controller mit "Hot Backups" arbeiten, wobei beide CPUs parallel den gleichen Schritt des Anwenderprogramms ausführen. Wird ein CPU-Fehler festgestellt, muss eine stoßfreie Umschaltung zwischen den Controllern initiiert werden. Die komplette Umschaltung muss in max. 10 ms einschließlich aller E/As und ohne Verlust von Alarmen oder Meldungen abgeschlossen sein.

Angeschlossene redundante I/O-Komponenten müssen im Fehlerfall innerhalb von 20 ms umschalten können.

5.4 Komponenten für die Spannungsversorgung

Spannungsversorgung

Es müssen Stromversorgungen mit 24 V DC oder mit 60/80/110/120/230 V AC 50/60 Hz zur Auswahl stehen.

Batteriepufferung

Der Projektierungsspeicher der Controller muss über eine Reservebatterie verfügen, damit der Controller bei einem längeren Stromausfall seine Projektierungs- und Statusinformationen beibehält. Die Programmausführung muss nach Wiederherstellung der Stromversorgung in einem vorher festgelegten sicheren Zustand fortgeführt werden.

5.5 Auswahl von Projektierungssprachen

Projektierungssprachen müssen angeboten werden, die herkömmlicherweise sowohl mit einer SPS- als auch mit einer DCS-Programmierumgebung in Verbindung gebracht werden. Das System muss Grafik- und Textprogrammiersprachen gemäß IEC 61131-3 unterstützen.

- Anweisungsliste (AWL)
- Strukturierter Text (ST)
- Funktionsplan (FUP)
- Kontaktplan (KOP)
- Sequential Function Charts (SFC)

Überdies muss das System die Industriesprache Continuous Function Charts (CFC) und die Konfiguration einer Ursache-Wirkung-Sicherheitsmatrix nach ISO 10418 für Sicherheitsanwendungen unterstützen.

5.6 Regelung

Standard-Software-Algorithmen müssen für die Ausführung von Regelungsfunktionen (Regulatory Control) verfügbar sein, und diese müssen einfach projektierbare Parameter aufweisen.

5.7 Betriebsarten eines Regelkreises

Es muss möglich sein, jeden einzelnen Regelkreis in einen manuellen, automatischen oder Kaskadenmodus zu setzen. Bei einer Kaskade muss es möglich sein, fernbetätigte Führungsgrößen (Sollwerte) von anderen Reglern oder Steuerbausteinen aus einzustellen.

Die Umschaltung zwischen allen Betriebsarten eines Controllers muss stoßfrei und ohne Ausgleich mit Windup-Schutz durchgeführt werden.

Regler müssen in der Lage sein, aufgrund von externen oder internen logischen Inputs die Betriebsart automatisch zu wechseln.

5.8 Berechnungen

Algorithmen müssen berechnet werden auf Basis von Gleitkommazahlen mit physikalischer Einheit oder entsprechenden anderen gleichwertigen Methoden, die keine Skalierung erfordern.

Eingabefunktionen

Die folgenden Eingabefunktionen müssen als Standardfunktionen bereitgestellt werden:

- Ziehen der Quadratwurzel zur Durchflussmessung
- Linearisierung von Thermoelementen Typ B, E, N, J, K, L, R, S, T und U
- Linearisierung von Widerstandsthermometern (RTDs)
- Impulssummierung eines digitalen Eingangs
- Umsetzung Impulseingang auf Frequenz

Rechenfunktionen

Die folgenden Rechenfunktionen müssen als Standardkonfiguration oder einfache algebraische Anweisungen bereitgestellt werden.

- Addition/Subtraktion
- Hochlaufgeber
- Lead-Lag
- Integrator/Akkumulator
- Totzeit
- Hoch/Tief-Auswahl
- Multiplikation/Division
- Zeitmittelung

- Signalwahlschalter
- Exponentielles Polynom
- Logarithmen
- Quadratwurzel
- Absolutwert
- Einschaltverzögerung
- Min./Max.-Auswahl
- Glättungsfunktion
- Rauschsignalgenerator
- Tiefpassfilter zur Signalglättung
- Alarmverzögerung

Kontinuierliche Regelungsfunktionen

Die folgenden Regelungsfunktionen müssen projektierbar sein:

- PID
- Auto/manuell mit Bias-Regelung
- Verhältnisregelung
- Schrittregler
- Regler mit Bereichsaufspaltung (Split Range)
- Kaskadenregelung
- Übersteuerung (Override)
- PID mit Vorwärtsregelung
- PID mit Smith-Prädiktor
- PID mit Überwachung der Sicherheitslogik und Regelkreisgüte
- PID mit Reglerparameteranpassung
- Modellprädiktiver Regler
- Selbsteinstellende Regelung (optional)
- Fuzzy-Logik-Regelung (optional)
- Mehrgrößenregelung (optional)

Frequenz der Regelkreisausführung (Zykluszeit)

Es muss möglich sein, die Ausführungsfrequenz jeder Geräteregelungsstrategie im Controller unabhängig auszuwählen. Der Controller muss mit einer Geschwindigkeit von 100-mal pro Sekunde (10 ms) Aufgaben verarbeiten und E/A scannen.

Regelkreis-Ausgabefunktionen

Die folgenden Ausgabefunktionen müssen als Standardfunktionen bereitgestellt werden und unabhängig von der Ausführung in der Systemsteuerung gleich sein:

- Linear
- Linear mit Klemmung (oben und unten begrenzt)
- Nichtlineare Charakteristik

Sollwertklemmen

Obere und untere Klemmen für alle Sollwerte (Setpoint Clamps) müssen projektierbar sein.

5.9 Diskrete Regelung

Die folgenden diskreten Funktionen müssen als Standardfunktionen bereitgestellt werden:

- Logikfunktionen: and, or, not, nand, nor, xor
- Erkennung von Zustandsänderungen
- Setzen/Rücksetzen von Flipflops
- Zeitgeber und Zähler
- Vergleichselemente: größer als, kleiner als, gleich, ungleich
- Multiplexer (wählt eines von max. 16 Signalen aus)
- Flankentrigger positiv, negativ, bidirektional

Das Anbietersystem muss umfangreiche technologische Baugruppen (Regler, Positionierbaugruppen, Zähler usw.) unterstützen können.

5.10 Ablaufsteuerung

Sequential Function Charts (SFC) müssen verfügbar sein. SFC ist eine strukturierte höhere Steuerungsprogrammiersprache gemäß IEC 61131-3.

SFC muss unter anderem die folgenden Merkmale aufweisen:

- Bereitstellung der notwendigen Einrichtungen für die Echtzeitsteuerung sequentieller Prozesse.
- Zugriff auf Prozesssteuerungs- und andere Datenbankinformationen.
- Möglichkeit der Änderung der Programmlogik, während andere Ablaufketten aktiv sind.
- Unterstützung der Ausführung des Funktionsplans in manueller oder automatischer Betriebsart.
- Möglichkeit der Projektierung mehrerer Fahrweisen und/oder Zustandslogiken in einem einzigen SFC-Container. Dies ermöglicht die effektive Koordinierung von Ablaufketten, die mehr als eine Fahrweise aufweisen (z.B. Heizen und Kühlen) oder die Safe-State-Logik enthalten (z.B. Aborting- oder Holding-Logik).
- Möglichkeit der Erstellung von Master-SFC-Elementen, die kopiert und in einer Projektierung wie Funktionsbausteine verwendet werden können. Änderungen des SFC haben automatische Aktualisierungen aller anderen Instanzen in der Projektierung für den Controller zur Folge.

- Automatische Erstellung der Anzeigen für die Visualisierung und Steuerung des SFC direkt aus der Projektierung des Controllers.
- Der SFC-Editor muss einen Test-/Debug-Modus enthalten, der nicht auf die Ausgänge schreibt.
- Namensänderungen in Plänen und deren Referenzen müssen automatisch angepasst werden, nicht manuell. Ablaufsteuerung in OS: Die Schrittkette des Anbietersystems gestattet Bedienereingriffe bei Prozessstörungen und muss beobachtet werden können.
- Aktionsmöglichkeit in Schrittübergängen muss möglich sein.
- Bei mehreren überlagerten SFCs, die dieselben unterlagerten SFCs nutzen, hat die Zuweisung und Verwaltung systemseitig zu erfolgen.

Funktionen für Schrittketten

Folgende Standardfunktionen müssen bereitgestellt werden:

- Ablauf anhalten – manuell oder zu festgesetzter Zeit
- Rücksprung zu früherem Schritt
- Überspringen von einem oder mehreren Schritten
- Automatischer Neustart nach vollständigem Ablauf (zyklischer Betrieb)
- Projektierung maximaler oder minimaler Ausführungszeiten der Schritte
- Möglichkeit der Projektierung einer optionalen Operator-Bestätigung für jeden einzelnen Transitionszustand

Betriebsarten

Auf welche Art der Funktionsplan von einem Transitionszustand zum nächsten Schritt übergeht, kann entsprechend den folgenden Betriebsarten gesteuert werden:

- Transition: Steuerung wird allein durch Erfüllung der Transitionsbedingung bestimmt
- Bestätigung: Steuerung wird allein durch Operator-Bestätigung bestimmt
- Transition und Bestätigung: Ablaufkette wird erst fortgesetzt, wenn die Transitionsbedingung erfüllt ist und die Operator-Bestätigung eingegeben wurde
- Transition oder Bestätigung: Ablaufkette wird fortgesetzt, wenn die Transitionsbedingung erfüllt ist oder wenn die Operator-Bestätigung eingegeben wurde

Phasen eines Schritts

Jeder Schritt eines sequentiellen Funktionsplans muss die folgenden Standardphasen der Schrittausführung unterstützen:

- Initialisierung: für die erstmalige Ausführung von Aktionen
- Ausführung: für die kontinuierliche Ausführung von Aktionen, bis die Transitionsbedingung erfüllt ist
- Terminierung: für die Nachbearbeitung (Postprocessing), um die einmalige Ausführung einer Aktion nach Erfüllung der Transitionsbedingung zu ermöglichen

Unterstützte Betriebszustände

Die folgenden 16 SFC-Betriebszustände (gemäß Standard S88) müssen durch das System unterstützt werden:

- Ready
- Starting
- Active
- Completing
- Error (Completing)
- Completed
- Holding
- Held
- Resuming
- Error
- Held (Error)
- Resuming (Error)
- Aborting
- Aborted
- Stopping
- Stopped

5.11 Überwachungssteuerung (Supervisory Control)

Die Überwachungsfunktionen des Prozessautomatisierungssystems müssen in die Controller-Funktionen vollständig integriert sein. Bei ausgewählten Kreisen müssen die Überwachungssteuerungsfunktionen auch die Möglichkeit der Sollwertanpassung bieten.

Überwachungssteuerungsanwendungen müssen nach Zeitplan, auf Anforderung oder ereignisgesteuert ausgeführt werden können.

Das Überwachungssystem muss Zugriff haben auf die vollständige Datenbank mit Berechtigungen für die Änderung von Objekten wie Steuerungsbetriebsart und Sollwert.

5.12 Autotuning

Eine integrierte PID-Autotuning-Funktion muss von der Engineering-Station aus verfügbar sein.

- Anwendbar auf Prozesse mit langsamer und schneller Dynamik
- Nutzung in Verbindung mit selbstregelnden und integrierenden Prozessen
- Festigkeit gegen Störspannungen und Prozesslaststörungen
- Mögliche Anwendung auf Standardbibliotheken und angepasste Bibliotheken
- Möglichkeit des Zugriffs direkt von der Engineering-Station aus

Die PID-Autotuning-Funktion muss eine bedienungsfreundliche grafische Oberfläche mit einem Setup-Assistenten bereitstellen, um Ingenieure und Techniker zu unterstützen, die mit dem Tool nicht vertraut sind.

5.13 Fehlerbehandlung

Der Status „ungültiger Wert" ist für Eingangswerte und berechnete Variablen zu generieren.

Ein Wert ist für ungültig zu erklären, wenn eine der folgenden Bedingungen zutrifft:

- Wert liegt außerhalb des Bereichs
- Wert kann nicht gemessen oder berechnet werden
- Wert wird durch ein Anwendungsprogramm für ungültig erklärt
- Wert wird durch den Sensor oder Messumformer für ungültig erklärt

Der Status „ungültiger Wert" (Datenqualität) ist durch Steuerungskonzepte zu verbreiten und muss beim HMI verfügbar sein.

Es muss möglich sein, die Erkennung und Verbreitung eines Status „ungültiger Wert" zu unterdrücken. Diese Auswahl muss wahleise verfügbar sein.

Es muss außerdem möglich sein, einen Status „ungültiger Wert" als logischen Eingang von Änderungen des Steuerungsalgorithmus zu verwenden.

Wenn der Eingang eines Steuerungsalgorithmus für ungültig erklärt wird, muss es möglich sein, den Ausgang wie folgt auf „Fehler" zu konfigurieren:

- Halten des letzten ordnungsgemäßen Werts
- Ausgangssignal null
- Benutzerdefinierter Ausgabewert

Bei einer Störung des Kommunikationssubsystems müssen Regelalgorithmen mit der zuletzt gültigen Information weiterarbeiten können.

5.14 Variable Zykluszeiten von Steuerungsfunktionen

Die Steuerungsausführungsraten für analoge und diskrete Funktionen müssen einzeln projektierbar sein.

Der schnellste Programmverarbeitungszyklus für diskrete und analoge Regelungsfunktionen muss bei 10°ms möglich sein.

5.15 Schaltschränke

Schaltschränke müssen den CE-Normen der EU für elektromagnetische Verträglichkeit (EMV) gemäß IEC 61000 entsprechen und den Schutz vor unbefugtem Zugriff, mechanischen Einflüssen, Verschmutzung und anderen Umgebungseinflüssen sicherstellen.

Der Standardschaltschrank muss der Schutzart IP20 entsprechen und die Möglichkeit des Schrankausbaus auf IP55 muss den Umweltbedingungen entsprechen.

5.16 Kommunikation der Controller über Systembus

Der Systembus, der für die Kommunikation zwischen Controllern und mit den Operator-Stationen (Server) verwendet wird, muss mit einer Datenübertragungsrate von 100 Mbit/s bzw. 1 GB/s betrieben werden können.

Die Verwendung von LWL-Kabeln für die störungsfreie Kommunikation zwischen weit voneinander entfernten Automatisierungs- und Operator-Stationen (wie bei vielen Verarbeitungsanlagen erforderlich) muss unterstützt werden.

ITP-Kabel (Industrial Twisted Pair) sind für Entfernungen bis zu 100 m zu verwenden.

Die Länge des Systembusses muss auf 150 km erweiterbar sein.

Der Systembus muss bis zu 1024 Stationen unterstützen.

Zur Sicherstellung maximaler Verfügbarkeit muss der Systembus die Konfiguration in einer redundanten Ringarchitektur unterstützen (mit LWL- und/oder mit Kupfermedien).

5.17 CPU-Reservekapazität

Zum Reservieren von CPU-Kapazität für eine künftige Erweiterung und zur Sicherstellung der schnellen Software-Reaktion auf Prozessstörungen darf die CPU-Belastung der projektierten Software-Anwendung XX% während der normalen Prozessüberwachung und -steuerung nicht überschreiten.

6 Eingänge und Ausgänge

6.1 Allgemeine Eingänge und Ausgänge

Gleichtakt-Unterdrückungsverhältnisse von mindestens 60 dB von Gleichspannung bis 60 Hz und ein Gegentakt-Unterdrückungsverhältnis von mindestens 30 dB bei 60 Hz sind erforderlich.

Das System muss die Potentialtrennung zwischen den Kanälen Baugruppenspezifisch bereitstellen.

Analoge Eingabe- und Ausgabebaugruppen müssen für den Austausch von Nicht-Steuerdaten (sowohl PROFIBUS, PROFINET als auch HART) mit Asset-Management-Anwendungen unter Verwendung der Infrastruktur des Systems durchgängig sein.

Für die Ausgabebaugruppen müssen folgende projektierbare Sicherheitsoptionen verfügbar sein:

- Steuern auf vorher festgelegte analoge Ausgabe oder Ausschalten bei digitaler Ausgabe
- Beibehalten des letzten ordnungsgemäßen Ausgabewerts für eine analoge Ausgabe oder Halten für eine digitale Ausgabe

Die oben aufgeführten Sicherheitsmaßnahmen müssen durchgeführt werden bei entsprechender Projektierung beim Anhalten des Controllers, bei Ausfall der Stromversorgung oder wenn es zu Kommunikationsfehlern zwischen dem Controller und der E/A-Baugruppe kommt.

Es muss möglich sein, Baugruppen in abgesetzten I/O-Racks bei eingeschaltetem Rack auszutauschen, ohne dass dadurch die Kommunikation mit anderen Baugruppen im Rack beeinträchtigt wird.

6.2 Unterstützung von dezentralen E/A-Architekturen

Remote-I/O-Stationen müssen direkt vom Leitsystem unterstützt werden, um die Verdrahtungskosten zu minimieren und eine kostspielige "Home Run"-Verdrahtung zu vermeiden. Das System muss die folgenden Remote-I/O-Stationsfamilien unterstützen:

- Eigensicher (EEx-i): zur Installation direkt in Gefahrenbereichen (per NEC Class 1 Div 2, Zone 1/Zone 2)
- Unterstützung fehlersicherer Anwendungen
- Unterstützung von HART-Feldgeräten
- Mit integrierten Klemmleisten
- Mit Spezialbaugruppen wie Motorstartern und Waagen
- Mit verschiedenen Ebenen der Diagnose und Auflösung (Anzahl signifikanter Bits)

Die PROFINET-Stationsfamilie muss folgende Funktionen aufweisen:

- Systemredundanz S2
- Medienredundanz MRP
- Änderbarkeit im laufenden Betrieb

Um Flexibilität bei der Platzierung von Geräten zu erreichen, muss das System des Anbieters die Installation dezentraler E/A-Baugruppen in weiter Entfernung (9,6 km bei Kupferkabel oder größere Entfernung bei Verwendung von LWL) von ihrem zugehörigen Controller unterstützen.

6.3 Redundanz

Das System muss die Nutzung von E/A-Redundanz unterstützen, wobei ein einzelner Messfühler oder ein einzelnes Stellglied an zwei gesonderten E/A-Baugruppen angeschlossen sein kann.

Ein redundanter Controller kann innerhalb des gleichen Systems eine Kombination redundanter E/A und nicht redundanter E/A nutzen.

Um die Möglichkeit von Fehlern mit gemeinsamer Ursache auf ein Minimum zu reduzieren können, müssen redundante E/A-Baugruppen in physikalisch voneinander getrennten Racks untergebracht werden. Die gemeinsame Nutzung der gleichen Rückwandplatine ist nicht zulässig.

Im PROFINET Umfeld ist zur Minimierung von Fehlern eine red. Stromversorgung, ein red. PROFINET-Anschluss (S2 oder R1) und eine red. E/A Baugruppe erforderlich.

Das System soll eine optimale Integration von redundanten Remote-I/O-Racks (RIOs), redundanten E/As und Feldbus (PROFIBUS PA und DP und PROFINET), sowohl in redundanter als auch nicht redundanter Ausführung bieten.

Es muss möglich sein, zwei Messstellen unter derselben Messstellenbezeichnung anzulegen und integrierte Redundanzfunktionalitäten ohne zusätzlichen Programmieraufwand anzuwenden.

6.4 Analoge Eingänge

Das System muss in der Lage sein, die folgenden Typen analoger Prozesseingangssignale zu unterstützen:

- 4-20 mA DC, 0-20 mA DC und ±20 mA DC, isolierte und nicht isolierte Eingänge
- 1-5 V DC, ±10 V DC, ±5 V DC und 0-10 V DC, isolierte und nicht isolierte Eingänge
- Thermoelemente Typ B, E, J, K, L, R, S, T und U
- Platin-Widerstandsthermometer (RTD) – PT100, PT500, PT1000, Ni100, Ni1000, Cu10 - gemäß IEC 60751
- Schneller Impulseingang – 1, 10, 20, 100, 250, 500 kHz, bei 24 V

Temperaturlinearisierung und Kaltlötstellenkompensation für Thermoelemente müssen bereitgestellt werden.

Die normale Auflösung muss mindestens 12 Bit sein; Spezialbaugruppen mit 16-Bit-Auflösung müssen verfügbar sein.

Typische analoge Eingabebaugruppen müssen bei 25 °C mit einem Basisfehler von max. ±0,25% des Eingangsbereichs arbeiten.

6.5 Digitale Eingänge

Das System muss in der Lage sein, die folgenden Typen digitaler Eingänge zu unterstützen:

- 24 V DC (mit Möglichkeit der Zeitmarkierung mit einer Auflösung von 1 ms)
- 125 V DC
- 48-120 V DC
- 24-48 V AC/DC, 50/60 Hz
- 120 V AC, 50/60 Hz
- 230 V AC, 50/60 Hz

6.6 Analoge Ausgänge

Das System muss Ausgänge der Typen 0-20 mA, 4-20 mA, ±20 mA, ±10 V DC, 0-10 V DC und 1-5 V DC unterstützen.

Analoge Ausgabebaugruppen müssen mit folgender Fehlergrenze arbeiten:

- Spannung: ±0,2% des Ausgangs
- Strom: ±0,3% des Ausgangs

6.7 Digitale Ausgänge

Die folgenden Bemessungsdaten für statische Ausgänge müssen verfügbar sein:

- 24 V DC
- 48-120 V DC
- 20-125 V DC
- 120 V AC, 50/60 Hz
- 230 V AC, 50/60 Hz

Spannungs- und erdungsfreie Relais- oder statische Ausgangskontakte müssen verfügbar sein.

Relaisausgänge mit einer Bemessungsspannung von 24 V DC bis 120 V DC bzw. 48 V AC bis 230 V AC (5A) müssen verfügbar sein.

Digitalausgabemodule mit (externer) Aktorabschaltung via Low-Signal oder High-Signal müssen verfügbar sein.

6.8 Vorkonfigurierte Abschlussbaugruppen/-komponenten (MTA)

Um Installationskosten und Installationszeit zu sparen, muss das System eine standardisierte Zusammenstellung von vorkonfigurierten Abschlussbaugruppen (MTA, Marshalled Termination Assemblies) anbieten. Damit soll sichergestellt werden, dass die Verbindung zur Feldebene schnell und einfach aufgebaut werden kann und Verdrahtungsfehler vermieden werden. Diese Abschlussbaugruppen müssen eine individuelle Absicherung der einzelnen Kanäle ermöglichen und auch individuelle Anzeigen bezüglich durchgebrannter Sicherungen und redundanter Stromversorgung bieten. Eine übliche Abschlussbaugruppe soll die Verbindung zu einem redundanten oder nicht redundanten E/A-Aufbau unterstützen.

Für eine schnelle, einfache (vermeiden von verdrahtungsfehlern) Verbindung zur Feldebene via PROFINET müssen die Profinet Feldgeräte folgende Eigenschaften aufweisen:

- höchste Verfügbarkeit an PROFINET mittels Systemredundanz S2 oder redundante PROFINET Konfiguration R1
- integrierte IO Redundanz (ohne MTA)
- Modultausch im laufenden Betrieb
- Medienredundanz MRP

6.9 Peripheriebus-Eigenschaften

Der Peripheriebus muss nachfolgende Eigenschaften besitzen:

- Vermeidung von unvorhergesehenem Anlagenstillstand durch erhöhte Verfügbarkeit.
- Automatischer Busabschluss
- Detaillierte Diagnosemöglichkeiten
- Änderungen an der Konfiguration müssen online durchgeführt werden können. Das beinhaltet Reparatur und Erweiterungen einschließlich Änderungen am Kabelbus.

6.10 Peripheriebus-Redundanz

Der Peripheriebus muss redundant ausgeführt werden können.

Der Anbieter muss eine Kopplerredundanz bereitstellen.

Der Anbieter muss eine redundante Ringstruktur des Peripheriebusses bereitstellen können.

Werterfassung von Feldgeräten muss fehlersicher (1oo2) und fehlertolerant (2oo3) durchgeführt werden können. Der Anbieter muss dies mit seiner Busarchitektur gewährleisten können.

6.11 Peripherieanschaltungen und Koppler

Die Peripherieanschaltungen und Koppler müssen in das Alarmsystem des Leitsystems integriert sein.

Die Peripherieanschaltungen und Koppler bieten auf Wunsch die Aufzeichnung von Ereignissen (SOE, Sequence of Events).

Die Peripherieanschaltungen sollten eine hohe Kanaldichte unterstützen (z.B. >320 diskrete oder >80 analoge E/A).

Die Peripherieanschaltungen/Koppler müssen HART-Sensoren unterstützen.

Die Scanrate für alle Kanäle soll nicht größer als 120 ms sein.

Eine Zeitstempelung von 1 ms für DI muss verfügbar sein (SOE = Sequence of Event Recording).

Das System muss eine Closed Loop (Regler) Scanzeit von bis zu 10 ms unterstützen.

6.12 Offene E/A-Kommunikation

Für die Kommunikation zwischen einem Controller und dessen E/A-Baugruppen sollen offene Standards verwendet werden, um die Anbindung von Drittanbieter-E/A mit Systemunterstützung (Diagnose und technische Bedienungsfreundlichkeit) auf dem gleichen Niveau zu ermöglichen, wie es durch den Anbieter zur Verfügung gestellt wird. Der Einsatz proprietärer Kommunikation zwischen E/A und dem Controller ist nicht akzeptabel.

Die Kommunikation zwischen Controller und E/A sollte der Norm IEC 61158 PROFINET entsprechen.

6.13 AS-Interface-E/A

Das System muss AS-Interface-Eingänge und -Ausgänge für diskrete Geräte wie z.B. Schalter und Magnetspulen unterstützen. Das AS-Interface muss eine Link-Baugruppe auf dem PROFIBUS-DP sein und mit den Feldgeräten über das serielle Kabel des AS-Interface kommunizieren.

6.14 EIB-Instabus-E/A

Das System muss EIB-Instabus-Eingänge und -Ausgänge unterstützen, wie sie in Gebäudeautomatisierungssystemen verwendet werden, und die Kombination des Gebäudeleitsystems (Building Control System) und des Anlagenleitsystems (Plant Control System) in einem einzigen System ermöglichen. Das EIB-Interface muss eine Link-Baugruppe auf dem PROFIBUS-DP sein und mit den Feldgeräten über das serielle Kabel des EIB-Interface kommunizieren.

6.15 HART-E/A

Das System muss HART-Eingänge und -Ausgänge unterstützen. Die HART-Schnittstelle muss eine Baugruppe auf PROFIBUS sein oder die HART-Geräte können mit herkömmlichen analogen Eingabe-/Ausgabebaugruppen verbunden werden. Alle Komponenten müssen Plug-and-Play-Fähigkeit bieten. Das technische System muss alle vom Feldgerät gelieferten Variablen ohne zusätzliche Verdrahtung lesen können.

7 Feldbus

7.1 Allgemeine Anforderungen

Das System muss alle vom Feldgerät gelieferten Variablen ohne zusätzliche Verdrahtung lesen können.

Diagnostische Informationen müssen von den Feldgeräten verfügbar sein, unter anderem Gerätefehler, Projektierungsfehler, Betriebsart und Wartungsanforderungen.

Kompatibilität mit Drittanbietergeräten

Das System muss alle Feldgeräte unterstützen, die von der zuständigen Standardisierungsorganisation für den betreffenden Feldbustyp zugelassen sind; ohne zusätzlichen Genehmigungen durch den Anbieter des Host-Systems.

7.2 Feldbus PROFINET

Das Automatisierungssystem muss PROFINET als Teil der Normen IEC 61158 und IEC 61784-2 unterstützen.

Das System muss den Anschluss von PA-Geräten und DP-Geräten / Segmenten in den PROFINET-Feldbus sicherstellen.

Maximale Kommunikationsbandbereite

PROFINET muss eine Übertragungsbandbereite von 100 Mbit/s im Vollduplex Betrieb unterstützen.

Nutzdaten pro Gerät

Pro Gerät muss PROFINET bis zu 1440 Byte Nutzdaten erlauben.

Netzwerkarchitektur

Die Netzwerkarchitektur muss individuell an die Anlage anpassbar sein via Ring-, Baum- und Stern-Topologien mit einem oder mehreren IO-Controllern.

Anzahl der PROFINET-Geräte pro Controller

PROFINET-Schnittstellen der Controller müssen den Anschluss von bis zu 500 PROFINET-Geräten unterstützen.

Maximale Segmentlänge

Die maximale Segmentlänge zwischen zwei PROFINET-Geräten muss für Kupferleitungen bis zu 100 m und für LWL-Leitungen einige km betragen.

Folgende Funktionalitäten müssen vom System unterstützt werden:

Systemredundanz S2 und redundante PROFINET Konfiguration R1

Änderbarkeit im laufenden Betrieb

Unterstützung von Switches

Das System muss über MRP fähige Switches verfügen, die ebenfalls den Anschluss von Geräten mit einfacher Systemredundanz S2 an Netzwerke mit R1 ermöglichen. Dabei bleibt die Netzwerktrennung der R1-Netzwerke unverändert.

Unterstützung von Industrial Wireless LAN (IWLAN)

Das System muss den Anschluss von bis zu 8 PN-Geräten hinter WLAN-Clients mit S2- und R1-Redundanz unterstützen.

7.3 Feldbus PROFIBUS DP

Feldbussegmente

Das Feldbussegment muss bis zu 125 Slave-Knoten (Geräte) unterstützen wie z.B. Analysatoren, frequenzgestellte Antriebe und Motorschutzgeräte, wobei jedes Gerät in der Lage ist, mehrere Prozessmessungen einzubringen.

Maximale Kommunikationsbandbreite

Um die erforderliche Anzahl von Segmenten (Netzen) zu minimieren, muss die PROFIBUS DP-Implementierung Datenübertragungsraten von bis zu 12 MB/s unterstützen.

Schnittstelle zu redundanten Medien

Das System muss den Anschluss von nicht redundanten Slaves an einen redundanten PROFIBUS unterstützen. Das System muss die Kombination von redundanten und nicht redundanten PROFIBUS-Segmenten unterstützen.

Maximale Kabellänge

Das serielle Multi-Drop PROFIBUS DP-Netz des Systems muss ein Zweileiterkabel nutzen und eine maximale Kabellänge von 9,6 km unterstützen. Bei Einsatz optionaler LWL-Kabel darf es keine praktische Begrenzung der maximalen Kabellänge geben.

Anzahl der Segmente pro Master

Das System muss bis zu 8 PROFIBUS DP-Segmente pro PROFIBUS -Master-System unterstützen.

Anzahl der PROFIBUS-Master-Systeme pro Controller

An einen Controller müssen bis zu 4 PROFIBUS DP-Stränge über interne Schnittstellen am Controller und bis zu 10 PROFIBUS DP-Stränge über zusätzliche Karten anschließbar sein. An einem PROFIBUS DP-Strang müssen bis zu 125, an einem Bussegment bis zu 31 Geräte mit PROFIBUS DP-Schnittstelle (32 Teilnehmer) betreibbar sein.

Online-Zuschaltung von Geräten (Slaves)

PROFIBUS-Slave-Geräte müssen dem PROFIBUS DP-Netz online hinzugefügt werden können (auch bei Systemen mit nicht redundanten Controllern).

Direkte Unterstützung der Steuerung von Motoren und Antrieben

Das System muss so leistungsstark sein, dass es intelligente MCC-Geräte über PROFIBUS DP unterstützen kann, ohne Nutzung von Übergangseinheiten (Gateways) oder zwischengeschalteter SPS zur Steuerung von Folgendem:

- Motoren
- Ventile
- Regelantrieb (VSD, Variable Speed Drive)
- Softstarter

7.4 Prozessfeldbus PROFIBUS PA/Foundation Fieldbus H1

Die Datenübertragungsrate für die Kommunikation mit Prozessfeldgeräten, die an den PROFIBUS PA/Foundation Fieldbus (FF) H1 angeschlossen sind, muss 31,25 kBit/s sein. Eine H1-Ringtopologie muss vorhanden sein, um bei einem Leitungsbruch oder einem Abklemmen die Kommunikation zu allen Feldgeräten aufrecht zu erhalten.

Interoperabilität

Das System muss den Einsatz von Geräten verschiedener Hersteller auf dem gleichen Feldbus unterstützen.

Wechselseitige Austauschbarkeit

Das System muss die Möglichkeit des Austauschs eines Feldgeräts eines bestimmten Herstellers durch ein Feldgerät des gleichen Typs eines anderen Herstellers unterstützen, ohne dass dadurch Funktionalität verloren geht (z.B. Temperaturmessumformer). Die Konfigurationssoftware muss diese Funktionalität unterstützen.

Minimierung der Verdrahtungskosten

Zur Minimierung der Verdrahtungskosten sollte es nicht notwendig sein, einzelne Kabel für jedes PROFIBUS PA-/FF H1-Segment den ganzen Weg vom Feld zurück in die Nähe des Controllers zu verlegen.

Anzahl an Geräten pro PROFIBUS PA/FF H1-Segment

Das PROFIBUS PA/FF H1-Feldbussegment muss bis zu 31 Geräte in einem Mehrzweckbereich und bis zu 9 Geräte in einem eigensicheren Bereich (EEx-i) unterstützen. (Unter Annahme einer durchschnittlichen Stromaufnahme von 12 mA pro Gerät.)

Minimierung der Anzahl physikalischer Geräte

Zur Minimierung potenzieller Ausfallpunkte im System sollte für die Stromversorgung von Feldgeräten kein getrennter physikalischer Geräteanschluss erforderlich sein.

Integrierter Busabschlusswiderstand (Bus Terminator)

Die PROFIBUS PA/FF H1-Schnittstelle des Systems muss einen Leistungsverbesserer (Power Conditioner) und einen integrierten Busabschlusswiderstand (Bus Terminator) umfassen, um die Zahl der Ausfallpunkte zu verringern und die Arbeitskosten für die Verdrahtung des Segments zu reduzieren.

Unterstützung eigensicherer Bereiche (EEx-i)

Das System muss die Platzierung von PROFIBUS PA/FF H1-Feldgeräten in eigensicheren Bereichen unterstützen (bis zur Class 1 Div 1/ZONE 1).

Integrierte Schranke für eigensichere Bereiche

Das Gateway des Anbieters zum eigensicheren PROFIBUS PA/FF H1-Feldbussegment muss eingebaute eigensichere Schranken für den Anschluss dieser Art von Geräten bereitstellen.

Integration des Foundation Fieldbus

Der Anbieter muss Feldgeräte über FF in die angebotene Leitsystemarchitektur integrieren können.

Das System muss eine Schnittstelle anbieten, die es erlaubt, FF-Geräte anzuschließen. Die folgenden Funktionen müssen unterstützt werden:

- Zyklischer und azyklischer Datenaustausch
- Diagnose
- Integration in die Wartungsstation des Systems
- "Kontrolle im Feld"

7.5 Redundanter und fehlertoleranter Prozessfeldbus

Für aufgabenkritische Applikationen muss das System die Erstellung von redundanten/fehlertoleranten Architekturen auf PROFIBUS PA/FF H1 und PROFINET-Ebene erlauben.

Das System muss den Aufbau von redundanten Ringstrukturen für Feldbusse unterstützen.

Höchste Verfügbarkeit durch Fehlertoleranz

Um aufgabenkritische Prozessinstrumentierung im Falle von Kommunikationsfehlern weiter lauffähig zu erhalten, muss das System ohne Unterbrechung die folgenden Fehlertypen verkraften:

- Betriebsstörung des Feldbuskopplers
- Kurzschluss oder Drahtbruch auf dem Feldbus
- Kurzschluss oder Drahtbruch an einem Feldbus-Stichleitungssegment
- Fehlender/vergessener Busabschluss

Online-Konfiguration

Das System muss Online-Konfigurationsänderungen wie zum Beispiel Reparaturen, Erweiterungen und Modifikationen am Bus unterstützen.

7.6 Feldbusverteiler

Feldbusverteiler an PROFIBUS DP

Für die Anbindung und den Anschluss von Feldgeräten muss das System entsprechende Anschlussbaugruppen bereitstellen. Diese Anschlussbaugruppen müssen folgende Merkmale aufweisen:

- Automatisches Beobachten des Busses
- Anschluss von mindestens 8 Geräten
- Automatischer Busabschluss
- IP65-Gehäuse, Anschluss von Konfigurations-PC
- Kurzschlusssichere Anschlüsse
- Temp.-Bereich: -25 °C bis 60 °C
- Einsatz innerhalb Zone 2 (Class 1 Div 2)
- Diagnose-LEDs

Feldbusverteiler für Profibus PA-Feldgeräte über PROFINET

Für die Anbindung und den Anschluss von PA Feldgeräten muss das System entsprechende Anschlussbaugruppen bereitstellen. Diese Anschlussbaugruppen müssen folgende Merkmale aufweisen:

- Einfache Integration in das Prozessleitsystem
- Automatische Initialisierung
- Automatisches Beobachten des Busses
- Anschluss von mindestens 8 PA Geräten
- Automatischer Busabschluss
- IP66-Gehäuse,
- Temp.-Bereich: -40 °C bis 70 °C
- Einsatz innerhalb Zone 2 (Class 1 Div 2)
- Diagnose-LEDs

Darüber hinaus sollte der Busverteiler zur einfacheren Integration von Sensoren bzw. Aktoren über konfigurierbare Kanäle (digitale Ein-/Ausgänge) verfügen

Generelle Anforderung an Feldbusverteiler

Die Feldbusverteiler müssen Schutz gegen Feldbuskurzschlüsse und Drahtbrüche bieten, sodass Verteiler/Feldbusgeräte dadurch nicht beeinträchtigt werden.

Installation, Erweiterung, Ausbau oder Austausch von Feldbusverteilern/-geräten muss möglich sein, ohne dass dabei vorhandene angeschlossene Geräte beeinträchtigt werden. Hierzu zählt u.a. auch die Beeinträchtigung durch einen inkorrekten Anschluss und/oder Flattern (Chattering) bei der (De-)Installation. Die Bitübertragungsschicht (Physical Layer) muss von Bus- und Stichleitungssegmenten vollständig getrennt werden.

Die Feldbusverteiler müssen mit integrierten Diagnosefunktionen ausgestattet sein.

Die Verteiler müssen in Industrie- und EEx (ia)-Ausführung erhältlich sein. Sie müssen außerdem für den Einsatz in Zone 1/2 zertifiziert sein.

8 Kommunikation und Vernetzung

Das System muss Industrial Ethernet auf dem Systembus für die Kommunikation zwischen Controller und ABKs verwenden.

Das System muss den Einsatz von marktüblichen Standard-Netzwerkkomponenten für den Terminalbus zur Kommunikation zwischen Servern und Clients unterstützen.

Das System muss den Einsatz von LWL- und Kupfermedien (Twisted Pair) unterstützen.

Das System muss die Datenübertragung mit 10 Mbit/s und 100 Mbit/s auf den Systembusnetzen und bis zu 1000Mbit/s auf den Terminalbusnetzen unterstützen.

Eine projektweite Netzsicht muss verfügbar sein.

Intelligente Feldgeräte (PROFIBUS DP, PA, HART, FF, PROFINET) müssen über ein integriertes Parametriertool ansprechbar sein.

Das System muss intelligente Antriebe über Feldbus ansteuern und diagnostizieren können.

Das System muss WLAN-Funknetze unterstützen.

Die folgenden maximalen Netzgrößen müssen unterstützt werden: elektrisch: max. 1,5 km; LWL: max. 150 km; WAN: weltweit (inkl. Web-Client).

Das Anbietersystem bietet Vernetzungsmöglichkeiten und Unterstützung für Hybridanwendungen und die Ankopplung von Package Units.

8.1 Unterstützte Netzwerk-Architekturen

Das System muss die Ring- und Ringredundanz Topologie beim Aufbau des Systembusses gewährleisten, darüber hinaus die Netz-Topologien Linear, Baum, und Stern.

Das System muss die Ring- und Ringredundanz Topologie beim Aufbau des Terminalbusses gewährleisten, darüber hinaus die Netz-Topologien Linear, Baum, und Stern.

Das System muss die folgenden Netz-Topologien beim Aufbau des Feldbusses unterstützen: Linear, Baum, Ring, Stern und Redundant.

Das System muss bei der Ring Topologie gewährleisten, dass bei einer Unterbrechung der Ringstruktur alle Teilnehmer im Netz erreichbar bleiben.

Bei höchsten Verfügbarkeitsanforderungen ist der Systembus und / oder Terminalbus jeweils auf redundante Ringe auszulegen.

8.2 Smart Switches für Industrieanwendungen

Optionale Smart Switches, die für den Einsatz in Industrieumgebungen ausgelegt sind, müssen zur Verwendung in Verbindung mit dem System verfügbar sein. Diese Switches müssen die folgenden Merkmale haben:

- Unterstützung von LWL- und Kupfermedien
- Eingebaute digitale Eingänge, die mit dem System verdrahtet werden können, um Benutzer vor Netzfehlern zu warnen

- Signalisierungskontakte zur Warnung von Benutzern vor Port- oder Stromversorgungsfehlern
- Redundante Stromeinspeisung
- Integrierte webgestützte Netzmanagementtools
- Schnelle Netzersatzschaltzeiten (Failover) von max. 300 ms
- Lüfterloser Betrieb
- Erweiterter Temperaturbereich -40 °C bis 70 °C

9 Integrated Engineering

Ein Engineering-System muss die Integration von Daten über alle Lebenszyklusphasen eines Projekts hinweg vom Konzept bis zum Anlagenbetrieb und zur endgültigen Außerbetriebsetzung erleichtern.

Das System muss eine homogene Engineering-Umgebung mit Integration von Folgendem bereitstellen:

- Engineering Management
  - Projektstrukturierung (Tagging, Dokumentennummerierung)
  - Integriertes Änderungs-Management
  - Mehrbenutzer- und Mehrprojekt-Engineering
  - Bulk-Engineering (IEA, PAA)
- Grundlegendes Engineering
  - Materialklassen
  - Layouts
  - Flussdiagramme, P&I-Fließschemata
  - Blockschaltbilder
  - Verbraucherlisten
  - usw.
- Detaillierter Aufbau & Konfiguration
  - Funktionspläne
  - Grafisches Engineering mit CFC, SFC und Safety Matrix
  - Schaltpläne
  - Projektierung des Prozessautomatisierungssystems
  - Kabellisten
  - Materialstückliste
  - Detaillierte Layouts
  - Isometrien
- Beschaffung und Herstellung
  - Material-Management (Anforderungen, Optimierung, Nachverfolgung)
  - Logistik
  - Qualitäts-Management (Gewährleistung, Tests und Archivierung)
- Konstruktion und Inbetriebnahme
  - Einbauanleitungen
  - Qualitäts-Management (Gewährleistung, Tests und Archivierung)
  - As-Built-Dokumentation
- Verfahren

- Schulung
- Wartungsunterstützung
- Revision
- Online Änderungen

Das Prozessautomatisierungssystem und das Lifecycle Engineering Tool müssen vollständig integriert sein und die Automatisierung des Engineering-Workflows ermöglichen.

10 Systemprojektierung

Dieses Kapitel spezifiziert die Engineering-Workstation und die Software-Tools, die für das Engineering, die Konfiguration und die langfristige Wartung des Systems zur Verfügung stehen müssen.

10.1 Allgemeine Anforderungen

Für die Engineering-Workstations müssen Standard-PC-Technologie mit moderner Hardware, Microsoft Windows-Betriebssystem und Datenübertragung über Industrial Ethernet eingesetzt werden.

Es muss möglich sein, in einem System mehr als eine Engineering-Workstation zu installieren.

Das Engineering-System muss ein offenes System sein, das beispielsweise den Import von Projektdaten aus Microsoft Excel oder aus CAD/CAE-Programmen zulässt. Der Import/Export von/nach Microsoft Excel muss für eine einfache Bearbeitung möglich sein.

Wechselspeichermedien müssen ebenfalls für jede Engineering-Workstation bereitgestellt werden.

Die Speicherung aller Datenbank- und Projektierungsdaten sowohl auf Wechselmedien als auch auf nicht wechselbaren Speichermedien für Datensicherungszwecke muss möglich sein, ohne dass das System dafür offline genommen wird.

Die Bereitstellung redundanter Speichermedien für die Projektierungsdatenbank muss möglich sein.

Die Engineering-Software muss eine intuitive Benutzeroberfläche ähnlich dem Microsoft Windows Explorer aufweisen, über die der Benutzer alle Aspekte der Projektierung von Controller, HMI, Netz, Hardware und Feldgeräten verwalten und abwickeln kann. Die Verwendung unterschiedlicher, inkonsistenter Oberflächen sollte möglichst vermieden werden.

Das System muss kurze Übersetzungs- und Ladezeiten bieten.

Das System muss eine Archivmarkierung für Variablen unterstützen. Markierte Variablen müssen automatisch archiviert werden.

Das System muss den Datenaustausch mit einem CAD/CAE-System ermöglichen. Unterstützung des Engineering-Workflow ist gefordert.

Die Bedien- und Beobachtungsebene muss sich automatisch ableiten lassen aus dem auf der Engineering-Station erstellten Projekt. Doppelte Eingaben sind zu vermeiden.

Im Bilddesign muss für übersichtliches Engineering die Multi-Layer-Technologie angewendet werden können.

Das Engineering muss mit grafischen Mitteln unterstützt werden, reines Programmieren wird nicht akzeptiert.

Das System muss die direkte Ableitung einer Bildhierarchie in der ABK (bzw. OS) aus der technologischen Hierarchie ermöglichen.

Das System muss hierarchische CFC-Pläne mit grafischer Bausteintyperstellung (Plan in Plan mit Kompilierung) unterstützen.

Das System muss Fehler bei der Projektierung erkennen, die Verbindung zweier ungleicher Datentypen muss überprüft und abgewiesen werden können.

Das System-Engineering muss auch ohne große Kenntnisse der objektorientierten Programmierung hantierbar sein.

Alle Prozessobjekte müssen automatisch eingebracht und verbunden werden können.

Das Anbietersystem muss eine Ablaufsteuerung in der ABK bedienbar darstellen.

Bausteinprogrammierquellen müssen für Anwender zugänglich sein.

Das System muss mit SQL, SYBASE, X Window System und TCP/IP harmonisieren.

Zentrales Engineering aller Komponenten inklusive Feldgeräte muss möglich sein.

10.2 Funktionen der zentralen Engineering-Station

Alle herkömmlichen Projektierungsaufgaben (Controller, HMI, Batch und Historie), die Feldbusprojektierung (Messumformer, Antriebe, Analysatoren usw.), die Datenbankgenerierung und die Editierung müssen auf einer einzigen Engineering-Workstation ausgeführt werden können. Es muss jedoch auch möglich sein, mehrere Engineering-Workstations gleichzeitig für diese Arbeiten einzusetzen.

Die zentrale Engineering-Workstation muss alle folgenden Funktionen unterstützen:

- E/A-Projektierung
- Projektierung der Hardware des Leitsystems (Controller, Operator-Stationen)
- Projektierung von Anlagen- und Feldkommunikationsnetzen
- Projektierung und Wartung von Feldbusgeräten
- Projektierung von Antrieben, Waagen und Motormanagementgeräten
- Projektierung der kontinuierlichen Regelungsvorgänge und Ablaufsteuerungsvorgänge
- Projektierung der Anlagenprozessstruktur/-hierarchie z.B. gemäß S88.
- Projektierung von fehlersicheren (Sicherheitssystem-)Funktionen
- Generierung und Änderung der OS-Bilder
- Projektierung des Messwertarchivs
- Projektierung von historischen und Echtzeittrends
- Management der Alarm- und Ereignisprojektierung
- Erstellung, Generierung und Änderung von Berichten
- Konfiguration von Anwendersicherheit und Zugriffsrechten

- Prozessobjektsicht mit Testmodus
- Datenaustausch mit einem CAD/CAE-System
- Der Operator muss online eine Bildzusammenstellung durchführen können.
- Chargenprojektierung und -planung (Rezepte, Verfahren, Formeln usw.)
- Asset Management-Konfiguration
- Zugriff auf externe Dateien und Programme wie z.B. Microsoft Excel
- Systemdiagnose
- Zuweisung von Servern, Clients und Tastaturen zu Anlagenbereichen
- Controller Simulation Tool für Test und Fehlersuche ohne Controller
- Es muss möglich sein, das Engineering-Projekt über ein benutzerspezifisches Passwort zu schützen.

10.3 Objektorientierte Engineering-Tools

Objektorientierte Projektierungsprogramme müssen zur Unterstützung der Systemprojektierung bereitgestellt werden. Es muss möglich sein, mit dem entsprechenden Tool sowohl Aspekte des Controllers als auch der OS für ein oder mehrere Prozessobjekte gleichzeitig zu projektieren. Das Tool muss für die Projektierung eine Oberfläche ähnlich einem Tabellenarbeitsblatt (Spreadsheet) bereitstellen. Diese soll mit Funktionen wie Kopieren/Einfügen, Suchen und Ersetzen, Sortieren nach Spalte und Anbindung an Microsoft Excel/Access Bedienungsfreundlichkeit gewährleisten. Die folgenden Parameter müssen über diese Oberfläche projektierbar sein:

- Steuerung: Regelkreiskennung (Loop Identifier), Alarmgrenzwerte, Tuning-Konstanten, Deskriptoren, physikalische Einheiten, E/A-Zuordnung.
- OS: Alarmprioritäten, Text von Alarmmeldungen, Zuweisung von HMI-Symbolen, Variablenarchivierungsraten.

Das Engineering-System muss über eine einheitliche Datenbank verfügen, die sicherstellt, dass Daten, die einmal vom Benutzer eingegeben wurden, für alle Tools im System verfügbar sind Auf diese Weise wird gewährleistet, dass Daten nur einmal eingegeben werden müssen (Single Point of Entry).

10.4 Optimierung der Ablaufreihenfolge

Zur Optimierung der Ablaufreihenfolge/Ablaufgruppe muss vom System die Möglichkeit der Kennzeichnung von Abarbeitungszyklen und Ablaufgruppen bereitgestellt werden.

Die Abarbeitungsreihenfolge der Funktionsbausteine muss veränderbar sein

10.5 Bulk Engineering-Funktionen (Massendaten-Projektierung)

Das System muss Tools für das Engineering von großen Datenmengen und für die einfache Duplizierung von standardmäßig durch das System bereitgestellten, oder spezifisch durch den Benutzer erstellten, Standard-Steuerelementen bereitstellen. Das Duplikations-Tool muss die Generierung von Instanz spezifischen Kopien über eine Export- / Kopier- / Import-Routine unterstützen und soll dabei ähnlich einem Tabellenkalkulationsprogramm zu benutzen sein.

Folgende Elementtypen müssen dupliziert und instanziiert werden können:

- Funktionsbausteine
- Funktionspläne (Steuerbausteine)
- Eine gesamte Teilanlage
- Ein gesamter Prozessbereich
- SFCs

Das Werkzeug muss das Klonen von Prozesssteuerungselementen durch Import von Projektierungsdaten aus einer externen Datei unterstützen.

Das Werkzeug muss außerdem einen menügesteuerten Prozess für die Definition reproduzierbarer Elemente und für die Auswahl Instanz spezifischer Attribute (wie z.B. Variablenname oder Projektierungsbereich) eines jeden Elements bereitstellen.

Eine Oberfläche, ähnlich einem Tabellenarbeitsblatt (Spreadsheet), muss für das Klonen von Elementen (wie z.B. Motoren, Ventilen und PID-Reglern) und für die Projektierung ihrer Instanz spezifischen Eigenschaften bereitgestellt werden.

10.6 Standard-Prozessautomatisierungsbibliothek für Controller und HMI

Eine Bibliothek von vorgefertigten Funktionsblöcken für die Prozesssteuerung muss in Verbindung mit ihren zugehörigen OS-Faceplates/Symbolen verfügbar sein. Optionale industriespezifische Bibliotheken müssen ebenfalls verfügbar sein. Die Standardbibliothek muss mindestens aus den folgenden Control-Strategien und vorgefertigten Symbolen/Faceplates bestehen:

- Standard-PID-Regler
- Cascade-PID-Regler
- Verhältnisregler
- Regler mit Bereichsaufspaltung (Split Range)
- Manueller Lader
- Summierer für Feststoffe und Flüssigkeiten
- Digitalwert Überwachung mit Alarmmeldung
- Analogwert Überwachung mit Alarmmeldung
- Motor (Start/Stopp) mit Verriegelungen
- Motor – zwei Drehzahlen
- Motor – vorwärts/rückwärts
- Ventil (auf/zu) mit 1 oder 2 Rückführsignalen
- Ventil (ein/aus) mit Verriegelungen
- Motorisierte Ventilsteuerung

10.7 Projektierungsstruktur

Die Anwendung muss in einer Hierarchie sichtbar und konfigurierbar sein. Die Projektierungselemente sind entsprechend der Anlagen- oder Prozessstruktur gruppiert. Diese Anlagenhierarchie muss das Prozessmodell und die physikalische Anordnung des Prozesses direkt darstellen können. Sie muss verwendet werden können, um die Bildhierarchie bei der Operator-Schnittstelle automatisch abzuleiten und die dynamischen Elemente der Prozessgrafik zu generieren.

Zur Sicherstellung höchster Flexibilität bei der Strukturierung des Controller-Programms muss das System die Erstellung einer Projektierungshierarchie mit mindestens acht Ebenen unterstützen.

10.8 Kopieren/Einfügen

Das System muss das *Kopieren und Einfügen* (Copy and Paste) aller Projektierungselemente in der hierarchischen Projektierungsstruktur unterstützen, u.a. der folgenden Elemente:

- Steuerbausteine (Funktionsbausteine oder Pläne)
- SFCs
- Prozessgrafiken

Das System muss die Möglichkeit des Kopierens und Einfügens verschiedener Ebenen der Hierarchie in einem einzigen Schritt bieten ("Deep Copy"), sodass vollständige Prozessbereiche oder -einheiten mit minimalem Projektierungsaufwand kopiert und geändert werden können.

10.9 Concurrent Engineering

Das System muss Concurrent Engineering-Verfahren unterstützen, d.h. die Möglichkeit des parallelen Arbeitens mehrerer Ingenieure an der gleichen Anwendung über eine vernetzte Umgebung oder über ein "Check-in/Check-out"-Verfahren für die lokale Projektierung auf verschiedenen PCs.

10.10 Dokumentation der Projektierung

Tools für die automatische Dokumentation der Projektierung und Projektdaten müssen verfügbar sein.

Das System muss bei automatischer Dokumentation auch die Verbindungen zwischen einzelnen Charts darstellen können.

10.11 Online-Änderungen der Projektierung

Das System muss die Durchführung von Änderungen an der Projektierung von Controller, E/A, OS, Batch und Kommunikationsnetz online ohne Betriebsunterbrechung unterstützen.

10.12 Change Management (allgemein)

Die Engineering-Station (ES) muss Versionskennzeichnung unterstützen.

Bei Erweiterungen, Änderungen und Streichungen der Projektierung müssen alle Module und Variablen, die von der Änderung betroffen sind, automatisch aktualisiert werden.

Änderungen der Projektierung müssen über eine Abfolge von Eingabeaufforderungen/Bestätigungen mit einem endgültigen Bestätigungsschritt vor dem Download der Änderung auf das Online-System abgewickelt werden. Es muss eine Option bereitgestellt werden, anhand dieser der Benutzer einen detaillierten Bericht der vorgenommenen Änderungen als Teil des Download-Bestätigungsprozesses einsehen kann.

Ungültige Projektierungseinträge müssen beim Kompilieren und Download von Projektierungsdaten erkannt werden und die betreffenden Parameter müssen angezeigt werden.

Es muss möglich sein, unabhängige Kreise im Controller zu ändern, zu löschen und hinzuzufügen, ohne dass dies Auswirkungen auf die anderen Kreise hat.

Im Multiprojektmodus muss das System den Abgleich von Bausteinen der Stammdatenbibliothek in Bibliotheken der Einzelprojekte unterstützen.

10.13 Mehrsprachige Projektierungsumgebung

Die Software des Prozesssystems muss mindestens die Sprachen Englisch, Deutsch, Französisch, Italienisch, Spanisch und Portugiesisch unterstützen. Der Benutzer muss in der Lage sein, zwischen den verschiedenen unterstützten Sprachen in der Projektierungsumgebung und im produktiven Operator-Betrieb hin und her zu wechseln, ohne dafür seine Applikation neu übersetzen zu müssen.

10.14 System-Management

Das System-Management hat zentral zu erfolgen. Die folgenden Hauptfunktionen müssen verfügbar sein:

- Bestands-Management (Inventarisierung) sämtlicher Hardware und Software
- Möglichkeit des Lesens von und Zugreifens auf Bestandsdaten von Servern, Operator-Stationen, Engineering-Stationen, Controllern, Kommunikationsschaltern und dezentraler Peripherie
- Versions- und Lizenz-Management der Hardware und Software
- Berichterstellung und Export der Systemprojektierung nach Excel
- Software-Installations-Management
- Aktualisierung von Server und Operator-Stationen
- Vorbereitung von Rollouts für Server und Operator-Stationen
- Status / Zustandsüberwachung von Zielstationen, Deaktivieren von Stationen zu Aktualisierungszwecken, Reaktivieren von Stationen zu Nutzungszwecken

11 Controller-Projektierung

11.1 Benutzerspezifische Funktionsbausteine

Das System muss Benutzern die Erstellung ihrer eigenen benutzerspezifischen Funktionsbausteine mittels KOP, SCL oder anderen Sprachen ermöglichen. Diese benutzerspezifischen Funktionsbausteine müssen der Anwenderbibliothek hinzugefügt werden können, so dass sie zur Wiederverwendung im gesamten Projekt verfügbar sind.

Benutzerspezifische Funktionsbausteine müssen in der Anwendung wie Standardfunktionsbausteine zu verwenden sein; so muss es beispielsweise möglich sein, sie in CFCs einzubetten oder mit Standardfunktionsbausteinen zu verbinden.

Benutzerspezifische Funktionsbausteine werden mit einem Passwort versehen,, sodass der Zugriff auf geistiges Eigentum des Erstellers geschützt werden kann.

Die Anzahl der benutzerspezifischen Objekte, die ein Benutzer erstellen und in einen Controller laden kann, darf keinen praktischen Einschränkungen unterliegen und wird allein durch dessen Speicherkapazität begrenzt.

11.2 Verbindung von Funktionsbausteinen und Steuerbausteinen (Anlagenteilen)

Die Ein- und Ausgänge aller Funktionsblöcke eines CFC-Plans müssen mit Funktionsblöcken in anderen CFC-Plänen verbindbar sein, ohne dass zusätzliche Parameterfunktionsbausteine benötigt werden.

Das System muss eine Autorouting-Funktion unterstützen, mit der Funktionsbausteine an beliebiger Position mit zwei Mausklicks schnell miteinander verbunden werden können.

Das System muss den Benutzer daran hindern, Funktionsbausteinparameter verschiedener Typen (Real, Bool, String usw.) miteinander zu verbinden.

11.3 Prozess- und Anlagenverriegelungen

Geräteverriegelungen können grafisch durch einfaches Zeigen und Anklicken zwischen Funktionsbausteinen projektiert werden. Dies erhöht die Bediener-freundlichkeit und minimiert die Projektierungskosten. Vom Benutzer darf die Programmierung von Verriegelungen mit Hilfe eines textbasierten Skripteditors verlangt werden.

11.4 Prüfung und Inbetriebnahme

Alle Projektierungswerkzeuge müssen über Prüf- und Inbetriebnahmefunktionen verfügen; z.B. muss es möglich sein, den Wert eines Eingangs oder Ausgangs im laufenden Betrieb anzuzeigen und zu ändern und bei SFCs im laufenden Betrieb Schrittbedingungen und -transitionen anzuzeigen.

Aus der Entwicklungsumgebung muss der Benutzer die Möglichkeit haben, Echtzeiteingabe- und -ausgabewerte vom Steuerungssystem in einer Darstellung ähnlich einem Tabellenarbeitsblatt zu betrachten.

Der Benutzer muss in der Lage sein, dynamische Trendanzeigen aus der Engineering-Umgebung zu erzeugen, um ausgesuchte Eingangs- und Ausgangsvariablen der Control-Strategie zu beobachten.

Die Ausführung eines projektierten Moduls muss deaktiviert oder die Übersteuerung des Ist-Werts durch bestimmte Werte erzwungen werden können (zum Beispiel: fest verdrahtete I/O-Signale), ohne dass dies Auswirkungen auf andere Module hat, die möglicherweise im gleichen Controller laufen.

11.5 Konfiguration/Management von Änderungen

Verfolgung der Änderung von Funktionsbausteinen (Change Tracking)

Jeder Funktionsbaustein oder Funktionsplan muss mit einem eindeutigen Datums-/Zeitstempel versehen werden, der den Zeitpunkt seiner letzten Änderung angibt. Auch diese Information muss als Objekteigenschaft angezeigt werden können, so dass sie direkt aus dem Engineering-Tool heraus aufgerufen werden kann.

Den Funktionsbausteinen/-plänen müssen eine eindeutige Versionsnummer und ein Urheber zugewiesen werden können. Auch diese Information muss als Objekteigenschaft angezeigt werden können, so dass sie direkt aus dem Engineering-Tool heraus aufgerufen werden kann.

Vergleichswerkzeug (Version Cross Manager)

Es muss ein optionales Werkzeug verfügbar sein, mit dem ein detaillierter Vergleich von zwei Applikationen oder von zwei Versionen einer Applikation durchgeführt werden kann. Dieses Werkzeug muss eine Oberfläche ähnlich dem Microsoft Windows Explorer aufweisen, auf der grafisch hervorgehoben werden kann, welche Elemente einer Projektierung unterschiedlich sind (CFCs, SFCs, Funktionsbausteintypen, Anwendungszyklus usw.). Über die Auswahl eines markierten Elements kann der Benutzer tiefer gehen, um genau zu bestimmen, worin der Unterschied besteht (z.B. Alarmgrenzwert oder Abstimmparameter).

Das Vergleichswerkzeug muss in der Lage sein, mindestens folgende Differenzen zu erkennen:

- Anwendungsprogramm (Funktionsbausteine, Pläne, SFC, Hierarchie/Layout)
- Hardware-Konfiguration
- Kommunikation/Netzkonfiguration
- Alarme
- SFC-Details (Schritte, Transitionen und Eigenschaften)

Projektspezifische Bibliotheken

Das System muss die Erstellung einer projektspezifischen Bibliothek unterstützen, die nur diejenigen Standardfunktionsbausteine, Funktionspläne und benutzerspezifischen Funktionsbausteine enthält, die durch den Benutzer entwickelt wurden oder für die Verwendung im Rahmen des Projekts zugelassen sind. Während der Projektierung können alle anderen Systembibliotheken verborgen werden, um sicherzustellen, dass das Projektteam in der Anwendungsentwicklungsphase nur die „projektzulässigen“ Elemente verwendet.

Zentrales Management von SFCs

Das System muss das zentrale Management von SFCs unterstützen, die das Kopieren und die Wiederverwendung eines einzelnen Funktionsplans (z.B. Reaktorheizphase) in einer Anwendung zulassen. Eine Änderung an einer Instanz des SFC muss die automatische Aktualisierung aller anderen Instanzen im Projekt zur Folge haben, was Projektierungszeit spart und die Möglichkeit der Einführung von Inkonsistenzen in der Anwendung minimiert.

Änderungsprotokoll (Change Log)

Ein optionales Werkzeug zur Verwendung auf der Engineering-Workstation muss bereitgestellt werden, um eine Benutzerzugriffskontrolle für die Ausführung geschützter Aktionen zu erzwingen (z.B. Download einer Projektierungsänderung auf den Controller) und die Aufzeichnung von Kommentaren (detaillierter Änderungsgrund) zu ermöglichen. Informationen werden in einer Änderungsprotokolldatei erfasst, die mit jeder neuen Änderung laufend aktualisiert wird. Das Änderungsprotokoll muss jederzeit aufgerufen werden können.

Assistenten

Für die Generierung aller Bausteine, die für die Diagnose von E/A-Baugruppen und Feldgeräten benötigt werden, muss ein Assistent (Wizard) verfügbar sein.

Benennung von Objekten

Für die Benennung von Objekten müssen mindestens 16 alphanumerische Zeichen verwendet werden können, und Benutzer müssen in der Lage sein, den Variablennamen eines Objekts zu ändern, ohne das Objekt oder Referenzen darauf (z.B. SFC-Pläne, Prozessbilder, Variablenprotokollarchive) zu löschen und erneut hinzuzufügen.

11.6 Dienstprogramme für Datenbankberichte und -änderungen

Dienstprogramm für globale Suche (Global Search Utility)

Für die globale Suche in der Datenbank müssen Dienstprogramme bereitgestellt werden. Diese Utilities müssen der Systemzugriffskontrolle unterliegen.

Querverweislisten (Cross Reference Data Listings)

Das System muss Listen mit folgenden Feldern generieren können:

- Variablenkennung
- Variablenbeschreibung
- Typ des Ein- oder Ausgangs
- Hardware-Adresse

Es muss möglich sein, in der obigen Liste die folgenden Funktionen auszuführen:

- Alphabetische Sortierung nach beliebigem Feld
- Filterung nach jedem Feld
- Ausdruck, Anzeige und Speicherung auf Medien
- Datenexport

Die obigen Listen müssen für alle Geräte im System verfügbar sein.

12 Projektierung und Management von Feldgeräten

Ein einziges Tool für das Management von Feldgeräten (Field Device Management Tool) muss zur Projektierung, Parametrierung, Inbetriebnahme und Diagnoseansicht für intelligente Geräte dezentral (über eine lokale Station im Netz) oder von einer zentralen Engineering-Station aus verfügbar sein.

Dieses Werkzeug muss eine zentrale und möglichst einheitliche Anzeige von Geräteparametern und Funktionen für alle unterstützten Geräte unabhängig von ihrer Kommunikationsverbindung bereitstellen (z.B. PROFIBUS DP, PROFIBUS PA und HART-Protokoll, Foundation Fieldbus H1, PROFINET).

Das Werkzeug muss die Möglichkeit bieten, Feldgeräte ohne Unterbrechung des Netzbetriebs online an das Netz anzuschalten.

Das Management Tool muss zudem die Projektierung und das Management von Drittanbietergeräten wie auch von Geräten des Systemanbieters unterstützen.

Das System muss die Möglichkeit bieten, auch Baugruppen anzuschließen, die außerhalb des Standardspektrums liegen.

Das System muss die Möglichkeit bieten, fehlersichere Feldbusinstrumente anschließen zu können.

Das System enthält fertige Lösungen zum Steuern und Diagnostizieren von Antrieben über den Feldbus.

Das Anbietersystem muss für HART-Baugruppen eine stabile Versorgungsspannung bereitstellen.

Die Projektierung von Interlocks muss ohne Programmiersprache durchgeführt werden können.

12.1 Zentralisierte Projektierung, Wartung und Diagnose

Das Management Tool für Feldgeräte muss in der Lage sein, von einem zentralen Standort aus per Routing mit abgesetzten Feldgeräten zu kommunizieren. Die Routing-Funktionalität muss die transparente Datenübertragung zwischen verschiedenen Netzen oder Subnetzen ermöglichen, sodass der Benutzer mit abgesetzten Geräten kommunizieren kann, ohne mit diesen vor Ort verbunden zu sein.

12.2 Kommunikationsbetriebsarten

Das Management Tool für Feldgeräte muss mindestens die folgenden Kommunikationsbetriebsarten unterstützen:

- PROFIBUS DP Interface
- PROFIBUS PA Interface
- HART Interface
- HART Multiplexer
- HART Modem
- Foundation Fieldbus Interface.
- PROFINET

12.3 Funktionen des Management Tools für Feldgeräte

Das Tool muss die folgenden Hauptfunktionen bereitstellen:

- Zuweisung/Konfiguration von Slave-(Netz-)Adressen
- Anpassung und Änderung von Geräten
- Vergleich von Geräten
- Plausibilitätsprüfung
- Simulation, u.a. mit einer Auswahl vordefinierter Simulationsroutinen wie Ramp up (Hochlauf), Ramp down (Herunterfahren), Randomisierung usw.
- Automatische Diagnose
- Management und Inbetriebnahme
- Online-Überwachung ausgewählter Werte, Alarme und Statussignale
- Life-Liste für die automatische Erkennung vorhandener Feldgeräte mit der Möglichkeit:
- Der Öffnung eines Geräteprojektierungsbilds direkt aus der Life-Liste
- Des Hinzufügens von Geräten aus der Life-Liste zur Applikation
- Des Parametrierens von Geräten aus der Life-Liste heraus (sowohl für Feldbus als auch für HART-Geräte)
- Das Anbietersystem muss in der Lifelist HART-Geräte unterstützen können
- Import/Export-Funktion für den Austausch von Feldgerätedaten mit anderen Projekten oder Werkzeugen.
- Export von Gerätestatusinformationen
- Dokumenten-Management, um den Online-Zugriff auf bis zu 10 Dokumente pro Gerät zu erlauben
- Änderungsprotokoll
- Integration von FDI Gerätedateipaketen

12.4 Benutzeroberfläche für das Management von Feldgeräten

Das Tool muss eine grafische Bedienoberfläche mit verschiedenen Sichten der Feldgeräte aufweisen:

- Hardware-Projektsicht
- Prozessgeräte-Netzsicht: Anzeige von Geräteinformationen mit Diagnosestatus, nach Netztopologie gruppiert
- Prozessgeräte-Anlagensicht: Anzeige von Geräteinformationen mit Diagnosestatus für alle Geräte im System aus allen projektierten Netzen
- Feldgeräte-Parametersicht: Anzeige detaillierter Geräteparameterinformationen in Tabellenform. Diese Ansicht muss die Anzeige der folgenden Parameterinformationen unterstützen: Parametername, Wert, Einheit und Status (Anfangswert, geändert oder ungültig)

12.5 Vergleich von Online- und Offline-Gerätedaten

Das Tool muss den direkten Vergleich der Online- und Offline-Gerätedaten ermöglichen. Der Vergleich muss in Form einer Gegenüberstellung angezeigt werden, wobei das Werkzeug die Unterschiede automatisch hervorheben muss.

12.6 Aktualisieren von Geräteprofilen und Hinzufügen neuer Geräte

Das Geräte-Management-Tool muss die einfache Integration von neuen Feldgeräten wie auch von Gerätetreiberaktualisierungen für vorhandene Geräte unterstützen, die vom Systemhersteller oder von Drittanbietern gekauft werden. Die erforderlichen Gerätebeschreibungsdateien und -treiber für die Aktualisierung des Management Tool können von der Internet-Seite des Herstellers heruntergeladen werden. Die Gerätebeschreibungsdateien müssen im EDDL-Format (Electronic Device Description Language) vorliegen (IEC 61804-4).

12.7 Gerätediagnosezustände

Das Management Tool muss mindestens die Bestimmung und Anzeige der folgenden Diagnosezustände unterstützen:

Kommunikationszustände: Nicht geprüft, fehlerhaft, ordnungsgemäß

Gerätestatus: Nicht geprüft, Projektierungsfehler, Fehler, Wartung notwendig, Wartung empfohlen, Simulation oder Handbetrieb, Prozessfehler, ordnungsgemäß

12.8 Rollenbasierter Benutzerzugriff und Sicherheit

Das Tool muss mindestens zwei unterschiedliche Mengen von Benutzerzugriffsberechtigungen und Zugriffschutz bereitstellen. Dies sind mindestens:

Wartungsingenieur (Maintenance Engineer): Kann nur Betriebsdaten ändern (Parameteränderungen).

Spezialist (Specialist): Kann alle projektierbaren Daten ändern. Hierzu zählt auch die optionale Festlegung eines Passworts für den Zugriffsschutz.

12.9 Protokoll-Tool

Für Zwecke der Fehlersuche muss das Geräte-Management-Tool eine integrierte Protokollfunktion aufweisen. Das Protokoll muss die Möglichkeit zur Aktivierung und Auswahl der Meldungstypen bieten, die im Tool angezeigt und zur späteren Prüfung in einer Datei gespeichert werden.

Die folgenden Arten von (wählbaren) Meldungen müssen im Rahmen der Protokollfunktion aufgezeichnet werden:

- Fehler
- Warnungen
- Kommunikationsmeldungen
- Details

13 Konfiguration der Operator-Schnittstelle

Die Operator-Station (OS) muss eine objektbasierte Process Graphics Engine für die Visualisierung und Steuerung von Prozessen bereitstellen. Ein Standarddienstprogramm muss bereitgestellt werden, das in der Lage ist, benutzerdefinierte farbige Bilder zu generieren und zu ändern. Es muss die gleichen Variablenkennungen verwenden, die in der Prozessdatenbank genutzt werden, um auf Echtzeitvariablen aus jeder Datenbank zuzugreifen. Es muss außerdem dem Systemzugriffsschutz unterliegen.

Das Anbietersystem muss ein drahtloses mobiles Eingabemedium anbieten können.

Die Anzahl von gleichzeitig geöffneten Fenstern muss unbegrenzt sein.

13.1 Funktionen der Grafikentwicklungswerkzeuge

Die OS muss bedienungsfreundliche Zeichenwerkzeuge, Grafikpaletten und Bibliotheken mit Standardgrafikobjekten umfassen.

Das Grafiksystem sollte *Assistenten* bereitstellen, um den Benutzer bei Konfigurationsvorgängen mit mehreren Schritten zu unterstützen: Beenden der OS mit oder ohne Betriebssystem, dynamische Umschaltung zwischen Sprachen, Bildschirmnavigation, Aufrufen einer externen Anwendung, Aufrufen eines Faceplate und Verbindung eines Symbols mit einem Prozessobjekt.

Die dynamischen Eigenschaften jedes Grafikobjekts (u.a. Füllniveau, Füllfarbe, Text) sollten sich einfach durch Zuweisung auf der Eigenschaftsliste des Objekts ändern lassen.

Das Grafiksystem muss die Konfiguration gesonderter Abtast-/Aktualisierungsraten für einzelne Grafikelemente (Symbol, Prozesswert usw.) unterstützen, um die Systemlast zu optimieren.

Die Workstation muss standardmäßige Microsoft Windows-Funktionen unterstützen wie: Ausschneiden, Kopieren und Einfügen, Drag and Drop, Gruppierung, Gruppierung aufheben und Schichtung von Objekten. Über die Funktionen Ausschneiden, Kopieren und Einfügen muss der Benutzer auch auf den Inhalt der Windows-Zwischenablage zugreifen können.

Das Grafiksystem muss ein wählbares Raster für die Ausrichtung von Objekten (vertikal, horizontal, links, rechts, oben, unten) und für die automatische Anordnung von Objekten mit gleichem horizontalen oder vertikalen Abstand bereitstellen. Werkzeuge für das horizontale und vertikale Drehen und Kippen von Objekten müssen ebenfalls bereitgestellt werden.

Das Grafiksubsystem muss bis zu 32 grafische Ebenen aufweisen, die individuell aktiviert/deaktiviert werden können (wie bei einem CAD-Zeichenpaket), um das Zeichnen komplexer Bilder zu erleichtern. Die folgende Ebenenfunktionalität muss bereitgestellt werden:

- Promote/Demote: Vorstufen/Rückstufen von Objekten zwischen Ebenen
- Zoom-Funktionen beim Erstellen von Bildern, u.a. Anwendung der *Gummibandtechnik* auf spezifische Bereiche, die von Interesse sind
- Minimale Desktop-Größe 1920 x 1200 Pixel

13.2 Standardgrafikelemente des Systems

Das System sollte unter anderem die folgenden Standardgrafikelemente bereitstellen: Linien, Polygonkurven, Polylinien, Kreise, Bögen, Ellipsen, Rechtecke, Vielecke, statischen Text, OLE-Objekte, ActiveX- Objekte, Eingabe- und Ausgabefelder, Balken, Bildobjekte (Bitmap BMP, Microsoft Windows Meta File WMF und Enhanced Microsoft Windows Meta File EMF), Statusanzeigen, Textlisten, 3D-Balken, Schaltflächen (Buttons), Check- und Radioboxes sowie Schieberegler (Slider).

Das System muss die Verwendung von Vektorgraphik-Dateien unterstützen, die sich der jeweiligen Auflösung der handelsüblichen Monitore und mobilen Geräte anpassen und sich stufenlos vergrößern oder verkleinern lassen.

Das System muss außerdem vorkonfigurierte *intelligente* Steuerobjekte zur Darstellung von Uhren, Messwertanzeigen, Tabellen, Anwendungsfenstern, Alarmfenstern und Trendfenstern bereitstellen.

Die OS muss mit einer umfassenden Bibliothek prozessorientierter Objekte für die Entwicklung von Prozessbildern bereitgestellt werden: Röhren, Motoren, Ventile, Pumpen, Tanks, Lüfter, Anzeigeelemente, Sensoren, Fördereinrichtungen, elektrische Symbole u.a. Diese Objekte müssen in verschiedenen Formaten zur Verfügung gestellt werden (statisch, geeignet für die dynamische Verknüpfung mit der Control-Strategie, 2D und 3D).

13.3 Dynamische HMI-Symbole für die leittechnische Bibliothek

Vorgefertigte Grafiksymbole sind für alle Prozesssteuerungselemente in der leittechnischen Standardbibliothek bereitzustellen (PID-Regler, Ventile, Motoren usw.). Diese vorgefertigten Symbole müssen so konzipiert sein, dass sie ihr zugehöriges Faceplate aufrufen und das dynamische Verhalten des zugrundeliegenden Steuerungselements darstellen, ohne zusätzlichen Projektierungsaufwand zu erfordern.

Die Workstation muss dem Benutzer die Erstellung von Bibliotheken mit benutzerspezifischen und zusammengesetzten Symbolen ermöglichen. Die Bibliotheksverwaltung muss ein integraler Bestandteil des Systems sein.

Das System muss eine identische Handhabung aller sicherheits- und nicht sicherheitsrelevanten PLT-Stellen in der OS/HMI (Visualisieren, Bedienen, Beobachten usw.) zur Verfügung stellen.

13.4 Globale HMI-Symbole

Das System muss die Erstellung globaler Symbole für die Darstellung von Prozesssteuerungselementen unterstützen. Die Editierung einer bestimmten Instanz eines globalen Symbols muss automatisch über einen Assistenten (Wizard) und ohne manuelle Umkonfigurierung auf alle anderen Instanzen des Symbols in der Anwendung übertragen werden.

13.5 HMI-Faceplates

Faceplates (Bildbaustein) müssen durch das System automatisch für jeden Funktionsbaustein/Funktionsplan generiert werden, der in der Prozesssteuerungsbibliothek enthalten ist (PID-Regler, Motor usw.).

Die individuelle Konfiguration einer Faceplate-Detailanzeige für jede Instanz eines Prozessobjekts oder Steuerbausteins darf vom Benutzer nicht verlangt werden.

Faceplates müssen mit einem entsprechenden Symbol wie z.B. einem Motor oder Ventil verknüpft werden. Das Symbol muss vom System automatisch so programmiert werden, dass es ohne manuelle Projektierungsschritte das zugehörige Faceplate aufruft.

Das System muss automatisch eine Faceplate-Liste (Variablenliste) erstellen. Anhand dieser Variablenliste kann ein Operator ein Faceplate durch Auswahl aus einer Liste von Variablennamen aufrufen.

Das System muss ein eigenes "Faceplate Designer"-Dienstprogramm bereitstellen, das die Erstellung benutzerspezifischer Faceplates erleichtert.

An der Operator-Station müssen gleichzeitig mehr als 3 Faceplate-Instanzen aufrufbar sein.

13.6 SFC-Visualisierung

Zur Minimierung der Projektierungskosten muss das System in der Lage sein, Darstellungen von SFCs (oder "SFC-Visualisierungen") auf die OS ohne zusätzliche Projektierung direkt aus der Control-Strategie zu generieren. Diese Bildschirmanzeigen müssen dem Operator die Statusüberwachung und die Interaktion mit einem SFC direkt von einer Operator-Konsole aus ermöglichen.

SFC-Statusanzeigen

Das System muss ein Standard-SFC-Statusanzeigeobjekt bereitstellen, das eine Übersicht über den Status der bereichsrelevanten SFCs gibt. Zusätzliche Informationen einschließlich des Faceplate der SFC-Visualisierung müssen ebenfalls von dieser Statusanzeige aus zugänglich sein.

13.7 Automatische Erstellung von Prozessgrafiken

OS-Bilder mit den dynamischen Elementen, die zur Darstellung von Funktionsbausteinen (wie Motoren, Ventilen und PID-Reglern) verwendet werden, müssen automatisch aus der Projektierung des Controllers generiert werden. Eine manuelle Projektierung zur Platzierung der dynamischen Elemente auf den Anzeigen oder zu ihrer Verknüpfung mit der Steuerungsprojektierung darf nicht erforderlich sein.

Die Bedienoberfläche soll die automatische Erstellung von statischen Prozessbildern unterstützen.

13.8 Automatische Erstellung der Anzeigenavigation

Ein hierarchisches Navigationskonzept muss vom System automatisch für den Aufruf von Prozessbildern durch den Operator erstellt werden.

13.9 Change Management

Um das Change Management zu vereinfachen und dabei Projektierungsfehler auf ein Minimum zu beschränken, muss das System die automatische Aktualisierung aller Referenzen von Änderungen (Change Management) auf einen Funktionsbaustein (u.a. Prozessgrafik, Faceplates, Archive und Scripts) unterstützen, unter anderem bei einer Änderung des Funktionsbaustein-Instanznamens.

13.10 OS Scripting

Die Entwicklungsumgebung muss der OS kundenspezifische Anpassung der Anwendung mit Hilfe leistungsfähiger Skriptsprachen bieten. Das System muss die folgenden Sprachen unterstützen:

- ANSI C
- Skripte

Die Programmierumgebung muss die folgenden Funktionen unterstützen:

- Möglichkeit des Zugriffs auf Eigenschaften und Methoden aller ActiveX-Steuerelemente, die in der Anwendung enthalten sind oder durch einen Drittanbieter bereitgestellt werden
- Möglichkeit des einfachen Aufbaus von Verbindungen zu anderen Anwendungen/Datenbanken (z.B. Microsoft Excel und SQL-Datenbanken).
- Ausführung von Systemfunktionen wie z.B. Anstoßen eines Berichts oder Generieren einer Operator-Meldung
- Festlegung kundenspezifischer Menüeinträge oder Konfigurationsdialoge
- Bedienungsfreundlicher Editor mit Debugging-Unterstützung
- Suchen- und Ersetzen-Funktion zur Erleichterung von Textänderungen
- Darstellungstechniken für Windows-Baum-/Listenansichten zur Erleichterung der Anzeige, Erstellung und Editierung von Programmskripten
- Möglichkeit des gleichzeitigen Öffnens mehrerer Funktionen oder Aktionen um mit "Drag and Drop" Code zwischen beiden auszutauschen.

Die Programmierumgebung muss das einfache Laden und Aufrufen benutzerentwickelter Funktionen und/oder Bibliotheken ermöglichen.

13.11 HMI-Datenbank

Das System muss dem Benutzer die Möglichkeit bieten, flexibel festzulegen, wie viele Ebenen der Anlagenstruktur (max. fünf) im OS-Variablennamen aufzunehmen sind.

Das Datenbanksystem muss sowohl interne (rechnerische) Variablen als auch externe (reale) Variablen unterstützen. Das Datenbanksystem muss die folgenden Variablentypen/Speicherformate unterstützen: binär, 8 Bit vorzeichenbehaftet, 8 Bit nicht vorzeichenbehaftet, 16 Bit vorzeichenbehaftet, 16 Bit nicht vorzeichenbehaftet, 32 Bit vorzeichenbehaftet, 32 Bit nicht vorzeichenbehaftet, 32 Bit IEEE 754 Gleitpunkt, 64 Bit IEEE 754 Gleitpunkt, 8 Bit Zeichentext, 16 Bit Zeichentext, rohe (benutzerdefinierbare) und strukturierte (Template) Variablen.

Variablenkennungen müssen im gesamten System eindeutig sein und der Zugriff auf alle Variablenparameter für die Projektierung muss direkt über die Variablenkennung möglich sein.

Das System muss die Möglichkeit der Festlegung alphanumerischer Deskriptoren in freiem Format für jeden Zustand eines Geräts mit mehreren Zuständen bieten, z.B. "offen", "geschlossen", "Hub" und "Fehler" für ein durch einen Motor angetriebenes Ventil (MOV).

Projektierungs- und Archivdaten müssen in einer relationalen Datenbank gespeichert werden, die mit ODBC (Open Database Connectivity) und Standard Query Language (SQL) gelesen werden kann.

Das Anbietersystem muss auch nach einem Systemausfall konsistente Archive bereitstellen können.

Die Projektarchivierung muss alle HMI-Segmente enthalten. Zusätzliche Arbeitsschritte werden nicht akzeptiert.

13.12 HMI-Textbibliothek

Zur Unterstützung der Lokalisierung mehrsprachiger Anwendungen muss das System eine Textbibliothek mit Terminologie bereitstellen, die so konfiguriert werden kann, dass sie Übersetzungen für eine beliebige Zahl vom Benutzer festgelegter Sprachen enthält. Diese Textbibliothek muss über die Operator-Schnittstelle während der Laufzeit zugänglich sein, so dass Meldungen und Textzeichenketten in der lokalen Sprache dargestellt werden können. Die Textbibliothek muss exportiert und importiert werden können, um die einfache Konfiguration mit Microsoft Excel zu ermöglichen.

13.13 Mehrfachzugriff und Konfiguration der OS

Zugriff und Konfiguration der OS muss für mehrere Anwender gleichzeitig möglich sein.

13.14 Unterstützung Multiversion

Für Systemerweiterungen und die schrittweise Hochrüstungen soll das HMI verschiedene versionierte Funktions-Blöcke und Kontroll-Module in der Steuereinheit unterstützen, Die HMI Faceplates sollen für die verschiedenen versionierten Funktions-Blöcke und Kontroll-Module in der Architektur und Hardware gebräuchlich sein.

14 Operator Interface Architektur und Hardware

14.1 Architektur

Das Bedien- und Beobachtungssystem muss so flexibel sein, dass alle möglichen Anwendungen von einem Einplatzsystem (Single Station) bis hin zu verteilten Client/Server-Architekturen abgedeckt werden. Die Architektur muss den Einsatz mehrerer Server- und mehrerer Client-Konfigurationen unterstützen.

Das System muss skalierbar sein und den Ausbau einer bestehenden Installation durch einfache Lizenzerweiterung ermöglichen.

Eine eigensichere Bedieneinheit (Operator Panel), die in bis zu 200 m Entfernung vom zugehörigen PC installiert werden kann, muss für den Einsatz in explosionsgefährdeten Bereichen verfügbar sein (EEx-i).

Das System muss mehreren Clients den Zugriff auf bis zu 18 Server oder 18 redundante Server-Paare ermöglichen. Jedes Server-Paar muss in der Lage sein, mit bis zu 40 Clients zu kommunizieren.

Es muss möglich sein, jeden Server-Rechner als dedizierten Rechner für spezifische Prozessfunktionalität einzusetzen (Alarmdienst, Erfassung historischer Daten usw.).

Die Archivierung von Prozessvariablen muss auf einzelnen Stationen, OS-Servern und einem ausgesuchten zentralen Archiv-Server möglich sein.

Allgemein muss es möglich sein, einen redundanten OS-Server oder zentralen Archiv-Server jederzeit in eine nicht redundante Struktur einzubauen.

Alle Clients müssen Zugriff auf alle Server inklusive der historischen Archiv-Server haben, ebenso die Server untereinander.

Die Software muss die Portabilität von Anwendungen zwischen Computern ohne Neuentwicklung oder Modifikation unterstützen.

Der Benutzer muss die Möglichkeit haben, den Prozess vom Client oder vom Server aus zu beobachten und zu bedienen. Hierzu zählt unter anderem:

- Gleichzeitige Ansicht der gleichen oder unterschiedlichen Anzeigen
- Durchführung von Prozessanpassungen und Quittierung von Alarmen
- Anzeige von Alarmen, Ereignissen, Trends und Berichten

Die Entwicklungs- und Laufzeitumgebungen müssen voneinander abgekoppelt sein, so dass der Benutzer die Möglichkeit hat, allein für die Laufzeit vorgesehene Clients (Runtime Only) ohne Entwicklungsfunktionalität zu konfigurieren.

Für kleine Systeme muss es möglich sein, alle Entwicklungsfunktionen, die Operator-Eingabe, Archivierung, Batch und Controller auf einem PC zu realisieren.

14.2 PC-Plattformen

Die Konsolen der Operator-Schnittstelle müssen Standard-PC-Technologie mit moderner Hardware, Microsoft Windows-Betriebssystem und Industrial Ethernet-Kommunikation nutzen.

Das System muss die Betriebssysteme Microsoft
Windows 7/Windows 2008 Server und Windows 10/Windows 2012 Server unterstützen.

Es muss möglich sein, die kompletten Projektdaten für die langfristige Datenspeicherung auf externe Platten auszulagern.

Für Server muss die Hardware eine Festplattenredundanz bis RAID XX unterstützen.

Sämtliche Bediener- und Servereinrichtungen müssen über eine ECC-Speicherunterstützung verfügen.

Die Prozessoren müssen mindestens ab der 4. Generation von Intel mit einer auswählbaren Leistung von i3 bis i7/XEON sein.

PC-Bestandteile müssen dem Industrieeinsatz entsprechen und für den Einsatz im Kontrollraum und/oder Prozessbereich geeignet sein.

Hochleistungs-PCs, wie z.B. Server, müssen der 19“-Einbaunorm entsprechen.

Standard-PCs, wie z.B. Clients, müssen sowohl im 19“-Rack-Format als auch im Kompakt-Design für den Feldeinsatz erhältlich sein.

Das Operator-Interface muss in der Form eines lokalen Bedienpanels (local operated panel (LOP)) mit hochauflösendem Touch-Screen und integrierten PC-Komponenten verfügbar sein.

14.3 Monitore

Die Bildschirme für Operator-Stationen müssen mindestens die folgenden Anforderungen erfüllen:

- 21-Zoll-Diagonale
- Auflösung 1920x1200
- 32.000 Farben

14.4 Multimonitorbetrieb

Das System muss 4-fach-Grafikkarten mit einer Auflösung von bis zu 1920x1200 Pixeln unterstützen.

Bei Verwendung von Multi-VGA-Karten muss jeder OS Client in der Lage sein, zwei bis vier Monitore mit entsprechender Reduzierung der Anzahl an Clients pro Server anzusteuern. Die Multimonitor-Workstation muss die benutzerkonfigurierbare Anordnung der Bildschirmansichten zulassen. Es muss möglich sein, entweder einen oder beide Monitore fest für das Bedien- und Beobachtungssystem vorzusehen. Darüber hinaus muss es möglich sein, den zweiten Monitor für die Ansicht anderer Anwendungen zu verwenden, ohne dass dadurch die Operator-Prozessgrafik und Operator-Prozessanzeigen verdeckt werden.

14.5 Drucker

Bildschirmausdruck

Die OS muss zum Ausdruck jeder aktiven Anzeige in der Lage sein.

Das System muss sowohl Farb- als auch Schwarz-Weiß-Ausdrucke aller Anzeigen unterstützen.

Das System muss lokale und Netzdrucker unterstützen.

Laserdrucker müssen unterstützt werden.

14.6 Uhrzeitsynchronisation mit dem Leitsystem

Das Bedien- und Beobachtungssystem muss zur Uhrzeitsynchronisation mit dem Leitsystem in der Lage sein, so dass zwischen Eingabe-/Ausgabeereignissen im Feld und der Zeitmarkierung (Time Stamping) der Ereignisse auf Bedien- und Beobachtungsebene keine Abweichung von mehr als 20 ms vorliegt.

Die Systemzeit basiert auf UTC. Das Microsoft Windows-Betriebssystem wandelt diese dann in die lokale Zeitzone um.

Das System muss die Verbindung mit einer extrem genauen Zeitquelle wie GPS (Global Positioning System) oder DCF77 unterstützen, die als Hauptzeit für das System verwendet werden kann.

Die Datums- und Uhrzeitsynchronisation muss überall auf der Welt mittels einer Satellitenquelle wie GPS möglich sein.

14.7 Web-/Thin-Client-HMI-Architektur

Das System muss Web-basierte Bedienungen aus einem Browser-Fenster des Microsoft Internet Explorers über Internet/Intranet oder eine TCP/IP-Verbindung zum Web-Server des Systems zulassen.

HMI-Web-Server

Der HMI-Web-Server muss so leistungsfähig sein, dass der Zugriff von bis zu 50 Web-Clients simultan unterstützt wird.

HMI-Web-Client

Web-Clients dürfen keine volle Installation der Bediensoftware verlangen, der Betrieb muss einfach mit geladenem Microsoft Internet Explorer und ausgesuchten Plugins, die über Internet ladbar sind, funktionieren.

Web-Client für mobile Geräte

Das System muss das mobile Bedienen und Beobachten mit allen handelsüblichen Mobilgeräten ermöglichen. Dafür ist keine Softwareinstallation auf den Endgeräten erforderlich und die mobilen Geräte müssen lediglich HTML 5 fähige Browser unterstützen.

Erstellen von Bildschirmdarstellungen für Web-/Thin-Client-Operationen

Die Bildschirmdarstellungen zur brauchbaren übersichtlichen Anzeige auf einem Web-Client müssen automatisch durch Veröffentlichen der Anwendung für den Microsoft Internet Explorer erzeugt werden können.

Web-/Thin-Client-Operation

Der Web-Client muss die gleiche Bedien- und Beobachtungsoberfläche wie das Hauptsystem anbieten. Die Zugriffsrechte basieren auf den Sicherheits-/Login-Informationen des Hauptsystems.

Zur Unterstützung der Operator muss der Web-Client im Falle einer Fehlermeldung akustische Alarme signalisieren können.

Basierend auf dem Passwortschutz müssen Web-Client-Benutzer mindestens die folgenden Standardoperationen durchführen können:

- Sollwertänderungen
- Automatische/manuelle Betriebszustandsänderungen
- Alarmquittierung

Die Sicherheit des Web-Servers der Operator-Station wird durch den Endnutzer durch Einschränkung des Zugriffs auf das Anlagen-/Firmennetzwerk mit Hilfe von Firewalls und Passwortauthentifizierung aufrechterhalten.

15 Das Bedien- und Beobachtungssystem im Betrieb

15.1 Allgemein

Alle Anzeigen und Grafiken, die Echtzeitdaten darstellen, müssen automatisch aktualisiert werden, während das entsprechende Bild angezeigt wird. Der Operator muss diese Aktualisierungen nicht eigens anstoßen.

Der Operator muss in der Lage sein, einfach auf bestimmte Anzeigen und Grafiken zuzugreifen: durch Drücken von hierfür reservierten Funktionstasten oder Übersichtsschaltflächen, durch Auswahl aus einer hierarchischen Liste von Bildern in Verzeichnissen oder Menüs oder durch Selektion in einer alphabetischen Liste von allen Bildern.

Das Wechseln zwischen zusammengehörigen Anzeigen und Grafiken auf unterschiedlicher oder gleicher Detailstufe muss mit maximal zwei Operatoraktionen möglich sein.

Ungültige Werte müssen besonders gekennzeichnet werden.

Das System muss eine Übersicht über den Alarmstatus aller Bereiche liefern, auf die ein Operator Zugriff hat, und zwar unabhängig davon, welches Bild gerade angezeigt wird.

Das Anbietersystem muss bei Überschreitung der Performance-Grenzen (Speicher, Zykluszeit) beim Download Hinweise anbieten.

Bedienfreigaben müssen instanzspezifisch modifizierbar sein (an Parametertyp gekoppelt).

Das System muss nach entsprechender Projektierung Informationen und Bedienungen über Intranet/Internet zulassen (Einsatz von Internet-Browsern).

15.2 Grafiksubsystem

Das Grafiksubsystem muss es dem Operator ermöglichen, eine Bedienaktion mit nur ein oder zwei Benutzereingaben anzustoßen. Die Bedienaktion muss mindestens wie folgt ausgelöst werden können:

- Drücken der Maustaste
- Loslassen der Maustaste
- Tastenbetätigung

Für die Dateneingabe durch den Operator müssen folgende Alternativen zur Verfügung stehen:

- Direkteingabe der Daten
- Verwendung der Tasten "Nach oben" oder "Nach unten"
- Bildlaufleiste oder Schieber (Slider)

Der Operator muss die Möglichkeit haben, die Bildhierarchie oben am Bildschirm zu durchsuchen, um die gewünschte Anzeige aufzurufen.

Benutzerkonfigurierbare Schaltflächen (Buttons) oder sonstige bedienbare Objekte zur Auswahl von Betriebsfunktionen oder Anzeigen mit einer einzigen Eingabe müssen bereitgestellt werden. Popup-Fenster müssen vom Operator verschoben und vergrößert werden können.

Alle vom Operator ausgelösten Kontrollaktionen müssen im Meldungsarchiv gespeichert werden.

Es muss möglich sein, die Zugriffsberechtigung zu ändern, um die Bedienung der Controller jedes Anlagenbereichs von jeder Operator Workstation aus durch Eingabe des zutreffenden Zugangskennworts zu ermöglichen.

Es muss eine SFC-Visualisierungsanzeige verfügbar sein, die Schritt- und Transitionsanzeigen mit Schrittkommentaren oder die dynamischen Schrittbedingungen wiedergibt.

Für Sicherheitssysteme, die anhand der Sicherheitsmatrix konfiguriert wurden, muss eine Visualisierungsanzeige verfügbar sein, die den Status der Ursache-Wirkung-Matrix online wiedergibt.

15.3 Faceplates

Faceplates (Bildbausteine) müssen mit dem System für den Controller und die Überwachung von Regel- und diskreten Steueralgorithmen bereitgestellt werden.

Faceplates müssen die Anzeige der folgenden Informationen unterstützen (soweit zutreffend):

- Variablenkennung
- Variablenbeschreibung
- Prozesseingabe, Sollwert und Ausgabewerte in numerischer Anzeige mit physikalischen Einheiten
- Prozesseingabe, Sollwert und Ausgabe in Balkendiagrammdarstellung
- Automatische/manuelle Betriebsart und Status von lokalen Führungsgrößen (Sollwerte)
- Visuelle Anzeige des Alarmstatus
- Symbolische und alphanumerische Anzeige der diskreten Zustände von Geräten mit zwei oder mehreren Zuständen.

Faceplates müssen so konfiguriert werden, dass sie auf dem Bildschirm geöffnet werden, wenn die entsprechende Stelle in einem Prozessbild (z.B. ein Symbol) mit der Maus ausgewählt wird.

Regelung

Faceplates müssen dynamische Prozess- und Statusinformationen über einen einzelnen Regelkreis liefern. Es muss möglich sein, von einem Faceplate aus die folgenden Bedienaktionen durchzuführen:

- Ändern der Betriebsart des Regelbausteins (Control Block)
- Ändern des Sollwerts und anderer vom Operator einstellbarer Parameter
- Anpassen der Ausgaben in manueller Betriebsart

Diskrete Regelung

Einzelne Faceplates müssen für die Regelung und Anzeige von Geräten mit mehreren Zuständen bereitgestellt werden. Ein Motorventil muss beispielsweise "offen", "geschlossen", "Zwischenstellung" und "Fehler" anzeigen. Ein Operator muss

in der Lage sein, das Gerät vom Faceplate aus zu bedienen (Start, Stopp, Öffnen, Schließen).

15.4 Prozessgrafikanzeigen

Eine neue Grafik muss in Betrieb genommen werden können, ohne dass die Fähigkeit des Operators zum Bedienen und Beobachten der Anlage dadurch unterbrochen wird.

Alle Steuerungs-, Überwachungs- und Statusattribute jeder Variable müssen auf Bildern angezeigt werden können. Bei analogen Messwerten bezieht sich diese Anforderung unter anderem auf Messwert, Sollwert, Alarmgrenzwerte und Ausgabe. Bei digitalen Messwerten bezieht sich die Anforderung auf den Eingabe- und Ausgabestatus. Statusinformationen sind u.a. Alarmstatus, Betriebsart und Steuerstatus.

Numerische Daten müssen individuell konfigurierbar sein. Wird der Dezimalpunkt nicht verwendet, so muss er unterdrückt werden.

Es muss möglich sein, jeden Status eines Geräts mit mehreren Zuständen durch eine eindeutige Kombination von Vorder- und Hintergrundfarbe darzustellen.

Inaktive Alarm- oder Statusmeldungen für den Operator müssen ausgeblendet werden können.

Die symbolische Darstellung von Daten in Bildern muss durch Farbveränderungen (Vordergrund und Hintergrund unabhängig) und Blinken in jeder Kombination realisiert werden.

Das System muss die Programmierung von Tooltipps (kleine konfigurierbare Fenster mit Textinformationen für den Operator) unterstützen, die automatisch erscheinen, wenn der Operator mit der Maus über dem betreffenden Element verweilt.

Es muss möglich sein, einen Bildschirmbereich zu konfigurieren, über den andere Anzeigen aufgerufen werden.

Es muss dem Operator möglich sein, während der Laufzeit Zoom-Funktionen zu benutzen.

15.5 Erweiterte Prozessgrafiken

Anlagenleiter, Schichtleiter, Betreiber und Bediener müssen durch erweiterte Prozessgrafiken unterstützt werden. Diese sollen zu einer besseren Einschätzung von Situationen durch die Bediener beitragen und somit für einen sicheren und zuverlässigen Betrieb durch Bereitstellung von leistungsfähigen HMIs sorgen.

Neben der Einhaltung der Norm ISO 11064-5 über die Schaffung einer ergonomischen Umgebung für Bediener muss das System erweiterte Funktionen bereitstellen, wie in den Richtlinien EEMUA 201, ISA S201 (Entwurf) sowie in den Richtlinien des ASM Consortiums (Effective Operator Display Graphics Guidelines) detailliert beschrieben wird.

Anhand der erweiterten Prozessgrafiken müssen Bediener Unregelmäßigkeiten schnell erkennen können. Außerdem müssen sie klare Übersichten über den Status und die Leistung einer Anlage bieten.

Die ergonomische Gestaltung zugunsten der Bediener soll mit Hilfe folgender Funktionen verbessert werden:

- Analoganzeigen zur Unterstützung von Mustern wie vertikale und horizontale Balkendiagramme mit erweiterbaren Informationsfenstern

- Trendanzeigen mit ansteigenden bzw. abfallenden und flexiblen Achsen zum Beurteilen von Situationen und Entscheiden über die operative Vorgehensweise
- Darstellung von Informationen anstelle von Daten, z.B. anhand von Netzdiagrammen (Sterndiagramme) für KPIs und den Prozessstatus

15.6 Speicherung von Bildschirmaufteilungen als Favoriten

Das System muss dem Operator die Möglichkeit bieten, bestimmte Bildschirmaufteilungen oder Bildanordnungen (Layouts) zu speichern, so dass sie zu einem späteren Zeitpunkt wieder aufgerufen werden können. Ein derartiger „Favorit" könnte zum Beispiel ein Prozessbild sein, in dem Faceplates für bestimmte Geräte und bestimmte Trendanzeigen auf spezifische Weise am Bildschirm angeordnet sind.

15.7 Dynamisches Umschalten zwischen Sprachen

Das Bedien- und Beobachtungssystem muss einen einfachen Online-Wechsel zwischen Sprachen und internationalen Zeichensätzen bieten. Es muss mindestens zwischen Deutsch, Englisch, Französisch, Italienisch, Spanisch und Portugiesisch umgeschaltet werden können. Für diese Funktionalität dürfen keine Umprogrammierung, erneute Übersetzung oder Neukonfigurierung der HMI-Software-Anwendung erforderlich sein.

15.8 Zugriffskontrolle

Das Tool für die Konfiguration der Zugriffskontrolle muss eine bedienungsfreundliche, einfache Oberfläche aufweisen, welche die Microsoft Windows-Standardtechniken wie Kopieren, Ausschneiden und Einfügen sowie Drag-and-Drop voll unterstützt.

Das System muss die Möglichkeit bieten, die Berechtigung eines Bedieners im Rahmen der Steuerlogik-/Scripting-Anforderungen programmorientiert zu ändern und/oder zu verifizieren.

Die Systemsicherheit muss die Konfiguration von Berechtigungsgruppen mit Möglichkeit der Zuweisung einzelner Benutzer zu diesen Berechtigungsgruppen zulassen.

Das Tool für die Zugriffskontrolle muss die Konfiguration prozessbereichsspezifischer Sicherheit für bis zu 256 verschiedene Prozessbereiche zulassen.

Das System muss die Konfiguration von bis zu 999 kundenspezifischen Sicherheits- und Zugriffsberechtigungsstufen unterstützen.

Standardsicherheitsstufen

Die OS-Systemsicherheit muss verschiedene Sicherheitsstufen bereitstellen, um den Zugriff auf den Prozess und die Interaktion mit dem Prozess zu kontrollieren. Mindestens die folgenden Zugriffsstufen sollten vordefiniert sein:

- Benutzerverwaltung (User Administration)
- Ansicht von Alarmen und Aufruf von Anzeigen für einen bestimmten Bereich der Anlage
- Navigation durch das System
- Prozessüberwachung: Ansicht des Prozesses ausschließlich im Überwachungsmodus (Monitor Only)

- Prozesssteuerung (Basis): Steuerung des Prozesses durch Senden von Befehlen, Quittieren von Alarmen, Ändern von Sollwerten usw.
- Prozesssteuerung (erweitert): Ändern von Alarmgrenzwerten, PID-Tuning-Koeffizienten usw.
- Auslösen von Berichten
- Steuerung der Archivierung/Speicherung

Erweiterte Zugriffskontrolle

Die Operator-Schnittstelle muss den optionalen Einsatz von Chipkartenlesegeräten oder einer Maus mit Fingerabdruckerkennung (biometrische Identifikation) zur Sicherstellung der eindeutigen Identifizierung von Benutzern unterstützen.

Globale Sicherheit

Das System muss ein optionales allgemeines Sicherheitssystem mit Nutzung des gleichen Benutzernamens (Login) und Passworts für das Microsoft Windows-Betriebssystem, die Projektierungsumgebung, das HMI-System sowie das Batch-System unterstützen.

15.9 Erweiterungsfähigkeit

Das System muss in der Lage sein, Daten von mehreren Datenservern zu erfassen, unter anderem von anderen OPC-fähigen Prozess- und Leitsystemen.

Der Austausch von Systemdaten mit Drittanbieter-Software, die mit Microsoft Windows-Betriebssystemen kompatibel sind, muss möglich sein.

Das OS-System muss auf einer offenen Architektur basieren und die Erweiterungsfähigkeit durch Nutzung der folgenden Mittel unterstützen:

- COM/DCOM
- ODBC (Open Database Connectivity)
- OCX/ActiveX Controls
- OLE (Object Linking and Embedding)
- OPC (OLE for Process Control) Data Access Protocol (DA)
- OPC Historical Data Access Protocol (HDA)
- OPC Alarms & Events Protocol (AE)
- OPC Historical Alarms & Events (HAE)
- OPC UA

Die Funktionalität des OS-Systems muss unter anderem durch die folgenden optionalen Add-ons erweitert werden können:

- Benutzerprogrammierte ActiveX-Objekte
- Automatische ereignisgesteuerte E-Mail-Benachrichtigung mit Echtzeitinformationen
- Ereignisgesteuerte Anzeige von "Life"-Prozessbildern
- Langfristige historische mediengestützte Datenspeicherung
- Projektierbare Messenger-Funktionen wie SMS, E-Mail, Pager

16 Alarme, Ereignisse und Meldungen

16.1 Allgemein

Das Alarmsystem muss ein umfassendes Alarm- und Ereignismanagement mit benutzerdefinierbarer Meldungsstruktur bereitstellen.

Das Alarmsystem muss die Festlegung von bis zu 16 Meldungsunterklassen und 16 Meldungstypen unterstützen.

Alarmmeldungen müssen im Controller mit einem Zeitstempel gemäß Bearbeitungszyklus versehen werden.

Das Anbietersystem muss eine Zeitstempelauflösung von bis zu 1 ms für Binäreingänge unterstützen.

Das Alarmsystem muss Alarme über alle vom System festgestellten Zustandsänderungen ausgeben, unter anderem über:

- Jede Verletzung von Grenzwerten
- Jede Änderung des Zustands eines an das System angeschalteten Geräts und aller seiner Peripheriegeräte
- Die Störung eines vom System verwendeten Kommunikationskanals
- Die Störung von System-Hardware, die eine automatische Ersatzschaltung der Systemfunktionen vom aktiven Gerät auf das Reservegerät (Standby) zur Folge hat.

Das Alarmsystem muss Alarmmeldungen so anzeigen, dass der aktuelle Alarmzustand leicht ausgewertet werden kann, unter anderem durch folgende Mittel:

- Unterschiedliche Text- und Hintergrundfarbe für Punkte, für die ein Alarm gemeldet wird, für die ein Alarm quittiert wurde und für die kein Alarm mehr anliegt
- Blinken der aktuellen Alarmmeldung(en) in der Alarmliste
- Alarme, die automatisch, durch das System oder durch den Operator verborgen wurden
- Es muss die Möglichkeit geben, Alarme in zeitlich aufsteigender oder absteigender Reihenfolge anzuzeigen.

Das Anbietersystem muss ein projektierbares, OS-übergreifendes Hupenkonzept bereitstellen.

Das Anbietersystem muss automatische Alarmveroderung in der Anlagenübersicht ohne Zusatzprojektierung bereitstellen.

Das Anbietersystem muss mehr als 4 Alarmprioritäten und mehr als 5 Berechtigungsstufen unterstützen.

Das Anbietersystem muss den kommenden IEC 62682 Standard „Verwaltung von Alarmsystemen in der Prozess-Industrie“ erfüllen.

Das System muss das Anlagen einer detaillierten Hilfestellung zu einem Alarm ermöglichen. Damit kann die hinterlegte Fehlerbeschreibung mit einer Operatoraktion angezeigt werden.

Alarmquittierung

Das Alarmsystem muss die Möglichkeit der Quittierung einer Alarmmeldung bei dessen Auftreten und/oder Gehen bieten. Das System muss die Alarmquittierung unter anderem wie folgt ermöglichen:

- Für einen einzelnen Alarm von der Übersicht (Overview) aus
- Für eine gefilterte Alarmgruppe von einer Übersichtsliste (Summary List) aus
- Vom Faceplate (Standardbedienbild) für das Gerät aus
- Von einer Prozessanzeige aus (Bildschirmquittierung)

Die Alarmquittierung von einer Operator-Station aus muss automatisch mit den anderen Stationen synchronisiert werden, um die zentrale Quittierung sicherzustellen.

Bei Quittierungen von Alarmen muss der Bedienername gespeichert werden.

Das System muss die Möglichkeit bieten, über einen zweiten Tastensatz Meldungen zu sperren oder freizugeben.

Alarmfilterung

Das Alarmsystem muss die Möglichkeit der Filterung von Alarmen bieten, um das Verhalten der Alarmanzeigen zu steuern. Folgende Filterattribute müssen unter anderem verfügbar sein:

- Datum
- Uhrzeit
- Alarmklasse
- Alarmtyp
- Alarmpriorität
- Status (Alarm liegt an, Alarm liegt nicht an, quittiert)
- Variablenname
- Bereich

Symbole für den Alarmstatus

Das Alarmsystem muss die Möglichkeit der Verdichtung und Darstellung des Systemalarmzustands in Form eines Standardsymbols für den Alarmstatus bieten (d.h. Alarmgruppenanzeige). Die Gruppenanzeige muss den Status eines einzelnen Geräts oder eines ganzen Prozessbereichs wiedergeben können. Bei Darstellung des Status eines Prozessbereichs muss die Gruppenanzeige eine logische *OR-Verknüpfung* der Alarmzustände aller Geräte im Prozessbereich vornehmen.

Die Gruppenanzeige muss mindestens die folgenden Standardalarmkategorien umfassen, die im Symbol jeweils mit einer anderen Farbe und Textdarstellung darzustellen sind:

- Alarm
- Warnung
- Systemalarm
- Operator-Meldung (Operator-Maßnahme erforderlich)
- Unterdrückt (die Alarme werden unterdrückt)

16.2 Alarmprioritäten

Zur Unterteilung von Alarmen nach Schweregrad muss das System die Zuordnung individueller Alarmbedingungen zu einer von mindestens 16 unterschiedlichen Alarmprioritäten unterstützen.

16.3 Kategorisierung von Alarmen und Meldungen

Prozess- und gekennzeichnete Systemalarme müssen gemeldet, angezeigt und in Archivdateien gespeichert werden. Normale Operator-Aktionen, Ereignisse und normale Systemaktionen und -ereignisse müssen nicht als Alarme gemeldet werden, sind aber in zentralen Archivdateien abzulegen.

Alarme und Meldungen müssen so gruppiert werden, dass der Benutzer Alarme und Zustände in seinem Verantwortungsbereich einfach erkennen und darauf reagieren kann (z.B. in der Reihenfolge ihrer Priorität).

Bei Prozessalarmen muss der Operator die Möglichkeit haben, mit maximal einem Bedienschritt eine Anzeige aufzurufen, von der aus er Korrekturmaßnahmen ergreifen kann.

Das System muss die Möglichkeit der jederzeitigen Anzeige der aktuellsten Alarme mit der höchsten Priorität bieten.

Operator-Aktionen speichern

Das System muss alle Operator-Aktionen, die sich auf Prozesssteuerungsparameter oder die Alarmquittierung auswirken, automatisch in zentralen Archivdateien ablegen. Hierzu zählen unter anderem die folgenden Aktionen:

- Unterdrückung/Aktivierung/Quittierung von Alarmen
- Änderung der Betriebsart eines Reglers
- Änderung des Sollwerts eines Reglers
- Änderung von Alarmgrenzwerten
- Änderung von Abstimmparametern (Tuning)

Projektierungsaktionen speichern

Das System muss die Möglichkeit vorsehen, dass Projektierungsaktionen mit Auswirkung auf den Controller und Überwachung des Prozesses in einer Protokolldatei mit einem Kommentar gespeichert werden. Dies bezieht sich unter anderem auf die folgenden Aktionen:

- Download der Controller-Projektierung
- Online-/Test-Modus
- Download der Batch-/Operator-Station-Konfiguration

16.4 Auslösung von Prozessalarmen

Es muss möglich sein, Prozessalarme durch Konfiguration von Alarmattributen für jeden Prozess-E/A-Punkt oder jeden berechneten Punkt auszulösen.

Bei analogen Variablen müssen unter anderem die folgenden Auslöser (Trigger) für Prozessalarme konfigurierbar sein:

- Überschreitung der oberen Warengrenze (High Limit) für eine Prozessvariable
- Überschreitung der oberen Alarmgrenze (High High Limit) für eine Prozessvariable
- Unterschreitung der unteren Warengrenze (Low Limit) für eine Prozessvariable
- Unterschreitung der unteren Alarmgrenze (Low Low Limit) für eine Prozessvariable
- Abweichung einer Prozessvariable vom Sollwert
- Unzulässiger Wert einer Prozessvariable (schlechte Qualität)

Bei digitalen Variablen müssen unter anderem die folgenden Auslöser (Trigger) für Prozessalarme konfigurierbar sein:

- Spezifischer Zustand (0 oder 1)

Unterdrückung/Deaktivierung von Alarmen

Das System muss die Möglichkeit der Deaktivierung oder Unterdrückung von Alarmen auf folgenden Stufen bieten:

- Für jede einzelne Alarmbedingung
- Für alle Alarmbedingungen, die mit einem Gerät oder Punkt verknüpft sind
- Für alle Alarmbedingungen, die mit einer Alarmgruppe oder einem Prozessbereich verknüpft sind oder auf einer Prozessgrafik angezeigt werden.

16.5 Begrenzung von Störalarmen (Nuisance Alarms)

Um das Auftreten und die Belästigung eines Operators durch Störalarme zu begrenzen, muss das System die folgenden Leistungen für Identifizierung, Management und Unterdrückung anbieten:

Alarm Totband- und Chatter-Unterdrückung

Wenn ein Punkt schnell in einen Alarmzustand wechselt und diesen wieder verlässt, tritt ein Flattern *(Chattering)* eines analogen Eingangs auf. Um dieses zu minimieren, muss es konfigurierbare Hysteresen auf Basis einzelner Variablen geben.

Zur Minimierung des Auftretens von Störalarmen (Nuisance Alarms) beim Hochfahren/Herunterfahren muss das System die Unterdrückung von „Alarm Chatter" auf Steuerungsebene ermöglichen. Diese Funktion muss sicherstellen, dass Alarme beim HMI nicht erneut ausgelöst werden, bevor sie quittiert wurden.

Bildschirmanzeige zum Identifizieren von Störalarmen

Damit der Anlagenbediener Störalarme identifizieren kann, muss das System die Standardleistung bieten, eine Alarmmengenanalyse durchzuführen, welche solche Alarme findet, die während einer bestimmten Zeit am meisten aufgetreten sind.

16.6 Auslösung von Systemalarmen

Störungen einzelner Komponenten des Systems müssen die Generierung einer Alarmmeldung zur Folge haben. Ein Systemalarm muss bei Störung mindestens der folgenden Komponenten generiert werden:

- Feldgerät
- Einzelner E/A-Kanal
- E/A-Baugruppe
- E/A-Baugruppenträger
- Kommunikationsbaugruppen (Bus und Netz)
- Stromversorgungen
- Kommunikationsnetz
- Controller
- Server/Clients
- Historischer Archiv-Server
- Zeitsynchronisation

Alle an das Kommunikationsnetz des Systems angeschalteten Geräte müssen auf Fehler überwacht werden. Ein Systemalarm muss für jeden festgestellten Fehler generiert werden.

16.7 Archivierung von Prozess- und Systemalarmen

Alle Alarme müssen in Archivdateien abgelegt werden, die auf Wechselspeichermedien archiviert werden können. Es muss möglich sein, diese Alarme später nach wählbaren Filterkriterien in Listen anzuzeigen und auszudrucken.

Siehe auch Kapitel 23 "Historische Datenarchive".

16.8 Alarmsignalisierung

Das System muss in der Lage sein, Prozess- und Systemalarme unter anderem wie folgt zu signalisieren:

- Aktivierung eines externen akustischen Alarms oder einer Lampe
- Aktivierung der internen PC-Soundkarte (Wiedergabe von WAV-Dateien)
- Aktualisierung einer Alarmanzeige mit dem aktuellen Alarm
- Aktualisierung einer Alarmübersicht, um anzuzeigen, dass in einem bestimmten Prozessbereich/einem bestimmten Bild ein Alarm aufgetreten ist
- Ausdruck der Alarmmeldung auf einem Alarmdrucker
- Farbänderung, Formänderung, Einblenden oder Ausblenden eines grafischen Objekts, das mit dem Alarmpunkt verknüpft ist (je nach Konfiguration)

Akustische Alarmsignalisierung

Bei der Projektierung müssen alle Alarme für einen Prozessbereich einer beliebigen Operator-Station zugewiesen werden können. Alle Alarme müssen dann auf der bezeichneten Operator-Station (oder den bezeichneten Operator-Stationen) angezeigt werden. Der Benutzer muss die Möglichkeit haben, verschiedene Töne oder Tonmuster für die akustische Alarmsignalisierung zu konfigurieren. Ein eindeutiger Ton oder Klang muss auf Basis der Alarmpriorität, Meldungsklasse oder Prozessbereich generiert werden können.

Das System muss eine zentrale Alarmquittierung unterstützen: Quittierung und Stummschaltung des akustischen Alarms auf allen betroffenen Workstations durch eine einzige Quittierung auf einer beliebigen Workstation.

Optische Alarmsignalisierung

Alarme müssen eine optische Alarmsignalisierung nur bei einer bestimmten Operator-Station aktivieren, die für die betreffenden Alarme konfiguriert ist. Die Signalisierung muss innerhalb von 3 Sekunden nach Feststellung des auslösenden Ereignisses erfolgen. Es muss möglich sein, Prozessalarme ausschließlich von jener Operator-Station zu quittieren, die für die betreffenden Alarme konfiguriert ist. Ein Operator muss in der Lage sein, jeden für seine Station konfigurierten Alarm mit maximal zwei Bedienaktionen zu quittieren.

16.9 Alarmübersichtslisten

Das System muss die Möglichkeit der Anzeige einer Alarmübersichtsliste mit mindestens den folgenden Elementen bieten:

- Aktive Prozessalarme
- Beseitigte Prozessalarme
- Quittierte Prozessalarme
- Aktive Systemalarme
- Beseitigte Systemalarme
- Quittierte Systemalarme
- Journal (Alarmhistorie)
- Liste der Operator-Aktionen
- Unterdrückte (gesperrte) Alarme
- Gespeicherte (verborgene) Alarme
- Alarmfrequenzanzeige

Der Zugriff auf eine Alarmübersichtsanzeige von einem beliebigen anderen Bild aus darf nicht mehr als eine Bedienaktion erfordern.

Die sichtbare Anzeige eines Alarms darf nicht ausgeblendet werden, wenn der Alarm nicht quittiert wurde und wenn das Objekt, das den Alarm ausgelöst hat, nicht in den Normalzustand zurückgekehrt ist.

Mehrseitige Anzeigen können verwendet werden. In diesem Fall muss es möglich sein, mit einer einzigen Bedienaktion vor- oder zurückzublättern. Alarme müssen in Tabellenform in der Reihenfolge ihres Auftretens mit dem aktuellsten Alarm an oberster Stelle angezeigt werden.

Es muss möglich sein, Alarme gesonderten Bereichen der Anlage zuzuordnen, sodass eingehende Alarme zur Erstellung bereichsbezogener Ansichten in Bereichsmeldungslisten erfasst werden.

16.10 Intelligente (Smart) Alarmunterdrückung

Um die Alarmmenge für den Operator und die Darstellung von im Kontext bedeutungslosen Alarmen zu minimieren, muss das System ein intelligentes Alarmmanagement bieten bei dem bestimmte Alarme automatisch auf Basis des Auftretens von speziellen Prozess- oder Anlagenbedingungen verborgen werden können.

Bestimmen des Anlagenstatus oder der Prozessbedingung

Das System muss einen Standardfunktionsbaustein zum Bestimmen/Signalisieren von Änderungen des Anlagenstatus bzw. der Prozessbedingung innerhalb der aktiven Control-Strategie anbieten. Dieser Funktionsbaustein muss auch mit benutzerdefinierter Logik kombinierbar sein.

Konfiguration des intelligenten Alarm-Managements

Das System muss Werkzeuge und Leistungen bieten, um verborgene Alarme basierend auf Anlagenstatus oder Prozessbedingung zu konfigurieren. Die Konfigurationsschnittstelle soll ein Standardbestandteil des Engineering-Systems sein. Eine tabellenähnliche Applikation sollte über einfache Checkboxen die Einstellmöglichkeit bieten, anhand der Alarme ein- bzw. ausgeblendet werden können.

Aufzeichnen und Anzeige von verborgenen Alarmen

Verborgene Alarme sollen nicht in den Standardalarmanzeigen oder in der Prozessgrafik erscheinen. Das Auftreten dieser Alarme soll im Alarmjournal aufgezeichnet werden. Eine spezielle Anzeige, die dem Operator verborgene Alarme anzeigt, muss zur Verfügung stehen.

16.11 Verbergen von Alarmen

Damit Anlagenbediener bei Störungen (Alarmflut) effektiv reagieren können, muss das System die Möglichkeit bieten, einzelne individuelle Alarme oder Gruppen manuell und temporär zu unterdrücken. Ein zentraler einstellbarer Timer muss das Anstehen von Alarmen überwachen und ihn erneut zur Anzeige bringen, wenn die eingestellte Zeit abgelaufen ist. Eine umfassende Anzeige aller auf Basis der intelligenten Alarmunterdrückung und durch den Operator manuell gespeicherten und verborgenen Alarme muss zur Verfügung stehen.

16.12 Alarm-Management und Leistungsabfrage

Um die Leistung eines Operators in Bezug auf das Alarm-Management zu optimieren, muss das System folgende Standardleistungen bieten:

Konfiguration von Informationen für die Fehlersuche und Korrekturmaßnahmen

Das System muss die Konfiguration einer informativen Textmeldung für jeden Alarmzustand erlauben. Diese Textmeldung kann zum Anzeigen des möglichen Grunds und zur möglichen Korrekturmaßnahme genutzt werden. Diese Textmeldungen müssen in der Standardalarmliste angezeigt werden können.

Aufzeichnen von Alarmkommentaren

Das System muss Operator-Kommentare über das Quittieren eines Alarms zulassen. Dieser Kommentar muss in Verbindung mit dem Ereignis in der Alarmhistorie gespeichert werden können. Diese Kommentare müssen zu einem späteren Zeitpunkt gesichtet werden können. Um das Auffinden von kommentierten Alarmen zu vereinfachen, muss die Alarmhistorienanzeige markieren, welche Alarme einen Kommentar haben, und Sortier- und Filterfunktionen bieten.

Alarmmengenanzeigen

Um dem Anlagenbediener zu helfen, Störalarme zu identifizieren, muss das System die Standardleistung bieten, eine Alarmmengenanalyse durchzuführen, die solche Alarme findet, die während einer bestimmten Zeit am meisten aufgetreten sind.

Alarmdauer/Zeit bis zur Quittierung

Um dem Anlagenbediener zu helfen, die Alarmquittierungen laufend zu verbessern und das Anstehen von Alarmen zu reduzieren, muss das System eine Anzeige bieten, die die anstehende Zeit des aktiven Alarms und die Zeitdauer bis zur Quittierung auflistet.

16.13 Ereignisgesteuerte Kommunikation

Zur Minimierung der Kommunikationslast auf dem Systembus muss das System eine änderungsbasierte Kommunikation für die Übertragung von Alarmen und Ereignissen sowie für die Übertragung von Prozessdaten vom Leitsystem zur Operator-Schnittstelle verwenden.

17 Fehlersuche/Wartung und Systemdiagnose

Eine Online- und Offline-Diagnose muss zur Unterstützung der Systemwartung und Fehlersuche bereitgestellt werden. Diagnose muss für jede wichtige Systemkomponente und Peripherie wie u.a. Steuerungen, Clients, Server und Kommunikationseinrichtungen bereitgestellt werden. Ist keine Diagnose für bestimmte Peripheriegeräte wie z.B. Drucker und Endgeräte verfügbar, muss das System bei Störungen dieser Geräte eine Fehleranzeige erkennen und bereitstellen.

Es muss möglich sein, PROFIBUS-Geräte und HART-Geräte vom Leitstand aus zu überwachen und die Fehlersuche durchzuführen, ohne ins Feld zu gehen. Das System muss in der Lage sein, Kalibrierungsinformationen und die Gerätestatushistorie für jedes Feldgerät zu speichern. Der Upload von Feldgeräte-Projektierungsänderungen, die im Feld projektiert wurden, muss für das System möglich sein. Nach Speicherung der Projektierungsinformationen im System muss der Download dieser Informationen auf andere ähnliche (neue oder Ersatz-) Geräte möglich sein.
Das System muss die Problem-/Fehlerdiagnose des Kommunikationskanals ermöglichen.
Die OS muss eine Lebenszeichenüberwachung des Zustands aller Controller und OS-Komponenten bereitstellen und bei Feststellung einer Änderung eine Meldung generieren.

Wird ein Fehler bei einem Reservegerät festgestellt, muss der Operator benachrichtigt und der Fehler protokolliert werden.

17.1 Ereignisse

Alle durch das System generierten Ereignisse müssen erfasst und elektronisch in einer Ereignisdatenbank aufgezeichnet werden, chronologisch und auf Festplatte in einem oder mehreren Servern oder Einzelstationen.

Es muss möglich sein, Ereignisse nach Zeitpunkt (aufsteigende oder absteigende Reihenfolge) oder nach Typ abzurufen und zu sortieren.

Alle Systemereignisse müssen am Ursprungspunkt einen Zeitstempel erhalten. Ereignisse, die im Controller generiert werden, müssen den Zeitstempel dort erhalten. Ereignisse, die in der Workstation generiert werden, müssen den Zeitstempel in der Workstation erhalten.

Systemereignisse müssen so definiert sein, dass sie mindestens folgende Ereignisse umfassen:

- Statusänderung intelligenter Feldgeräte (z.B. Fehler, Wartungsbedarf)
- Kanalausfall (z.B. Kabelbruch)
- Störung von E/A-Baugruppen (z.B. Feststellung eines externen Baugruppenfehlers)
- Störung von Baugruppenträgern
- Störung von Kommunikationsbaugruppen
- Störung der Stromversorgung (z.B. Batterieausfall, Störung der 24-V-Quelle)
- Störung des Kommunikationsnetzes (z.B. Systembusfehler)
- Störung der Steuerung (z.B. Ersatzschaltungsereignisse)
- Server-Fehler (z.B. Redundanzverlust)
- Zustands- und Performance-Überwachung

17.2 System- und Diagnoseanzeigen

Online-Anzeigen müssen die Ergebnisse von Selbstdiagnoseprüfungen wiedergeben. Die Fehlerdiagnose muss so spezifisch sein, dass angezeigt wird, welche Komponenten, Baugruppen oder Geräte gestört sind. Die Anzeigen müssen so konzipiert sein, dass sie das Wartungs- und Technikpersonal bei der Diagnose von Fehlern im System und auf den Kommunikationswegen unterstützen. Jede Kategorie von Diagnoseanzeigen muss logisch so aufgebaut sein, dass daraus ihre Position in der Hardware-Architektur des Systems hervorgeht.

Bei der OS muss eine Anzeige verfügbar sein, die Auskunft über den Status aller Controller und OS-Komponenten gibt.

18 Asset Management und Maintenance-System

18.1 Geforderte Kernfunktionen

Das Maintenance-System muss folgende Kernfunktionen bereitstellen:

- Überwachung der Komponenten des Leitsystems
- Überwachung von technologischen Komponenten (z.B. Wärmetauschern, Ventilen)
- Überwachung von Anlagenkomponenten
- Erfassung der Identitäten der Assets
- Condition Monitoring (Zustandsüberwachung)
- Erfassung von Detaildiagnosen
- Schnittstelle zu Spezialistenwerkzeugen
- Generierung von Instandhaltungsanforderungen (auch vorausschauend)
- Bereitstellung der Maintenance-Daten für alle Assets in einheitlicher Struktur und Form für nachfolgende Bearbeitungsstufen
- Inbetriebsetzungsunterstützung
- Protokollierung von Ereignissen und Instandhaltungsmaßnahmen
- Controller-Ladeanalyse: Auslastung, Tasks, Alarm, wenn konfigurierbare Ladegrenzen überschritten wurden.
- Redundanter Status für den Terminal- und Anlagenbus
- Redundante Ein-/Ausgänge auf Kanalebene
- Hitliste für Asset-Alarme
- Durchgängige Asset-Kommentare kommen zur Anzeige auf der OS
- Einem Gerät können bis zu 10 Dokumente zugeordnet werden.
- Performance und Auslastungsauswertung müssen ohne zusätzliche Hardware-Kosten möglich sein.
- Das System muss kanalindividuelle Diagnose und Parametrisierung unterstützen.
- Diagnoseinformationen zum Netzwerk (Buslast, Bursts, Telegrammverluste usw.)

18.2 Geforderte Eigenschaften

Das Maintenance-System muss folgende Eigenschaften erfüllen:

- Branchenneutrales Paket
- Integriert ins Prozessleitsystem
- Engineering-Daten müssen ohne zusätzlichen Aufwand genutzt werden können.
- Es muss eine anlagenweite einheitliche Darstellung des Diagnose- und Instandhaltungszustands zur Verfügung stehen (mit einheitlichen Symbolen bzw. Icons).
- Feldgeräte aller Hersteller müssen integrierbar sein.
- Instandhaltungsinformationen und prozessrelevante Informationen müssen getrennt auswertbar sein.
- Alle Anlagenteile müssen einheitlich visualisiert werden können.
- Das "Look and Feel" der Bedienung soll dem des Prozesssystems entsprechen.
- Es soll eine Workflow-Optimierung von der Diagnose bis zum Abschluss der Instandhaltung möglich sein. Produktionsausfälle und Stillstandzeiten müssen minimiert werden können.
- Es muss eine durchgängige Unterstützung der zustandsbasierten Instandhaltung bereitstehen.
- Es muss eine zyklische Exportfunktion zum Speichern der Diagnosedateien für die Identifikationsdaten und Gerätezustände oder Geräteparameter und Gerätezustände (Field Device Management) verfügbar sein.

18.3 NAMUR

Das System soll auf nachfolgenden NAMUR-Empfehlungen basieren:

- NAMUR NE 91 Anforderungen an Systeme für anlagennahes Asset Management
- NAMUR NE 105 Anforderungen an die Integration von Feldbusgeräten in Engineering-Tools für Feldgeräte
- NAMUR NE 107 bzw. VDI/VDE/NAMUR/WIB 2650 Selbstüberwachung und Diagnose von Feldgeräten

Das Anbietersystem muss komponentenübergreifende und automatische Systemdiagnose- und Hilfefunktionen sowie eine rollenbasierte Asset-Bearbeitung (lesend, schreibend, Instandhalter, Spezialist) zur Verfügung stellen.

Für alle kritischen Anlagenteile wie Motoren, Pumpen, Antriebe, Messgeräte, Messwertgeber und Stellungsregler muss das System Werkzeuge und Dienste zur Verfügung stellen, die vorbeugende und vorausschauende Wartungsdienste ermöglichen.

18.4 Maintenance Station

Das System muss die Einführung einer geeigneten integrierten Maintenance Station erlauben, welche umfassende Wartungs- und Pflegeinformationen für alle Anlagenteile bereitstellen kann.

Die Maintenance Station muss die gleiche Bedienoberfläche bieten, die ein Standard-Operator-Bildschirm für die Prozessbeobachtung bietet.

Ein einheitlicher Satz Faceplates muss die Basisdiagnosedaten von allen Anlagenteilen anzeigen. Detaillierte Diagnoseanzeigen bieten auch folgende Darstellungen:

- Ein Online-Blick auf die Hardware-Konfiguration
- Ein Online-Blick auf ein intelligentes Feldgerät über das Feldgeräte-Management-Werkzeug.

18.5 Integriertes Plant Asset Management-System

Das System muss ein integriertes Asset Management-System für die folgenden Anlagenteile bieten:

- Messwertgeber und Stellungsregler
- Motoren, Pumpen und Antriebe
- Messgeräte
- PCs (Server, Clients, Historians usw.)
- PLS-Hardware (Controller, E/A-Bausteine usw.)
- Netzwerkausrüstung (Switches usw.)
- Anlagenausrüstung (vom Benutzer definierbar)

Das integrierte Asset Management muss folgendes unterstützen:

- Konfiguration und Auslesen von Feldgeräte-Parametern über HART oder Fieldbus (PROFIBUS-DP/PA, Foundation Fieldbus H1, HART und PROFINET)
- Unterstützung einer großen Auswahl an Feldgeräten und Hinzufügen von neuen Feldgeräten
- Unterstützung eines üblichen User Interface, unabhängig vom Feldgeräte-Hersteller
- Unterstützung der Inbetriebnahme von Geräten
- Unterstützung von Prüfungsketten und Änderungsprotokollen
- Unterstützung der grafischen Darstellung von Geräte-Parametern (Trendanzeigen etc.)

18.6 Automatische Generierung der Asset Management

Das System muss die Asset Management-Datenbank automatisch aus dem Anwendungsprogramm und der Hardware-Konfiguration erstellen können. Es dürfen für die Asset Management-Konfiguration keine zusätzlichen Eingaben notwendig sein.

Faceplates und Symbole müssen automatisch innerhalb des Bediensystems erstellt werden, um dem Anlagenpersonal das einfache Darstellen und Beobachten des Leistungsverhaltens der Anlagenteile zu ermöglichen. Für die Beobachtung von Asset-Alarmen müssen spezielle Summendarstellungen angeboten werden.

18.7 Zustands- und Performance-Überwachung

Oft ist es notwendig, verschiedene prozessbedingte, chemische und mechanische Bedingungen für das Wartungskonzept einer Anlage zu berücksichtigen. Deshalb muss das System die Möglichkeit der Zustandsüberwachung anbieten, welches den Benutzer automatisch über Grenzüberschreitungen bei kritischen Anlagenteilen (wie Pumpen und Kugellager) informiert.

Standardfunktionsbaustein für das Beobachten von benutzerdefinierten Anlagenteilen und Bedingungen

Das System muss einen Standardsatz von Funktionsbausteinen und Faceplates anbieten, welches für die Beobachtung (Zustand und Performance) von benutzerdefinierten Anlagenteilen geeignet ist. Das System muss benutzerdefinierte Logik verbunden mit aktuell gemessenen Werten unterstützen, um die Leistung von kritischen Anlagenteilen wie einem Wärmetauscher (Verschmutzung) und Pumpen (Leistungsverbrauch, Ableitungen von charakteristischen Kurven usw.) überwachen zu können.

Der Status der benutzerdefinierten Anlagenteile muss in der Maintenance Station neben den automatisch durch das System erzeugten Status angezeigt werden können. Informations- und Statusanzeigen müssen durch einen einfachen Satz von Faceplates und zusammenfassenden Listen auswertbar sein.

Das Prozessautomatisierungssystem muss eine erweiterte Leistungsüberwachung und die Evaluierung von Pumpen und Ventilen bereitstellen, damit eine vorbeugende Wartung durchgeführt werden kann und die Folgen eines Geräteausfalls vermieden werden können.

Für Pumpeneinheiten müssen die folgenden Funktionen verfügbar sein:

- Anzeige und Analyse der Betriebsleistungsdaten (Durchfluss, Druck, elektrische und mechanische Leistung und Effektivität)
- Grenzwertüberschreitung von Leistungswerten (mechanisch und elektrisch)
- Überlastungsschutz (hohe Durchflussrate)
- Kavitations- oder Gasfördererkennung
- Schutz vor blockiertem Rotor und Trockenlauf
- BOP- (Best Operating Point) und Abweichungsanalyse
- Abweichungen von der Sollwertanalyse
- Pumpenverschleiß über einen gewissen Zeitraum
- Statistische Daten (Stunden in/außer Betrieb)

Die Funktion muss für Einheiten mit fester als auch variabler Drehzahl verfügbar sein.

Für Regelventile müssen die folgenden Funktionen verfügbar sein:

- Statistische Daten (maximale Anzahl an Stunden ohne Bewegung/Stunden im Dauerbetrieb/zulässige Richtungsänderungen)
- Überwachung der Reaktionszeit von Ventilen
- Erkennung von Bewegungen ohne Einschaltbefehl

- Verlagerung der oberen und unteren Endposition
- Bestimmung der verbleibenden Steuerabweichung
- Spezifizierung von Stützpunktkoordinaten

Für Strömungsnetz-Komponenten wie z.B. Pumpen, Filter, Wärmetauscher und Rohrleitungen müssen folgende Funktionen verfügbar sein:

- Anzeige und Analyse von Betriebs-Messdaten (Durchfluss, Druck, Flüssigkeitsgrad, elektrische und mechanische Leistung und Effizienz) einschließlich der Visualisierung von:
- Charakteristische Kurven
- Aktueller Betriebspunkt
- Druckabfall abhängig von Durchfluss und Flüssigkeitsgrad

Die Konfiguration der erweiterten Leistungsüberwachung hat über die Engineering-Station des Prozessautomatisierungssystems im manuellen und selbstlernenden Betrieb zu erfolgen.

18.8 Dokumenten-Management

Das System muss ein Dokumenten-Management-System bereitstellen. Es muss das Speichern und Anzeigen von bis zu 10 verschiedenen Dateien (DOC, PDF, MPG, AVI usw.) pro Gerät zulassen. Damit muss man Informationen wie Standardablaufprozeduren, Verdrahtungspläne, P&IDs oder Hilfedateien aus der zentralen Maintenance Station beziehen können.

19 Chargenprozesse

19.1 Allgemein

Der Anbieter muss ein Chargensystem mit nachfolgenden Funktionen bereitstellen:

- Konformität mit S88 Teil 1 und 3
- Das System muss für PLS-, Chargen- und Sicherheitsanwendungen entworfen sein. Es muss Hochgeschwindigkeitsanforderungen erfüllen können.
- Das System muss die nahtlose Integration von kontinuierlicher Steuerung, Chargensteuerung (Batch Control) und Sicherheitsschutzsteuerung einschließlich einheitlichen Software Tools vorsehen.
- Das System muss in Anlagen jeder Größe einsetzbar sein, skalierbar vom Einplatzsystem bis zur verteilten Client-Server-Architektur, für Rezeptsteuerungen in kleinen bis großen Anwendungen.
- Das System muss mit modularem Aufbau und flexibler Skalierung an die jeweiligen Anforderungen optimal anpassbar sein.
- Rezeptgesteuerte Chargenprozesse müssen sich wirtschaftlich realisieren lassen.
- Das System muss auch eine Chargenprozessautomatisierung über einen Batch-Server und mehrere Batch-Clients, die zusammen ein Anlagenprojekt bearbeiten, ermöglichen.
- Das System muss rezeptgeführte Fahrweisen unterstützen.
- Komplexe Aufgaben mit wechselnden Steuerungsabläufen müssen einfach und flexibel bearbeitet werden können.
- Batch-Namen müssen leicht mithilfe vordefinierter und dynamischer Komponenten erstellt werden können.
- Batch-Server-Stationen müssen bei Bedarf redundant auslegbar sein.
- Das System muss ein optionales allgemeines Sicherheitssystem mit Nutzung des gleichen Benutzernamens (Login) und Passworts für das Microsoft Windows-Betriebssystem und das Batch-System unterstützen.
- Die Projektierungsaktion: Download der Batch-/Operator-Station-Konfiguration muss in einer Protokolldatei mit einem Kommentar gespeichert werden.
- Das System muss die Durchführung von Änderungen an der Projektierung von Batch online ohne Betriebsunterbrechung unterstützen.
- Das System muss Batch-Berichte mit integrierten Trendanzeigen bereitstellen.
- Batch-Änderungen im Rezept dürfen nur nach Rücknahme der Freigabe ausgeführt werden können.
- Die Batch-Bildbausteine müssen das gleiche Aussehen und die gleiche Handhabung besitzen wie die des Leitsystems.

19.2 Nahtlose Integration

- Das Batch-System soll voll im Anbietersystem integriert sein.
- Die Anlagendaten müssen komplett über das Engineering-System projektiert werden können.
- Alle für die Rezepterstellung notwendigen Daten müssen vom Engineering-System an den Batch-Server übergeben werden.
- Die Trennung zwischen Rezeptbearbeitung und Engineering-System muss vom System unterstützt werden.
- Projektierungsänderungen müssen vom Engineering-System per Update-Funktion (Online/Offline) auf den Batch-Server übertragbar sein.
- Das Batch-System muss mit den Controllern über die Anbieter-OS kommunizieren.
- In die Kommunikation müssen sich auch Operator-Anweisungen und -Dialoge integrieren lassen.
- Alle herkömmlichen Projektierungsaufgaben (Controller, OS, Batch, Historie), die Feldbusprojektierung (Transmitter, Antriebe, Analysatoren usw.), die Datenbankgenerierung und die Editierung müssen auf einer einzigen Engineering-Workstation ausgeführt werden können. Es muss jedoch auch möglich sein, mehrere Engineering-Workstations gleichzeitig für diese Arbeiten einzusetzen.

19.3 Basis-Software-Paket

Das Basic-Paket muss mindestens 10 Teilanlagen unterstützen und folgende Funktionen bieten:

- Das Control Center ist die "Kommandozentrale" für die Überwachung und Steuerung von Chargenprozessen. Es muss alle relevanten Daten über eine grafische Bedienoberfläche verwalten. Komfortable Auftrags- und Chargenplanung muss ebenso möglich sein wie die grafische Darstellung der Teilanlagenbelegung.
- Eine Überwachungs- und Steuerzentrale für Chargenprozesse
- Der Rezepteditor muss zum einfachen, intuitiven Erstellen und Modifizieren von Grundrezepten und Bibliotheksoperationen verwendet werden können.
- Das System muss über eine grafische Bedienoberfläche, Microsoft Windows typische Bearbeitungsfunktionen für einzelne und gruppierte Objekte sowie eine strukturelle Syntaxprüfung verfügen.
- Basis für die Rezepterstellung bilden die Batch-Objekte aus der Batch-Anlagenprojektierung mit dem Engineering-System z.B. Teilanlagen und technologische Funktionen.
- Der Batch-Rezepteditor muss einzeln gestartet werden können, muss aber auch vom Control Center aus aufrufbar sein.
- Das Basispaket muss sich einfach erweitern lassen. Für den Ausbau der Client-Server-Konfiguration mit weiteren Batch-Clients müssen Optionspakete verfügbar sein.
- Single Station, Batch Clients und Batch Server müssen mit Hilfe von Optionspaketen zudem funktionell erweitert werden können.

19.4 Optionale Zusatzfunktionen

- Das System muss zusätzliche Planungsfunktionalität durch eine vorausreichende Chargenplanung ermöglichen. Chargen müssen eingeplant, geändert, storniert, gelöscht und freigegeben werden.
- Das System muss eine hierarchische Rezeptstruktur gemäß S88 unterstützen:
- Rezeptprozedur für die Steuerung des Prozesses bzw. der Produktion auf Anlagen
- Teilrezeptprozedur zur Steuerung einer Prozessstufe auf Teilanlagen
- Rezeptoperation/Rezeptfunktion zur Erfüllung der verfahrenstechnischen Aufgaben/Funktionen auf technischen Einrichtungen
- Das System muss eine Anwenderbibliothek für Rezeptoperationen zur Verfügung stellen. Diese müssen zentral verwaltet und geändert werden können.
- Das System muss eine Trennung zwischen Prozedur und Formula zulassen. Eine durch teilanlagenneutrale Rezepte erreichte Flexibilität muss weiter erhöht werden können, indem man Prozedur und Parametersätze (Formulas) voneinander trennt.
- Verschiedene Grundrezepte müssen sich durch Verknüpfen mehrerer Formulas mit einer Rezeptprozedur erstellen lassen. Zentrale Prozeduränderungen müssen möglich sein.
- Die Struktur der Formula muss durch die vom Anwender definierte Formulakategorie bestimmt werden können.
- Zur Programmierung spezieller branchen- und projektspezifischer Applikationen muss eine offene Schnittstelle für Erweiterungen enthalten sein.
- Der Import von Rezepten, die in der Beschreibungssprache Batch Markup Language (BATCHML) definiert sind, muss unterstützt sein.

19.5 Erweiterungen

- Arithmetische Ausdrücke zur Berechnung in Phasenparametern und Transitionen.
- Textvergleich in Transitionen
- Eine Versionsverwaltung: Unterstützt werden sollen Master-Rezepte, ROP-Bibliotheken, Rezepte mit voreingestellten 2 Ziffern.
- Produktdaten müssen in Rezepten genutzt werden können.
- Roaming User, d.h. benutzerspezifische Einstellungen werden von einem Bedienplatz zum anderen übernommen.
- Sprachoberfläche direkt online umschaltbar
- Integration von Wegesteuerung
- Das System muss für Batch-Anwendungen Soft- und Hardware-Redundanz bieten.
- Rezeptbezogene Beschränkungen können zusätzlich zu den Gerätebeschränkungen in den Phaseninstanzen definiert werden, ebenso die Überprüfung dieser Grenzen bei der Eingabe des Operators.

19.6 Belegungsstrategien

Das Batch-System muss benutzerdefinierte Belegungsstrategien unterstützen:

- Prozessparameter
- Am längsten nicht benutzt. Die am längsten nicht benutzte Teilanlage wird belegt.
- Operatorauswahl
- Bedingungen
- Belegungsänderung bei laufender Charge. Diese muss nach Chargenstart und vor der Teilanlagenbelegung noch möglich sein.

19.7 Elektronische Unterschrift

Für den gesamten Lebenszyklus eines Rezepts (siehe auch Kapitel 26 Elektronische Aufzeichnungen/Elektronische Unterschriften) sowie für Chargensteuerungsschritte (wie Starten, Stoppen, Abbrechen, Löschen, Kommentieren usw.) muss vom Batch-System die elektronische Unterschrift möglich sein. Diese elektronische Unterschrift muss ein wesentlicher Bestandteil der Standardsystemfunktion sein. Überdies muss sie einfach zu konfigurieren sein und mehrere Unterschriften mit konfigurierbaren Signierrollen und -sequenzen umfassen.

20 Charge (Alternative)

Für zahlreiche Industrien und Anwendungen führt die Einhaltung der Anforderungen der Norm ISA S88 und der Bestimmung 21 CFR Teil 11 der FDA zu einer Entwicklungslösung, die für die Anwendung möglicherweise nicht wirtschaftlich ist. Im Folgenden wird eine alternative Anforderungsspezifikation aufgeführt für Chargenprozesse, die weniger komplex und in vielen Fällen ausreichend sind.

Das Prozessautomatisierungssystem muss eine Standardanwendungsstruktur zur Verwaltung der folgenden Punkte bereitstellen:

- Materialien
  - Pflege der Materialstammdaten
  - Handhabung und Nachverfolgung der Materiallosdaten
  - Verwaltung von Materialstatus, -verbrauch, -eingang, -bestand
- Parameter (oder Rezepte)
  - Rezeptpflege
- Aufträge
  - Auftragslisten
  - Auftragsbearbeitung
  - Auftragsstatusübersicht
  - Auftragsabschlussprotokoll
- Archive
  - Speicherung und Verwaltung von Bestell-, Material- und Rezeptdaten

21 Materialtransport und Wegesteuerung

Der Anbieter soll die Möglichkeit der PLS-Erweiterung um ein branchenneutrales System zur Projektierung, Steuerung, Überwachung und Diagnose von Materialtransporten in Rohrleitungsnetzen anbieten.

21.1 Allgemein

Die Wegesteuerung muss folgende Funktionalität zur Verfügung stellen:

- Bedienen von einfachen Transportwegen bis zu komplexen Wegenetzen
- Automatische Wegesuche für Transporte von Materialien in Anlagen und Tanklagern.
- Konfiguration, Kontrolle, Beobachtung und Fehlerdiagnose von Materialtransport in Rohrleitungsnetzen.
- Verwendung in Anlagen mit vielen komplexen Wegekombinationen oder umfangreichen Tanklagern
- Bedienen von Anlagen mit zahlreichen Leitungswegen mit hoher Flexibilität

21.2 Projektierung

Die Wegesteuerungsprojektierung muss auf der Basisprojektierung des Prozessleitsystems mit Bausteinen aus der Standardbibliothek des Anbieters basieren. Bestehende Anlagen müssen einfach mit der Wegesteuerung erweitert werden können.

Das System muss Projektierungskomponenten anbieten:

- Bibliothek mit einheitlichen Schnittstellenbausteinen zur Konfiguration
- Assistent als Schnittstelle zwischen Wegesteuerungsprojektierung und Prozessleitsystem-Basisprojektierung
- Engineering-Tool für die einfache Projektierung von Wegen, Teilwegen und Eigenschaften

21.3 Architektur

Wegesteuerung muss die Basis-Hardware des Prozessleitsystems nutzen können.

Bei kleinen Anlagen müssen Operator-System und Wegesteuerung auf einem Einplatzsystem kombiniert werden können.

Die Wegesteuerung muss Client-Server-Konfigurationen ermöglichen, ausbaubar mit bis zu 32 Wegesteuerungs-Clients je Server.

Das Control Center für die Wegesteuerung muss auf einem OS-Client oder einem Batch-Client installiert werden können, muss aber auch als separater Wegesteuerungs-Client konfigurierbar sein.

Das Wegesteuerungs-Engineering muss im Engineering-Toolset des zentralen Engineering-Systems des Anbieters integriert sein.

21.4 Wegesteuerung im Betrieb

Zum Bedienen, Visualisieren und Diagnostizieren von Materialtransporten müssen folgende Runtime-Komponenten zur Verfügung stehen:

- Wegesteuerung-Bausteinsymbol (Status eines Weges, z.B. Handbetrieb, Fehler usw.)
- Wegesteuerung-Faceplate (Bedienen und Beobachten für einen Weg)
- Wegesteuerung-Center (Bedienen und Beobachten für alle Wege)

21.5 Maintenance in der Wegesteuerung

Servicepersonal muss beim Wegesteuerungssystem die Möglichkeit haben, das Automatisierungssystem in den "Maintenance"-Zustand zu versetzen. Neue Materialtransporte sind dann gesperrt.

21.6 Fehlertoleranz

Das Wegesteuerungssystem muss fehlertolerante (Failsafe) und nicht fehlertolerante Automatisierungssysteme unterstützen. Entsprechende Wegesteuerungs-Bibliotheksfunktionen sind bereitzustellen.

21.7 Betriebssystem

Das Wegesteuerungssystem muss auf Microsoft Windows oder einem Microsoft Windows Server Betriebssystem lauffähig sein.

21.8 Engineering-Station

Das System muss die Konfiguration des Wegesteuerungsservers über die zentrale Engineering-Station unterstützen. Hierbei müssen Assistenten die Generierung der bezeichneten Kommunikationsverbindungen unterstützen.

21.9 Materialänderung

Das System muss die Möglichkeit bieten, Material in einem aktiven Materialtransport manuell zu ändern. Spezielle Materialeigenschaften müssen eingestellt werden können.

21.10 Systemsicherheit Wegesteuerung

Das System muss zur Systemsicherheit das Lesen/Schreiben von verteilten Microsoft Windows-Verzeichnissen nur für bestimmte Wegesteuerungs-benutzergruppen zulassen können. Das Attribut "Everyone" ist nicht zulässig.

22 Prozesssimulation

Ein Prozesssimulator ist als Unterstützung für Folgendes erforderlich:

- Prozess- und Operationalitätsanalyse zur Verbesserung der Anlagensicherheit
- Evaluierung von abnormalen Prozesszuständen und Gerätestörungen (vor und nach einem Ereignis)
- Testen der Notfallüberwachung und des Notfallschutzes
- Analyse beim Hochfahren/Herunterfahren
- Optimierung operativer Verfahren
- Bedienerschulung (auch vor der Inbetriebnahme)
- Umfassende werkseitige Geräteprüfung und Controller-Voreinstellung
- Verbessern und Testen der vollgrafischen Bedieneranzeigen

Der Simulator muss folgende Punkte erfüllen:

- Er muss den Prozess kontinuierlich simulieren können. Außerdem muss die Möglichkeit bestehen, Feldein- und -ausgaben, Feldinstrumente und das Prozessautomatisierungssystem zu simulieren.
- Er muss die ursprüngliche Controller-Logik der Anlage anhand Soft-SPS, die in einer Microsoft Windows-Umgebung laufen, emulieren können.
- Er muss die Projektierung und den Download der Controller-Logik in die Emulation anhand des eigentlichen PLS-Entwicklungssystems unterstützen. Außerdem müssen die Diagnosefunktionen des eigentlichen PLS-Entwicklungssystems genutzt werden können.
- Er muss das Szenarien-Management unterstützen. Szenarien müssen im Simulator erstellt, gespeichert, geladen, bearbeitet und aktiviert werden können.
- Er muss Echtzeit-, Einzelschritt- und Rückverfolgungsbetriebsarten bereitstellen und er muss zu einem beliebigen Zeitpunkt gestartet und gestoppt werden können.
- Er muss die Integration von Simulatoren von Fremdanbietern für komplexe Geräte oder Prozesse unterstützen.
- Er muss verschiedene Simulationsebenen (vollständig, teilweise, vereinfacht) gemäß den Anforderungen unterstützen.
- Er muss die Durchführung von Firmware Update der angeschlossenen HW, das Ändern von Namen, IP-Adresse, Subnetzmasken und den Import von GSD und GSDML Dateien ermöglichen.
- Er muss die redundante PROFINET Konfiguration R1 und den Prozess Alarm PROFINET unterstützen.

Der Simulator muss sich vollständig in die Geräte des Prozessautomatisierungssystems integrieren lassen, d.h. insbesondere in Komponenten wie HMI, Kommunikationsbusse, Automatisierungskomponenten. Dadurch sollen verschiedene Simulationsebenen ermöglicht und eine nahezu reale Umgebung für den Benutzer geschaffen werden.

Der Simulator muss die eigentlichen Bedienoberflächen und die grafische Anzeige der Anlage nutzen.

Der Simulator muss mit der virtuellen Steuerlogik des Prozessautomatisierungssystems als auch mit realen Controllern arbeiten. Das System muss demnach vorhandene Architekturinformationen importieren können, um doppelte Datenerfassung und Fehlermöglichkeiten zu vermeiden.

Die Logik- und Prozesssimulation sowie die damit verbundene Emulation müssen eine logische Validierung ermöglichen, was auch als virtuelle Inbetriebnahme bezeichnet wird.

Das vorhandene Know-How eines Verfahrenstechnikers oder Automatisierungstechnikers muss für eine schnelle umfassende Einarbeitung ausreichen. Spezielle Simulationskenntnisse dürfen nicht erforderlich sein.

Das Simulationssystem muss auf einem PC-basierten System mit Microsoft Windows-Betriebssystem laufen.

22.1 Simulation des Controllers

Ein Controller Simulation Tool zur Simulation von Feldeingaben und -ausgaben innerhalb der Regelungslogik und zur Erleichterung der Prüfung und Fehlersuche beim Controller-Programm muss verfügbar sein. Es darf keine Controller- oder E/A-Hardware erfordern und muss für die Simulation sowohl von Chargen- als auch von kontinuierlichen Prozessen verwendet werden können. Besondere Modifikationen des eigentlichen Controller-Programms zum Zweck der Ausführung im Simulationsmodus dürfen nicht erforderlich sein.

22.2 Simulation von dezentralen E/A- und Profibusgeräten

Das System muss die Nutzung von Karten unterstützen, die in der Lage sind, die tatsächlichen elektrischen Signale und Rückmeldungen von Remote-E/A-Stationen und Profibusfeldgeräten an einen realen Controller zu simulieren.

Die zu simulierenden Feldgeräte müssen aus der Hardware-Konfiguration der Anlage importiert werden können.

Die Simulation der PROFIBUS DP/PA-Teilnehmer muss rückwirkungsfrei auf die Controller durchgeführt werden können, d.h. die Controller erkennen nicht ob simulierte oder echte Feldgeräte über den Bus kommunizieren.

Das System muss Fehlersimulation am PROFIBUS erlauben. Hierzu gehören:

- Stationsausfall
- Modulausfall
- Kanal- und Leitungsdiagnose

Das System muss die Simulation von Aggregaten durch vorgefertigte Bibliotheken und editierbare Software-Funktionen anbieten (Schrittketten, Verriegelungen, DP-Redundanz).

Die Simulation muss den Test von virtuellen Feldgeräten (am PROFIBUS DP/PA) ohne mechanische Belastung oder Gefährdung der realen Installation erlauben.

22.3 Prozessmodellierung

Zur Modellierung der Prozessdynamik muss das System die Nutzung höherer Prozesssimulationsprogramme unterstützen. Diese Programme müssen das tatsächliche Controller-Programm zur Entwicklung des Modells (Maximierung der Wiederverwendung) nutzen können (mit Export/Import der Hardware-Konfigurations- und Signalschnittstellendaten).

Die Controller-Simulation muss mit verschiedenen Kommunikationsanschaltungen (OPC usw.) kommunizieren können. Hierfür muss der Anbieter vorgefertigte, frei programmierbare Bibliotheken zur Verfügung stellen können.

Die Simulation muss das Modellieren von prozesstechnischen Zusammenhängen mit skalierbarer Detailgenauigkeit ermöglichen und mit nachfolgender Funktionalität unterstützen:

- Drag-and-Drop-Modellierung auf grafischer Oberfläche
- Integrierte Mathematik
- Komponentenbibliotheken mit definierbaren Eigenschaften
- Gleichungsorientierte Modellierung
- Makrokomponenten
- Teilmodelle
- Dynamische Grafiken und Animationen

Das System muss den Ablauf in Echtzeitsimulation ermöglichen. Eine Realzeitsynchronisierung muss möglich sein.

Modellierte Szenarien müssen wiederverwendbar gespeichert werden können. Die Wiederverwendbarkeit soll durch eine integrierte Verwaltung einfach anwendbar sein.

Das Simulationssystem muss den Anschluss an eine Prozessvisualisierung unterstützen. Der Simulationsablauf muss visualisierbar und animierbar sein.

Das System muss Simulationsanalysen mit Protokollen, Kurven und Meldungen unterstützen.

Software-Änderungen müssen unabhängig von der realen Anlage getestet werden können.

Die Simulation muss auf Prozessebene, Geräteebene (Stellglied /Messfühlerebene) und Signalebene möglich sein.

23 Behandlung historischer Daten

Ein integriertes System zur Verwaltung historischer Daten mit Funktionen zur Unterstützung von Folgendem ist erforderlich:

- Erfassung von Prozesswerten, Alarmen, Ereignissen und Batch-Daten
- Nachbearbeitung (Mittelwert, maximaler/minimaler Wert, Änderungsrate, Datenverdichtung, Filterung)
- Archivierung
- Abfrage und Visualisierung
- Berichte
- Systemprojektierung

Das System muss Daten gemäß einer konkreten Projektkonfiguration erfassen können. Zudem muss es rechtzeitig auf Datenabfrageanforderungen reagieren, ohne dabei die Datenerfassung zu beeinträchtigen oder sonstige Leistungseinbußen zu bewirken.

Benutzer müssen auf Daten zugreifen können, ohne dass dafür Fachkenntnisse des Prozessautomatisierungssystems oder andere Personen erforderlich sind.

Das System muss die Möglichkeit bieten, jede beliebige Variable im Prozessautomatisierungssystem auszuwählen, der Archivierung hinzuzufügen und dafür zu konfigurieren. Variablen, die im Prozessautomatisierungssystem konfiguriert oder geändert werden, müssen automatisch und ohne zusätzliche Projektierung im System für die Verwaltung historischer Daten angezeigt werden.

Das System für die Verwaltung historischer Daten muss die folgenden zwei Subsysteme umfassen:

- Kurzfristiges Subsystem: Eine lokale Komponente, die auf dem HMI-Server ausgeführt wird, um Daten vom Prozessleitsystem aufzuzeichnen
- Langfristiges Subsystem: Der eigentliche Historian, der auf einer dafür vorgesehenen Maschine ausgeführt wird, der Daten vom kurzfristigen Subsystem erhebt und archiviert

Sowohl das kurz- als auch das langfristige Subsystem müssen ein relationales Microsoft SQL-Datenbankmanagementsystem (RDBMS) in Echtzeit zur Speicherung aller prozessrelevanten Informationen nutzen.

Das kurzfristige Subsystem ist Teil des HMI-Servers und muss Clients (HMI, OPC DA Client, OPC A&E Client usw.) historische Daten des Prozessautomatisierungssystems in folgender Form bereitstellen:

- Trends
- Alarm- und Ereignislisten
- Batch-Daten

Das kurzfristige Subsystem muss einfach konfigurierbar sein und die Bearbeitung von zu archivierenden Daten, Archivraten, Archivtypen usw. unterstützen.

Die Projektierung des kurzfristigen Subsystems wird vom langfristigen Subsystem automatisch übernommen.

Das langfristige Subsystem muss sämtliche Aktivitäten verwalten, um einen kontinuierlichen Zugriff auf Archivdaten, solange Bedarf besteht, zu gewährleisten. Das langfristige Subsystem kann über eine Schnittstelle mit höherrangigen Systemen

(z.B. MES) sowie mit anderen Systemen, die Prozessautomatisierungs-Systemdaten benötigen, verbunden werden.

Es darf unter keinen Umständen möglich sein, dass Benutzer Datenzugriff auf das Datennetzwerk des Prozessautomatisierungssystems, auf Server oder das Automatisierungssystem usw. über das langfristige Subsystem erhalten.

Die HMI kann Daten des kurz- und langfristigen Subsystems auf unterschiedliche Art und Weise, wie etwa in Form von Trends und Tabellen, anzeigen:

23.1 Archivierungskapazität

Das Konfigurations-Tool für die Archivierung muss die Möglichkeit bieten, Archivierungsraten in Sekunden-, Minuten-, Stunden- oder Tagesschritten festzulegen.

Der Historian muss über eine Funktion zur Archivierung von Werten einschließlich u.a. folgender Werte verfügen:

- Ist-Wert
- Maximaler Wert
- Minimaler Wert
- Summe
- Mittelwert

Der Historian muss die Möglichkeit bieten, digitale Werte entweder auf einer Anstiegs- oder auf einer Abfallflanke zu archivieren.

Eine Teilanlage kann mit archivierten Werten verknüpft werden.

23.2 Datenbankkapazität

Das System muss die Archivierung von bis zu 80.000 unterschiedlichen Variablen pro HMI-Server unterstützen.

Ein historischer Archiv-Server muss die Archivierung von bis zu 120.000 unterschiedlichen Variablen unterstützen.

Der Historian muss mindestens 5.000 Werte pro Sekunde kontinuierlich archivieren können.

Um den Speicherbedarf der Archive auf ein Minimum zu begrenzen, muss ein Datenkompressionsalgorithmus verfügbar sein.

23.3 Sicherung/Wiederherstellung der Historian-Datenbank

Das System muss Werkzeuge für die Sicherung der Datenbank auf Wechselspeichermedien oder an einem alternativen Speicherplatz zur Verfügung stellen. Das Sicherungsdienstprogramm (Backup Utility) muss in der Lage sein, die Datenbanksicherungen auf Basis eines der folgenden konfigurierbaren Kriterien auszuführen:

- Nach einem bestimmten Zeitplan (z.B. jede Woche)
- Das System muss das komplette Speichern und Zurückspielen von historischen Datenbanken in einer Datei unterstützen.

23.4 Redundanz

Das System muss die Nutzung redundanter historischer Archive mit Unterbringung der Archivdatenbank auf getrennten Servern unterstützen.

Redundante historische Archive müssen automatisch synchronisiert werden, wenn der Partner wieder in Betrieb genommen wird.

Kein Datenverlust: Wurde die Verbindung zwischen dem Historian und dem HMI-Server aus einem beliebigen Grund unterbrochen, werden die Daten kontinuierlich auf dem HMI-Server gespeichert (lokales Speicherungs- und Übermittlungsprinzip). Nachdem die Verbindung wiederhergestellt wurde, werden alle fehlenden Daten vom HMI-Server automatisch wiederhergestellt.

23.5 Verbindung zu Fremdsystemen

Das System muss die Verbindung zu Fremdsystemen unterstützen über:

- OPC UA-Server
- MQTT Cloud-Anschluss

24 Trendanzeigen

Jede Operator Workstation (OS-Client) muss Ansichten von Echtzeit- und historischen Trendinformationen bereitstellen. Daten, die in einem Historian-Paket erfasst sind, müssen auf allen Workstations verfügbar sein. Das System muss eine zentralisierte Methode für die Erfassung historischer Daten unterstützen.

Das System muss benutzerdefinierte Trends unterstützen, sodass häufig betrachtete historische Informationen einmalig in Trends festgelegt werden können und dann durch Auswahl eines vorkonfigurierten Bildschirmobjekts auf der grafischen Oberfläche einfach aufgerufen werden können. Die Anzahl der Trends, die definiert werden können, darf keinen praktischen Begrenzungen unterliegen. Jedes Trendbild muss bis zu 8 unterschiedliche Kurven unterstützen. Punkte, die angezeigt werden sollen, müssen menügesteuert ausgewählt werden können.

Historische Trends müssen die nahtlose Integration von Echtzeit- und historischen Daten in einem einzigen Trendfenster mit nahtloser Bewegung zwischen beiden unterstützen. Wandert das Bild nach links, werden historische Werte aus Dateien mit den historischen Daten abgerufen. Wird die Trendanzeige weit genug nach rechts gefahren, so sind die aktuellen Echtzeitdaten zu sehen, die gerade erfasst werden.

Vergrößern/Verkleinern (Zoom in/out) und zeitliches Vorwärts-/Rückwärtsfahren müssen mit nicht mehr als zwei Bedienaktionen möglich sein. Ein Mechanismus für die Auswahl eines Punkts auf dem Trend, z.B. eine Leselinie mit Ausgabe der numerischen Werte der Trends zu diesem Zeitpunkt, muss bereitgestellt werden.

Es muss möglich sein, neue historische Trends aufzurufen und online über die OS zu konfigurieren.

Vorkonfigurierte Echtzeittrends müssen verfügbar und leicht verwendbar sein.

Es muss möglich sein, die Daten eines aktuell gezeigten Trends zu exportieren (CSV-Datei) und mit MS Excel anzuzeigen.

25 Berichte

Das Prozessautomatisierungssystem muss ein integrales Berichtssubsystem für Berichte über aktuelle und archivierte Daten bereitstellen.

Dieses Berichtsubsystem muss Standarddarstellungstechniken (Baum-/Listenansichten) für das Management und die Verwaltung von Berichten nutzen.

Das Berichtsubsystem muss die Festlegung von Berichten sowohl für die Bildschirmanzeige (Visualisierung) als auch für den Ausdruck ermöglichen. Berichtvorlagen (Report Templates) müssen bereitgestellt werden, die angepasst oder unverändert übernommen werden können.

Das Berichtsubsystem muss die Möglichkeit bieten, einzelne Berichte im Rahmen der Steuerlogik-/Scripting-Anforderungen programmorientiert zu ändern und/oder zu nutzen.

Das Berichtsubsystem muss die Festlegung sowohl dynamischer als auch statischer Berichte ermöglichen, unter anderem mit:

- Berücksichtigung von archivierten Daten, Alarmdaten oder Ereignisdaten
- Kundenspezifischer Anpassung von Format, Layout und Bildern, die in den Bericht eingefügt werden
- Konfiguration der automatischen Generierung von Berichten mit Angabe des Zeitpunkts oder Ausgabezyklus und einer Liste von alternativen Ausgabegeräten für den Fall, dass Probleme bei der automatischen Erstellung auftreten

Die Anzahl der Berichte, die konfiguriert werden können, darf durch das Berichtsubsystem nicht begrenzt werden.

Das System muss den Einsatz optionaler Drittanbieteranwendungen (d.h. Microsoft Excel, Crystal Reports) zur Generierung von Berichten unterstützen.

Generierung von Berichten

Es muss möglich sein, alle Berichte sowohl auf dem Bildschirm einer Workstation anzuzeigen als auch auf einem Berichtdrucker auszudrucken. Stündliche, tägliche, monatliche, Monatsend-, vierteljährliche und jährliche Berichte müssen unterstützt werden.

Berichte müssen ausgedruckt und/oder auf Festplatte gespeichert werden, wenn ein Prozessereignis auftritt. Es muss möglich sein, Berichte auf folgende Weise anzustoßen:

- Auf Anforderung (Operator-Anforderung)
- Nach Zeitplan (Schicht, täglich und monatlich)
- Bei Auftreten eines Ereignisses

Berichtsvorlagen

Das Berichtsubsystem muss unter anderem mit den folgenden vorkonfigurierten Berichten bereitgestellt werden:

- Dokumentation grafischer Anzeigen
- Historische Archivierung
- Alarmarchivierung

Reportgenerierung

Das Berichtsubsystem muss beim Exportieren XML und MS HTML-Formate unterstützen.

26 Elektronische Aufzeichnungen/Elektronische Unterschriften

26.1 Allgemeine Anforderungen

Das System muss den Zugriffsschutz und die Datenintegrität anhand folgender Komponenten unterstützen:

Zugriffskontrollen: Das System muss den Zugriff auf befugtes qualifiziertes Personal beschränken. Die Verwaltung von Benutzern, Benutzergruppen und Benutzerrechten muss in Form einer zentralen Benutzerverwaltung erfolgen.

Datenintegrität: Das System muss die Möglichkeit der Aufzeichnung von Daten und der Erkennung von geänderten Aufzeichnungen bieten. Integrierte Prüfungen auf eine korrekte und sichere Handhabung von Daten sollten für manuell eingegebene Daten sowie für mit anderen Systemen elektronisch ausgetauschte Daten bereitgestellt werden.

Aufbewahrung von Aufzeichnungen: Das System muss die Möglichkeit der Aufbewahrung, des Schutzes und des Abrufens von Aufzeichnungen während der gesamten Aufbewahrungsfrist bieten. Systeme müssen elektronische Aufzeichnungen sowohl in für den Menschen lesbarer als auch in elektronischer Form reproduzieren können.

26.2 GMP-Anforderungen

Neben den zuvor erwähnten allgemeinen Anforderungen muss das System den Anforderungen des GAMP5-Leitfadens der ISPE, den GMP-Richtlinien der EU und der Bestimmung 21 CFR Teil 11 der FDA entsprechen.

Die Datensicherheits- und Datenintegritätsmerkmale müssen den seitens der Bestimmung 21 CFR Teil 11 geforderten Kontrollen zum Schutz von elektronischen Aufzeichnungen entsprechen:

Validierung: Das System muss eine für die Systemvalidierung geeignete Entwicklungsdokumentation unterstützen, um eine präzise, zuverlässige und konsistente Datenaufbereitung in Übereinstimmung mit den Normen sicherzustellen.

Prüfungsketten: Für elektronische Aufzeichnungen müssen sichere, computergenerierte, mit einem Zeitstempel versehene Prüfungsketten genutzt werden. Anhand dieser werden Datum und Uhrzeit von Einträgen und Vorgängen des Bedieners unabhängig aufgezeichnet Außerdem werden durch diese elektronische Aufzeichnungen erstellt, geändert oder gelöscht. Änderungen an Aufzeichnungen dürfen zuvor aufgezeichnete Informationen nicht unkenntlich machen.

Elektronische Unterschriften: Das System muss Maßnahmen bieten, anhand derer sichergestellt werden kann, dass die Nutzung einer elektronischen Unterschrift ausschließlich auf den rechtmäßigen Eigentümer beschränkt wird und dass Versuche einer Nutzung durch andere Personen umgehend erkannt und aufgezeichnet werden. Nicht biometrische Systeme müssen zwei eindeutige Identifikationskomponenten (z.B. Benutzerkennung und Passwort) bereitstellen, die beim Leisten der Unterschrift einzugeben sind. Für spätere Unterschriften innerhalb derselben Sitzung muss mindestens das Passwort erneut eingegeben werden. Das System muss Maßnahmen beinhalten, anhand dieser die Fälschung von elektronischen Unterschriften mit Hilfe von Standardwerkzeugen verhindert werden kann.

27 Virtualisierung

Das Prozessautomatisierungssystem muss die Virtualisierung von OS-Servern, OS-Clients und Engineering-Systemen auf Grundlage von VMware ESXi bereitstellen.

Der Anbieter muss Die Virtualisierungsumgebung, die Virtualisierungs-Hardware zum Hosten der Fremd-Software umfasst, muss vom Anbieter getestet und zugelassen worden sein.

Es muss die Möglichkeit bestehen, mehrere virtualisierte Maschinen unterschiedlicher Typen in einer angemessen dimensionierten Computer-Hardware auszuführen. Berechnungsrichtlinien müssen die Dimensionierung der Host-Hardware ermöglichen.

Virtualisierte Maschinen müssen von auf separater Hardware laufenden Thin Clients aus ausführbar sein.

Virtualisierte Maschinen müssen möglichst unabhängig von der Host-Hardware sein und eine einfache Migration in neue Hardware und einen Schutz gegen Veralterung bieten.

Es muss die Möglichkeit der zentralen Verwaltung virtualisierter Maschinen bestehen sowie u.a. eine allgemeine Wartung sowie die Durchführung von Installationen, Upgrades und Backups.

Die zentrale Überwachung der Hostsystemleistung muss möglich sein (Betriebszustand, Arbeitsspeicher-, CPU-, Festplatten- und Netzwerkauslastung).

Die Konfiguration realer oder virtualisierter OS-Server und OS-Clients muss gegenüber realen oder virtualisierten Engineering-Stationen transparent erfolgen.

Der Betrieb virtualisierter Maschinen aus Sicht des Bedieners darf sich nicht vom Betrieb realer Operator-Clients und -Server unterscheiden. Jegliche Beschränkungen bzw. Einschränkungen sind eindeutig zu definieren.

Host-Maschinen sind in ein Sicherheitskonzept, d.h. Patches, aufzunehmen.

28 Erweiterte Prozessregelungen Advanced Process Controls

Das System muss auch komplexe Regelungsalgorithmen unterstützen, wie:

- Selbstoptimierende Regelungen
- Modellprädiktiver Regler (MPC) 10x10x10
- Adaptive Regler (feed forward/backward)
- Virtuelle Sensorik (Softsensoren oder virtuelle Online-Analyser) für nicht direkt messbare Mengen
- Unterstützung einer externen Verarbeitung mit Matlab/Excel
- Fuzzy-Regelungen

29 Technologische Objekte

Standardisierte technologische Objekte (STO) müssen für die Automatisierung von gängigen industriellen Komponenten und Anwendungen verfügbar sein. Zu den technologischen Objekten zählen u.a.:

- Software-Objekt für die Steuerung
- Integrierte Alarme und Meldungen
- Bildbausteine des Operator-Systems zur Steuerung und Überwachung (sowohl für Operator-Clients als auch für lokale Bedienelemente)
- Funktionelle Dokumentation

Der Zweck der STOs besteht darin, die Entwicklung benutzerspezifischer Anwendungen hinsichtlich zahlreicher Standardaufgaben zu senken und somit die Implementierung, Inbetriebnahme sowie Testdauer und -kosten bei gleichzeitiger Erhöhung der Systemzuverlässigkeit zu reduzieren. Das "Look and Feel" der STOs muss den Operatoren ähneln.

STOs müssen für Folgendes verfügbar sein:

- Die meisten Ventiltypen (Absperr-, Drossel-, Rückschlag-, Entlastungs-, Kugel-, Kegel-, Regelventile usw.)
- Antriebe (DOL, Stern-Dreieck, Umkehrung, Dahlander, Softstarter, variable Drehzahl, Stellungsregler usw.)
- Messwerte (analoge Messungen, polygone Kurvenanpassung, Interpolierung, erweiterte Beschränkungen/Niveaus usw.)
- Heiz-, Entlüftungs- und Klimamodule (Berechnung der Heizleistung, abgestrahlten Energie, Enthalpie, Feuchtigkeit, Sättigungsfeuchtigkeit und Umrechnungsfunktionen)
- Zeitplanungsprogramme (Timer, Aggregatumschaltung, externe Auslösung)
- Mathematik (Mittelwertbildung, Filterung, Akkumulatoren)
- Tolerante Hierarchien für dezentrale Anwendungen (mehrstufige Toleranz, Multi- oder Parallel-Steuervorgänge usw.).

30 Verbindungen mit anderen Systemen und Fernzugriff

30.1 Unterstützung von Verbindungen mit Drittanbietersystemen

Das System muss in der Lage sein, unter Verwendung der folgenden Schnittstellen und Protokolle mit Leitsystemen von Drittanbietern zu kommunizieren:

- OPC
- PROFIBUS
- Foundation Fieldbus (FF)
- Ethernet (z.B. Modbus TCP)
- Serielle Schnittstelle (z.B. Modbus RTU), RK512, 3964R

30.2 Serielle Schnittstelle

Die folgenden Möglichkeiten müssen für die Kommunikation mit zusätzlichen Systemen (Hilfssystemen) verfügbar sein:

- RS-232C, RS-422 und RS-485 mit Full-Duplex- und Half-Duplex-Betrieb und wählbaren Baudraten (19200, 38400, 57600 und 115200)
- IEEE 802.3 Ethernet-Protokoll mit 10 oder 100 Mbit/s und TCP/IP
- Modbus, in einer Master-Slave-Beziehung konfiguriert, mit dem System als Master und dem zusätzlichen System als Slave

30.3 OPC-Schnittstelle

Das System muss in der Lage sein, mittels OPC bidirektional mit zusätzlichen Systemen zu kommunizieren. Die OPC-Schnittstelle muss in einer Client-Server-Beziehung konfiguriert sein und das System muss je nach Anforderung als OPC Client oder OPC Server arbeiten können.

Das Anbietersystem muss über OPC-Standard-Schnittstellen DA, HDA, AE, HAE oder OPC UA Zugriff auf Werte, Alarme und Ereignisse bieten. OPC UA Prozesswerte können mit einem Schreibschutz versehen werden.

Das Schreiben von kundenspezifischem Code zur Einrichtung der OPC-Schnittstelle darf nicht erforderlich sein. Die Konfigurierung von OPC muss mit Hilfe von Drag-and-Drop-Funktionalität zur Verknüpfung der Datenquelle und des Ziels möglich sein.

Die OPC-Schnittstelle muss mindestens eine Zykluszeit von 500 ms und 1 s unterstützen.

Die Schnittstelle muss den Durchsatz von 10.000 Variablen/Sekunde bearbeiten können.

30.4 Verbindung mit Enterprise-Systemen

Das System muss Schnittstellen zu ERP-Systemen (wie z.B. SAP) unterstützen, wobei für diese Verbindung optionale IT Software-Module entsprechend den Normen 62264/ISA S95 eingesetzt werden müssen. Die folgenden optionalen IT-Module müssen mindestens verfügbar sein:

- Production Scheduling
- Asset/Maintenance Management
- Material Management
- Historical Records/KPI Management
- Compliance Management

IT-Module müssen eine Plug-in-Architektur unterstützen, durch die ein Framework für die Verbindung zwischen dem Prozessautomatisierungssystem und dem ERP/MES-System bereitgestellt wird.

Das System muss Funktion wie „elektronisches Chargenprotokoll-Management“ für MES-System zur Verfügung stellen.

30.5 Sicherheit mit Netzkomponenten

Beim fernbedienten Zugriff über LAN auf ES oder Controller muss der Anbieter maximale Sicherheit gewährleisten. Über eine spezielle Netzwerkkomponente muss der Datenverkehr zwischen internem und externem Netzwerk kontrolliert werden können.

Für eine erhöhte Übertragungssicherheit und Transparenz wird ein Virtual Private Network (VPN) Tunnel gefordert.

Zwischen Sicherheitsmodulen wird ein verschlüsselter Datenverkehr gefordert.

Das Anlagennetzwerk muss hohe Performance und Standby-Redundanz bieten. Es wird die Leistung eines Gigabit Backbones benötigt. (SCALANCE X414-3E):

30.6 Wägesysteme

Das System muss eine integrierbare Wägetechnik mit aufwandarmem Engineering anbieten.

30.7 Videointegration

Das System muss eine Videointegration anbieten.

30.8 Fernzugriff

Der Fernzugriff auf das System per Modem (DSL oder ISDN) zu Zwecken der Fehlersuche muss möglich sein.

Der Benutzer muss in der Lage sein, diese Funktion zu deaktivieren, ohne das Modem abzuschalten.

31 Elektrizitätsversorgungssysteme

Das Prozessautomatisierungssystem muss sich in Elektrizitätsversorgungssysteme entsprechend dem Protokoll nach IEC 61850 mittels des Manufacturing Message Protocol (MMS) und Generic Object Oriented Substation Events (GOOSE) integrieren lassen.

Basiert das Elektrizitätsversorgungssystem auf dem FMS/PROFIBUS DP-Standard, muss die Möglichkeit der Integration von IEDs unter Anwendung dieses Standards möglich sein.

Das System muss die intelligenten elektronischen Geräte (IEDs) des Elektrizitätsversorgungssystems, die das Protokoll nach IEC 61850 unterstützen, überwachen und regeln können. Die Automatisierung der Geräte muss möglich sein, jedoch ist das System nicht für Hochgeschwindigkeits-Schaltvorgänge ausgelegt.

IEDs sind u.a. vom Typ:

- Schutzrelais
- Elektronische Sensoren
- Leistungs-, Qualitäts- und Phasenmessung
- Messsysteme (auf Umsatz bzw. nicht auf Umsatz ausgerichtet)
- Fehlerregistrierapparate

Das Prozessautomatisierungssystem muss mit IEDs anderer Anbieter kompatibel sein.

Das Prozessautomatisierungssystem muss über Vorlagen für OS-Clients für die gängigsten IEDs verfügen. Bediener müssen IEDs von den OS-Clients aus visualisieren und steuern können.

Der OS-Server muss mit Standard-Firmware, Treibern und/oder Lizenzen ausgestattet sein, die für die Kommunikation mit den IEDs auf Grundlage des Protokolls nach IEC 61850 notwendig sind. Die historische Archivierung von Elektrizitätsinformationssystemen hat über eine Standard-Software zu erfolgen, die lediglich projektiert werden muss.

Speziell für die Konfiguration der Funktionalität des Elektrizitätsversorgungssystems ist eine Engineering-Station bereitzustellen. Hinsichtlich der allgemeinen Funktionen des Elektrizitätsversorgungssystems (z.B. Einspeisung, Motor, Generator, Transformator, Leitung) sind technologische Funktionsbausteine zu Entwicklungs- und Visualisierungszwecken (Überwachung und Betrieb) bereitzustellen und homogen in das System zu integrieren.

Das Prozessautomatisierungssystem muss die redundante Kommunikation mit den IEDs unterstützen. Überdies hat die Anbindung des Kommunikationssystems über Lichtwellenleiterkabel zu erfolgen, die eine höhere EMV-Immunität in störanfälligen Umgebungen mit elektrischer Energie aufweisen.

Die Zeitsynchronisation ist bei IEDs kritisch. Daher muss das Prozessautomatisierungssystem sämtliche IEDs innerhalb von 1 ms synchronisieren können.

Es muss die Möglichkeit der Automatisierung von IEDs anhand einer Automatisierungskomponente des Prozessautomatisierungssystems bestehen. Der Controller des Automatisierungssystems muss über sämtliche Vorlagen und Funktionsbausteine verfügen, die für die Anbindung an die und die Kommunikation mit den IEDs erforderlich sind.

Energie-Management

Das System muss die energieintensiven Verbraucher und Prozesse identifizieren können, um Maßnahmen zur Verbesserung der Energieeffizienz abzuleiten.

Das System muss Funktionen für Last-Management bereitstellen, um Lastspitzen vermeiden zu können.

32 Fernwirkeinrichtungen

Das Prozessautomatisierungssystem muss die Integration von Fernbedienungsterminals (RTUs) auf Grundlage eines oder mehrerer Standard-Fernwirkübertragungsprotokolle (IEC 60870-5-101, IEC 60870-5-104, DNP3 oder Modbus RTU) unterstützen.

Vernetzungstypen

Die Vernetzung des Systemsteuerungs-Centers mit den Out-Stations erfolgt über ein WAN (Wide Area Network). Es müssen unterschiedlichste Netzwerktypen und Betriebsmodi, einschließlich IP-basierte Netzwerke, unterstützt werden:

- Dedizierte Leitungen (Kupfer- und Lichtwellenleiterkabel)
- Private Drahtlosnetzwerke
- DFÜ-Netzwerke (analog, ISDN)
- Drahtlose Ethernet-Verbindung
- Industrial Wireless LAN (IWLAN)
- Lichtwellenleiter, z.B. durch Verwendung von
- Schaltern mit optischen Ports
- Mobilen Diensten (E)GPRS oder UMTS
- Öffentlichen oder privaten IP-Netzwerken

Das Fernwirksystem muss die folgenden Merkmale haben:

- Möglichkeit der flexiblen Konfiguration von Netzwerken mit beliebiger Topologiekombination (Stern-, lineare Bus- und Teilnehmertopologie)
- Redundante Kommunikation
- Unterstützung von RTU zu Hilfskommunikationswegen der Master Station über unterschiedliche Kommunikationswege und -protokolle
- Ein RTU kann mit mehreren Master-Stationen gleichzeitig über verschiedene Übertragungsprotokolle und -wege kommunizieren
- Peer-to-Peer-Kommunikation zwischen RTUs

Fernwirkanwendung

Sämtliche kommunizierten Daten sind am Ursprungsort mit einem Zeitstempel zu versehen. RTUs müssen die Zeitsynchronisation durch das Prozessautomatisierungssystem und von lokalen GPS-Uhren automatisch unterstützen. Die Umschaltung zwischen Sommer- und Standardzeit hat bei Bedarf automatisch zu erfolgen.

Die folgenden Datenübertragungsmodi müssen möglich sein:

- Allgemeine Abfrage (anlauf- oder benutzerinitiiert)
- Zyklisch initiiert vom Master-Gerät
- Spontan
- Ausgeglichene oder unausgeglichene Kommunikation
- Datenpriorisierung

RTUs müssen sämtliche Standardfunktionen für die Verarbeitung von analogen Daten zur Senkung des Telemetriedatenverkehrs einschließlich Hysterese von Absolutwerten und Änderungsgeschwindigkeitswerten umfassen.

Das Prozessautomatisierungssystem muss über passende Vorlagen auf Client- und Server-Ebene verfügen, die fernwirkspezifischen Baugruppen auf RTU-Ebene entsprechen. Vorlagen müssen für Prozessobjekte wie Motoren und Ventile sowie für Meldungen und Messwerte einschließlich den entsprechenden Trends verfügbar sein.

Fernsteuerung und Fernbetrieb müssen konfigurierbar sein, um Konformität mit operativen Sicherheitsverfahren einschließlich entfernten/lokalen/manuellen/automatischen Verriegelungen zu ermöglichen. Es muss die Möglichkeit bestehen, die Schaltbefugnis zwischen unterschiedlichen Master-Stationen zuzuweisen.

Engineering

Eine einheitliche Engineering-Plattform ist anhand des Engineering-Systems des Prozessautomatisierungssystems zur Konfiguration der Fernwirkkomponenten bereitzustellen. Es muss die Möglichkeit bestehen, vom Engineering-System aus RTUs zu konfigurieren und Wartungsvorgänge auszuführen, wenn das Engineering-System vom selben Anbieter wie das Prozessautomatisierungssystem stammt. Die Konfiguration von RTUs und die Ausführung von Wartungsvorgängen müssen ohne Unterbrechung der RTUs möglich sein.

Die Prozessautomatisierung muss über Standardvorlagen und Funktionsbausteine verfügen, die für die meisten Prozessobjekte nur die Konfiguration erfordern. Außerdem müssen neue Benutzerbausteine erstellt werden können.

Datensicherheit

Das Fernwirksystem muss über umfassende Funktionen zur Verhinderung von Datenbeschädigung und -verlust verfügen.

IP-basierte Netzwerke sind anhand dedizierter VPN-Lösungen und Firewalls zu schützen.

Für den Fall, dass die Kommunikation per Fernwirksystem unterbrochen werden sollte, muss der RTU mit einer lokalen Datenrahmen-Pufferspeichertechnologie für die kontinuierliche Datenaufzeichnung ausgestattet sein. Anhand dieser Technologie können fehlende Daten nach der Wiederherstellung der Kommunikation vollständig übertragen werden.

33 Industrielle Sicherheit

Alle Prozessautomatisierungssysteme müssen mit umfassenden technischen Sicherheitsfunktionen ausgestattet sein, um folgendes zu verhindern: das unbefugte bzw. unerwünschte Eindringen, die beabsichtigte bzw. unbeabsichtigte Beeinträchtigung des ordnungsgemäßen bzw. vorgesehenen Betriebs oder den zweckwidrigen Zugriff auf Informationen einschließlich Computer, Netzwerke, Betriebssysteme, Anwendungen und andere programmierbare und konfigurierbare Komponenten des Systems.

Das System sollte eine Kombination aus diversen möglichen Gegenmaßnahmen, die sich mit Gefährdungen der industriellen Sicherheit befassen, sowie Folgendes zulassen:

- Authentifizierung von Benutzern, Gruppen und/oder Computern
- Zugriffskontrollen
- Digitale Unterschriften
- Protokollierungsmechanismen
- Scannen auf schadhafte Software
- Sicherheits-Patchen von Software
- Nutzung von Whitelisting-Mechanismen
- Überwachung der Systemaktivität
- Sicherer Fernzugriff
- Physikalische Sicherheit

33.1 Verwendung von "Defense in Depth"-Architekturen

Ein ganzheitlicher Systemansatz ist auf Grundlage unterschiedlicher Schutzebenen bereitzustellen, was auch als "Defense in Depth" bezeichnet und in der Norm IEC 62443 beschrieben wird. Hierzu zählen u.a.:

- Anlagensicherheit
    - Betriebliche Sicherheit
    - Physikalische Verhinderung des Zugriffs auf kritische Komponenten durch unbefugte Personen
- Netzwerksicherheit
    - Überwachte Schnittstellen zwischen involvierten Netzwerken, z.B. durch Firewalls
    - Zulassen der Netzwerksegmentierung und von Sicherheitszellen
    - Sichere Kommunikation
- Systemintegrität
    - Malware-Erkennung und -Vermeidung (z.B. Antiviren- und Whitelisting-Software)
    - Wartungs- und Aktualisierungsprozesse, Patch Management
    - Account Management (z.B. Benutzerauthentifizierung für Bediener)
    - Integrierte Zugriffsschutzmechanismen in Automatisierungskomponenten

33.2 Netzwerkarchitektur

Es muss die Möglichkeit bestehen, das Prozessautomatisierungssystem entsprechend dem Zonen- und Leitungssystem zu projektieren, wie in der Norm IEC 62443-1-1 und der Bestimmung 21 CFR Teil 11 der FDA beschrieben.

Das System muss über diverse Produkte für die industrielle Sicherheit zur Bildung von Zonen und Leitungen verfügen:

- Netzwerkmodule mit integrierten Firewalls, Portfilter, NAT/NAPT, DHCP-Server, konfigurierbar wie im Routing-, Switch- oder Bridge-Modus, Stateful Inspection, Denial of Service (DoS)-Schutz und Bandbreitenbegrenzung
- VPN-Verschlüsselung muss unterstützt werden
- Verschlüsselte Kommunikation auf dem Terminalbus soll voreingestellt sein
- IPsec-Tunnel müssen für die Kommunikation zwischen Zonen unterstützt werden

Das System soll eine klare Abgrenzung zwischen dem geschützten internen Netzwerk (Prozessleitsystem LAN) und den ungeschützten oder nicht vertrauenswürdigen externen Netzwerken bieten. Schnittstellen, sofern vorhanden, zum Office-IT-System und das Intranet/Internet unterliegen eindeutig definierten Sicherheitsmechanismen und können dementsprechend überwacht werden.

33.3 Sichere Netzwerkzugangspunkte

Einsatz von Firewalls

Um den selektiven Datenverkehr zwischen Netzwerkzonen (Subnetzen) oder von einem Netzwerk zu einem Gerät zu blockieren, soll das System den Gebrauch von Firewalls unterstützen. Für den optimalen Schutz müssen in den Firewalls Regeln erstellt werden können, die den notwendigen Zugriff mit den folgenden Techniken unterstützen:

- Paketfilterung
- IP-basierte Regeln
- MAC-Adressen-basierte Regeln
- Port-basierte Regeln
- Stateful Inspection
- Netzwerküberwachungs- und Protokollierungsmechanismen

Unterstützte Firewalls

Mindestens eine der folgenden Firewalls soll unterstützt werden:

- Microsoft Windows Firewall
- Palo Alto NG
- SIMATIC Scalance SC6x

Sicherheitsmodule für industrielle Umgebungen

Der Anbieter soll robuste, industrietaugliche Sicherheitsmodule anbieten, die die folgenden Charakteristiken aufweisen:

- Integrierte Firewall, die auf IP-Adressen, Mac-Adressen und Ports filtert
- Folgende zusätzliche Funktionen müssen unterstützt werden: NAT, DHCP-Server, VPN-Technologie
- Redundante Stromversorgung
- Konfigurierbarkeit ohne Expertenwissen

Schaffung von Perimeternetzen bzw. demilitarisierten Zonen (DMZs)

Das System muss in der Lage sein, Netzwerke unter Verwendung von Perimeternetzen bzw. demilitarisierten Zonen (DMZ) zu segmentieren. DMZ sollen verwendet werden, um den folgenden Anwendungen einen sicheren Zugriff zu gewährleisten:

- Data Historian (wenn die Anwendung eine Kommunikation außerhalb des geschützten Netzwerks erfordert)
- Web Server
- OPC Server
- Sicherheits-Server (z.B. Virus Scan Server Management System)
- Microsoft Windows Server Update Services (WSUS)

33.4 Benutzerverwaltung und Zugriffskontrolle

Zentrale Benutzerverwaltung

Das System muss die Möglichkeit der zentralen Benutzer-/Gruppenverwaltung innerhalb des Active Directory (Windows-Domain) oder der Windows-Arbeitsgruppe mit den folgenden spezifischen Funktionen bereitstellen:

- Anlegen, Löschen und Ausloggen von Benutzern
- Anlegen, Löschen und Verwenden von Operator-Berechtigungsgruppen
- Two-Level-Kennung (Benutzername und Passwort) oder Login-Werkzeug (z.B. Kartenleser)

Passwortsicherheit

Um die Sicherheit des Passworts für den Zugang zu gewährleisten, muss das System Folgendes leisten:

- Festlegen von Passwortrichtlinien (Mindestlänge, Sonderzeichen usw.)
- Zeitliche Begrenzung der Passwortgültigkeit
- Das zuletzt benutzte Passwort für die nächsten "x" Generationen sperren
- Nach dem ersten Anmelden muss das Passwort geändert werden
- Automatisches Abmelden, wenn der Benutzer einige Zeit inaktiv ist
- Sperren des Benutzers nach "x" falschen Anmeldeversuchen

Rollenbasierter Zugriff

Das System soll Benutzerkonten mit konfigurierbarem Zugriff und Rechten in Verbindung mit benutzerdefinierten Rollen zur Verfügung stellen. Das System muss das Prinzip von minimalen Rechten unterstützen, d.h. Benutzer und Computer können genauso viele Zugangsrechte erhalten, wie sie für die Ausübung ihrer Funktion benötigen.

Single Sign On

Das System muss die Single Sign On (SSO)-Identifizierung unterstützen. Das SSO gewährt dem Benutzer den Zugang zu allen Programmen (PC/Desktop, Engineering-Tools, HMI, Batch) ohne weitere Anmeldungen. Das SSO soll zusammen mit dem rollenbasierten Zugriff verwendet werden können.

33.5 Software Security Patch Management und Test

Der Anbieter des Prozessautomatisierungssystems muss einen nachweislichen lebenszykluslangen Sicherheits-Support für das Prozessautomatisierungssystem einschließlich Folgendem anbieten:

- Testen und Bereitstellen von Patches/Updates für Automatisierungssystem-relevante Firmware und Anwendungsprogramme des Automatisierungssystems
- Testen von Sicherheits-Patches/-Updates für Betriebssysteme, Internet Explorer, MS SQL Server, MS Office und Virenscanner
- Unterstützung bei der Installation von Patches und beim Ausführen von Updates
- Projektinterne Unterstützung für Patch-/Update-Verteilung über einen zentralen Patch-Server (z.B. WSUS) in der DMZ

Eine umfassende öffentlich verfügbare Konfigurationsdokumentation über Sicherheitsaspekte verwendeter Komponenten des Automatisierungssystems ist obligatorisch.

Für eine sichere Netzinfrastruktur ist ein kontinuierliches und sofortiges Testen der aktuellen Security Patches Voraussetzung.

Testen der Microsoft Security Patches

Um sicherzustellen, dass die letzten Microsoft Security Patches auf Kompatibilität mit dem System getestet worden sind, muss der Anbieter die Patches auf ihre Verträglichkeit prüfen. Es bleibt dem Endbenutzer überlassen, die Updates zu benutzen.

Windows Server Update Services

Das System muss die Nutzung der Windows Server Update Services (WSUS) von Microsoft zur Umsetzung einer effektiven Nutzung von Sicherheits-Patches auf allen am Prozessleitsystem angeschlossenen PCs unterstützen. Der WSUS-Server soll die zur Installation bereitstehenden Patches anzeigen und dem Benutzer die Freigabe der Patches nach einer vom Benutzer bestimmten Anweisung ermöglichen.

33.6 Einsatz von Virenscannern

Das System unterstützt den Einsatz von Virenscannern auf allen am Prozessleitsystem angeschlossenen PCs.

Empfohlener Virenscanner:

- Microsoft Defender Antivirus

Minimierung der Auswirkung auf die System-Performance

Um auszuschließen, dass der Virenscanner negative Auswirkungen auf das System hat, muss der Anbieter eine Anleitung zum Einstellen und Konfigurieren des Virenscanners liefern.

Updates und Tests der neuen Signature Files

Um sicherzustellen, dass der Virenscanner auf dem neuesten Stand ist, muss der Anbieter die aktuellen Updates prüfen und für sein System freigeben.

Installation und Betrieb des Virenscanners

Bei der Installation und dem Betrieb des Virenscanners ist Folgendes zu beachten:

- Engineering-Stationen und andere PCs, auf denen Engineering-Daten in das Leitsystemnetzwerk eingespeist werden können: Diese Komponenten sollen im Echtzeitmodus alle empfangenen Daten scannen. Die Scanrate soll im Offline-Betrieb auf manuell oder periodisch einstellbar sein.
- Operator-Stationen: Virenscanner sollen nur im Echtzeitmodus den eingehenden Datenverkehr prüfen.

33.7 Automatische Systemsicherheitseinstellungen

Zur Erhöhung der Standardsicherheit und zur Minimierung des Auftretens von Fehlern während der Konfiguration von Sicherheitseinstellungen muss das System die automatische Konfiguration der lokalen Microsoft Windows-Firewalls, DCOM-Einstellungen und Registrierungseinträge unterstützen.

33.8 Sicherer Zugriff für Fernwartung/Fehlerbehebung

Das System muss eine Fernwartung zur Instandhaltung und Fehlerbehebung über eine sichere Verbindung unterstützen. Der Zugangspunkt muss die Firewall-Technologie und mindestens eine der folgenden Zugriffs- und Autorisierungsverfahren bereitstellen können:

- Authentifizierung und Verschlüsselung mit IP Security (IPsec)
- Authentifizierung und Verschlüsselung mit Secure Sockets Layer (SSL und https)
- Benutzung von VPN (Virtual Private Network) Tunneln
- Network Access Quarantine Control für den sicheren Support-Zugang

33.9 Schwachstellentest

Das System muss einen Schwachstellentest unter Verwendung von Microsoft Baseline Security Analyzer (MBSA) unterstützen. Der Test muss möglich sein, um mindestens die folgenden Gegebenheiten zu erkennen:

- Benutzerkonten ohne Passwort
- Fehlende Microsoft Security Patches

33.10 Sicherheitszertifizierung

Das Prozessleitsystem muss Achilles™ zertifiziert sein.

Der Anbieter muss eine Liste der Achilles™ zertifizierten Komponenten bereitstellen.

Für das Prozessleitsystem ist eine Security Zertifizierung nach IEC-62443 nachzuweisen.

34 Sicherheit

Shutdown-Systeme gelten als sicherheitskritische Systeme. Daher muss die Systemfunktionalität zum Schutz von Personen, der Umgebung und Anlagen gemäß IEC 61508 und IEC 61511 ausgelegt werden. Das Prozessautomatisierungssystem muss der entsprechenden Sicherheitsintegritätsstufe (SIL) bis SIL 3 entsprechen.

Wahlweise muss die Realisierung fehlersicherer Anwendungen bis SIL 3 mit Standard-Controller-Hardware und besonderen fehlersicheren E/A-Baugruppen in einfachen und/oder redundanten Konfigurationen möglich sein. Das System muss modular aufgebaut sein, damit es entsprechend den SIL 2 bzw. SIL 3-Anforderungen der integrierten Sicherheitsfunktionen (SIF) projektiert werden kann.

Fehlersichere Systeme müssen in das Prozessautomatisierungssystem integriert werden[9] (oder separat und unabhängig davon aufgebaut werden).

Für die Programmierung von fehlersicheren Anwendungen muss dieselbe technische Umgebung wie für die Projektierung von Prozessanwendungen verwendet werden und hinsichtlich Ursache-Wirkung-Sicherheitsmatrizen im Controller und der HMI zu unterstützen.

Die Sicherheitsfunktion ist durch ein System mit höchster Verfügbarkeit aufgrund einer Architektur mit Mehrfachfehlertoleranz und integriertem Sicherheitsfeldbus sicherzustellen.

Sicherheitskritische Anwendungen (SIL 1 bis 3) werden von einem Logiksystem gemäß IEC 61508 ausgeführt und von einer unabhängigen Einrichtung (TÜV oder vergleichbare Einrichtung) zertifiziert.

Das Sicherheitssystem muss in das Prozessautomatisierungssystem integriert werden (oder ein Teil davon sein)[9]. Die Visualisierung der Sicherheitsfunktionalität erfolgt über das Prozessautomatisierungssystem.

Die Anwendungslogik muss gegen unbefugte Änderung oder unbefugten Zugriff von externen Quellen geschützt werden.

Konfiguration des Sicherheitssystems

Die Konfiguration fehlersicherer Systeme muss automatisch die benutzerspezifischen CFCs mit denjenigen Funktionen ergänzen, die für die Fehlererkennung und -reaktion erforderlich sind. Die Konfiguration fehlersicherer Systeme muss mit den gleichen Werkzeugen ausgeführt werden, die auch für die Prozesssysteme verwendet werden.

Das System muss die Safety-Programmierung mit Folgendem unterstützen:

- CFC gemäß IEC 61131-3
- Ursache-Wirkung-Sicherheitsmatrix für die Programmierung

Die Konfiguration von Sicherheitsfunktionen muss mit Hilfe einer Sicherheitsmatrix erfolgen, die sicherheitsrelevante CFC-Pläne automatisch erzeugt. Die automatisch erzeugten Sicherheitsbausteine müssen den SIL 3-Anforderungen entsprechen.

Für Berechnungen muss ein Standardwerkzeug verfügbar sein. Anhand dessen soll sichergestellt werden, dass alle Sicherheitskreise die Verfügbarkeit und Zuverlässigkeit entsprechend der zugewiesenen SIL-Stufe erfüllen. Die Ausfallraten der einzelnen Sicherheitssystemkomponenten aller dokumentierten Regelkreise sind in die SIL-Berechnung einzubeziehen.

[9] Abhängend von Projektzielen und -anforderungen

Unterstützung für die sichere Kommunikation

Das System muss die Nutzung von PROFIsafe zur Kommunikation mit intelligenten Feldgeräten auch bei einer redundanten/fehlertoleranten Architektur sicherstellen. Das PROFIsafe-Protokoll stellt sicher, dass eine zuverlässige und fehlersichere Kommunikation (bis SIL 3) zwischen intelligenten Feldgeräten und ihrem Controller über PROFIBUS PA stattfindet.

34.1 Optionale Bibliothek für fehlersichere Controller

Das System muss eine optionale spezifische Bibliothek fehlersicherer Funktionsbausteine anbieten. Diese Bausteine müssen TÜV-geprüft sein und einfach von den für die Prozesssteuerung verwendeten Bausteinen zu unterscheiden sein. Die Bausteine müssen mit dem CFC-Tool verbunden und parametriert werden können.

Nutzung gemeinsamer Hardware

Um die erforderliche Ersatzteilhaltung zu minimieren, muss das System die Nutzung gemeinsamer Hardware (CPU, Stromversorgung, Rückwandplatine und Kommunikationsbaugruppen) für sowohl sicherheitsrelevante als auch nicht sicherheitsrelevante Anwendungen unterstützen.

35 Explosionsschutz

Für den explosionsgefährdeten Bereich muss der Anbieter zukunftsweisende dezentrale Lösungen für die Automatisierungstechnik bieten. Über den Systembus müssen sich diese Lösungen einfach und schnell in jede Steuerung integrieren lassen.

35.1 Dezentrale Hardware

Das System muss eigensichere Anschaltungen/ Koppler und eine dezentrale Peripherie sowie eine zusätzliche Peripherie bereitstellen. Letztere muss eigensicher sein und für sicherheitskritische Anwendungen gemäß SIL 2 und 3 konfiguriert werden. (siehe Kapitel 34).

Ein Einsatz in Zone 2 und 1 wird gefordert. Aktoren und Sensoren müssen auch in Zone 0/20 betrieben werden können. Es muss die Möglichkeit bestehen, Prozessperipherie direkt in Bereiche der Zone 1 zu installieren. Die Peripherieanschaltungen und Koppler müssen auch in explosionsgefährdeten Bereichen (Ex-Bereichen) eingesetzt werden können.

Diese müssen modular und flexibel aufbaubar sein und einer robusten Aufbautechnik genügen.

Durch eine Schiene und integrierte Steckverbindungen muss der Installationsvorgang mit wenig Aufwand durchgeführt werden können.

Die Sensoren und Aktoren müssen über das Bussystem angeschlossen werden können.

Es muss eine "stehende Verdrahtung" realisiert sein, damit ein einfacher Modultausch ohne Lösung der Verdrahtung möglich wird. Der Tausch muss im laufenden Betrieb möglich sein (Hot Swapping). Anschaltungen im Ex-Bereich müssen gezogen und gesteckt werden können.

Alle Geräte müssen nach der ATEX-Richtlinie 94/9/EG zugelassen sein.

35.2 Projektierung und Diagnose

Die Parametrierung und Diagnosemöglichkeit muss lokal oder zentral über die Projektierung des Anbietersystems möglich sein.

Es wird die Möglichkeit der vollen Online-Erweiterung gefordert.

35.3 Hardware-technische Daten und Grenzen:

Das Anbietersystem muss dezentrale Lösungen für die mindestens unten aufgeführten 3 Anforderungen anbieten.

Anforderung 1 erfüllt auch Anforderung 2 und 3

Anforderung 2 erfüllt auch Anforderung 3

	Anforderung 1	Anforderung 2	Anforderung 3
ATEX 94/9/EG IEC 60079-0	II 2 G (1) GD EEx de [ia/ib] IIC/IIB T4	II 3 G EEx nA II T4/T5	II 3 G EEx nA II T4/T5
FM NEC 500/505	IS, Class I Zone 1 EEx ib [ia] IIC, T4 Class I, II, III Division 2 Groups A, B, C, D, E, F, G, T4	Class I Division 2 Groups A, B, C, D, T4/T5 Class I Zone 2 IIC, T4/T5	Class I Division 2 Groups A, B, C, D, T4/T5 Class I Zone 2 IIC, T4/T5
Temperatur 2	-20 °C bis +70 °C	0 °C bis +60 °C	0 °C bis +60 °C

36 Geräteinstallation

Gemäß Projektanforderungen – vom Benutzer zu entwickeln.

37 Dokumentation

Dokumentation zu System-Hardware, Software und Konfigurationswerkzeugen muss zur Verfügung gestellt werden.

Der Systemanbieter muss einen vollständigen Satz von Handbüchern auf CD-ROM/DVD-Medien vorlegen.

Das System muss umfassende kontextsensitive Hilfe bieten.

Überall, wo dies möglich ist, muss der Anbieter kundenspezifische Dokumentation unter Verwendung ins System eingebetteter Standardfunktionalität zur Verfügung stellen. Sämtliche Dokumentation muss in Englisch, Deutsch, Französisch, Italienisch, Spanisch und Portugisisch bereitgestellt werden.

Ein Dienstprogramm für die Anlagendokumentation (Plant Documentation Utility), welches Anlagendokumentation in Übereinstimmung mit Normen und Richtlinien erstellt, muss verfügbar sein.

38 Support-Dienstleistungen

Der Anbieter muss Support per Telefon und E-Mail, Internet-Informationen und Schulungskurse zur Verfügung stellen.

Der Anbieter muss einen weltweiten 24/7-Support für die gesamte System-Hardware und -Software bieten. Dieser Service muss Ersatzteile, Wartung und technischen Support umfassen.

Der Anbieter muss eine veröffentlichte 800-Rufnummer für telefonischen Support während der normalen Geschäftszeiten anbieten.

Während der normalen Geschäftszeiten muss es für normale Produktanfragen einen kostenlosen Support geben.

Der Anbieter muss umfassenden, über das Internet abrufbaren technischen Support anbieten, der u.a. die folgenden Leistungen beinhalten muss:

- E-Mail-Kontakt mit dem technischen Support
- Wissensbasis (Knowledge Base) mit Suchfunktion
- Produktkataloge und Handbücher
- Frequently Asked Questions (FAQs) zu den Produkten
- Synchronisierte System-Software-Update-Sammlungen
- Anwendungsbeispiele
- Anwendungstipps

Als Option muss der Anbieter einen umfassenden Software-Wartungsplan bereitstellen, über den u.a. Folgendes bereitzustellen ist:

- Neueste Produktversion(en)
- Aktualisierte Wissensbasis
- Aktualisierte elektronische Handbücher

39 Schulung

Der Anbieter muss vollständige und umfassende Schulungsprogramme für Bediener, Techniker, das Inbetriebnahme- und Wartungspersonal sowie für IT- und Netzwerkspezialisten anbieten. Die Schulung hat sich auf das grundlegende Prozessautomatisierungssystem sowie auf in der Spezifikation angeführte Geräte und Anwendungen für Spezialisten zu erstrecken.
Der Anbieter muss in der Lage sein, individuelle Schulungsprogramme sowie ein strukturiertes Standard-Schulungsprogramm anzubieten, an dem das Personal teilnehmen kann.

39.1 Basisschulung zum Prozessautomatisierungssystem

Die Basisschulung muss sich auf die folgenden Geräte erstrecken:

- Schulungskurse zur Controller-Hardware des Automatisierungssystems müssen u.a. folgenden Inhalt haben:
    - - CPU, Stromversorgung, Kommunikationskarten, Rückwandplatinen, lokale und abgesetzte E/A-Baugruppenträger.
    - - E/A-Baugruppen
    - - PROFIBUS-, PROFINET IO- und Ethernet-Kommunikation
    - - Fehlertolerante Architektur und fehlersichere Architektur.
- Schulungskurse zur OS-Hardware müssen u.a. folgenden Inhalt haben:
    - - Übersicht über das OS-System
    - - OS-Client- und -Server-Architektur mit Vernetzung und Redundanz
    - - Die Anzeigehierarchie und die grafischen, Trend-, Alarm-, Berichts- und Batch-Anzeigen
- Schulungskurse zur Projektierung des Controllers müssen u.a. die Tools für folgende Aufgaben behandeln:
    - - Projektierung der E/A-Hardware-Geräte
    - - Projektierung der Kommunikationsnetze
    - - Projektierung der kontinuierlichen Regelungsvorgänge und Ablaufsteuerungsvorgänge
    - - Entwurf und Planung von Betriebs- und Überwachungsstrategien
- Schulungskurse zur OS-Projektierung müssen u.a. die Tools für folgende Aufgaben behandeln:
    - - Erstellung einer OS-Systemanwendung
    - - Verwaltung und Management einer OS-Systemdatenbank
    - - Erstellung, Verwaltung und Management von grafischen Anzeigen
    - - Verwaltung und Management des Systemalarmwesens
    - - Verwaltung und Management des Subsystems für Archivierung
    - - Verwaltung und Management des Subsystems für Berichte
- Wartungsschulung
- Schulung für Systemadministratoren

39.2 Fortgeschrittene Schulung

Eine modular aufgebaute, fortgeschrittene Schulung muss entsprechend den Anforderungen dieser Spezifikation verfügbar sein und sich auf Hardware- und Anwendungssoftware für Spezialisten erstrecken:

Beispiel:

- Erweiterte Prozesssteuerung
- Technologische Objekte
- Fernwirkeinrichtungen
- Batch- oder Routing-Systeme
- Elektrizitätsversorgungssysteme
- Asset Management
- Funktionale Prozesssicherheit

40 Vorschriften und Normen

Geräte, die mit Bezug auf diese Spezifikation geliefert werden, müssen den unten aufgeführten Vorschriften und Normen entsprechen wie in den Anforderungen dieses Dokuments im Einzelnen beschrieben wird:

- **International Electrotechnical Commission (IEC)[10]**

IEC 60079-0:2011-06 Explosionsfähige Atmosphäre - Teil 0: Ausrüstung – Allgemeine Anforderungen

IEC 60079-10-1:2015-09 Explosionsfähige Atmosphäre - Teil 10-1: Einteilung der Bereiche - Gasexplosionsgefährdete Bereiche

IEC 60079-10-2:2015-01 Explosionsfähige Atmosphäre - Teil 10-2: Einteilung der Bereiche - Staubexplosionsgefährdete Bereiche

IEC 60529 Ausg. 2.1 (2009-10) Schutzarten durch Gehäuse (IP-Code)

IEC 60751:1983-01 Messfühler für industrielle Platin-Widerstandsthermometer

IEC 60870-5-101:2003-02 Fernwirkeinrichtungen und -systeme - Teil 5-101: Übertragungsprotokolle; Anwendungsbezogene Norm für grundlegende Fernwirkaufgaben

IEC 60870-5-104:2006-06 Fernwirkeinrichtungen und -systeme - Teil 5-104: Übertragungsprotokolle - Zugriff für IEC 60870-5-101 auf Netze mit genormten Transportprofilen

IEC 61000-6-2:2005 Elektromagnetische Verträglichkeit (EMV) – Teil 6-2: Fachgrundnormen - Störfestigkeit für Industriebereiche

IEC 61000-6-4 Ausg. 2.1:2011-2 Elektromagnetische Verträglichkeit (EMV) – Teil 6-4: Fachgrundnormen - Störaussendung für Industriebereiche

IEC 61131-2:2007-07 Speicherprogrammierbare Steuerungen – Teil 2: Betriebsmittelanforderungen und Prüfungen

IEC 61131-3:2013-02-01 Speicherprogrammierbare Steuerungen – Teil 3: Programmiersprachen

IEC 61158-1 Ausg. 1.0:2014-05 Industrielle Kommunikationsnetze – Feldbusse Teil 1: Überblick und Leitfaden zu den Normen der Reihe IEC 61158 und IEC 61784.

IEC 61158-2:2014-07 Feldbus für industrielle Leitsysteme – Teil 2: Spezifikation der Bitübertragungsschicht (Physical Layer)

IEC 61508-1:2010-04 Funktionale Sicherheit sicherheitsbezogener elektrischer/ elektronischer/programmierbarer elektronischer Systeme Teil 1: Allgemeine Anforderungen

IEC 61508-2:2010-04 Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme

[10] Es wird Bezug genommen auf IEC-Standards – für europäische Projekte sollten harmonisierte EU-Normen gewählt werden, falls vorhanden

IEC 61508-3:2010-04 Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 3: Anforderungen an Software

IEC 61508-4:2010-04 Funktionale Sicherheit sicherheitsbezogener elektrischer/ elektronischer/ programmierbarer elektronischer Systeme - Teil 4: Begriffe und Abkürzungen

IEC 61511-1:2016-02 Funktionale Sicherheit - Sicherheitstechnische Systeme für die Prozessindustrie - Teil 1: Allgemeines, Begriffe, Anforderungen an Systeme, Software und Hardware

IEC 61511-2:2016-07 Funktionale Sicherheit - Sicherheitstechnische Systeme für die Prozessindustrie - Teil 2: Anleitungen zur Anwendung des Teils 1 (IEC 61511-1)

IEC 61511-3:2016-07 Funktionale Sicherheit - Sicherheitstechnische Systeme für die Prozessindustrie - Teil 3: Anleitung für die Bestimmung der erforderlichen Sicherheits-Integritätslevel

IEC 61784-1 Ausg. 3.0:2010-07 Industrielle Kommunikationsnetze – Profile Teil 1: Feldbusprofile

IEC 61804-2:2006-09 Funktionsbausteine für die Prozessautomation - Teil 2: Festlegung des Funktionsbausteinkonzepts

IEC 61804-4:2015 Funktionsbausteine für die Prozessautomation und elektronische Gerätebeschreibungssprache - Teil 4: Interpretation von Gerätebeschreibungen

IEC 61850-8-1:2011-06 Kommunikationsnetze und -systeme für die Automatisierung der elektrischen Energieversorgung - Teil 8-1: Spezifische Abbildung von Kommunikationsdiensten (SCSM) - Abbildungen auf MMS (nach ISO 9506-1 und ISO 9506-2) und ISO/IEC 8802-3

IEC 62061 Ausg. 1.2:2015-08 Sicherheit von Maschinen - Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme

IEC 62443 *Industrial communication networks – Network and system security*

IEC 62443-2-1:2010-11 Industrielle Kommunikationsnetze - IT-Sicherheit für Netze und Systeme - Teil 2-1: Einrichten eines IT-Sicherheitsprogramms für industrielle Automatisierungssysteme

IEC 624433-3-3: Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels

IEC 624433-4-1: IT-Sicherheit für industrielle Automatisierungssysteme - Teil 4-1: Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung

IEC(/TR) 62541:2010-02 Vereinheitlichte OPC Architektur

IEC 62682:2014-07: Entwurf) Alarmmanagement für die Prozessindustrie

- **Institute of Electrical and Electronics Engineers (IEEE)**

IEEE Std. 1815:2012 for Electric Power Systems Communications - Distributed Network Protocol (DNP3)

IEEE 754:2008-01 Gleitkommaarithmetik/Ausgabedatum

IEEE 802.3XX Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications (series)

- **Object Linking and Embedding for Process Control (OPC) Foundation**

Die Normen finden Sie unter www.openfoundation.org. In der vorliegenden Spezifikation werden diese Normen mit vorangestelltem "OPC" kenntlich gemacht.

- **The OPC Unified Architecture (UA)**

OPC UA ist eine plattformunabhängige serviceorientierte Architektur, die alle Funktionalitäten der einzelnen OPC Classic-Spezifikationen in ein erweiterbares Framework integriert.

- **National Fire Protection Association**

NFPA 70 National Electrical Code – Article 250: Grounding and Bonding (geltende Version am Standort gültig)

NFPA 70 National Electrical Code – Article 500: Hazardous (Classified) Locations, Classes I, II, AND III, Divisions I AND 2 (geltende Version am Standort gültig)

NFPA 70 National Electrical Code – Article 505: Zone 0, 1 and 2 Locations (geltende Version am Standort gültig)

NFPA 79 (2007) (geltende Version am Standort gültig) NFPA 79 Electrical Standard for Industrial Machinery

- **National Electrical Manufacturers Association (NEMA)**

NEMA 250:2008-01 Enclosures for Electrical Equipment (1000 Volts maximum)

- **Underwriters Laboratories**

UL-Zertifikat

- **Canadian Standards Association**

CSA-Zertifikat

- **International Organization for Standardization (ISO)**

ISO 9001:2015-09 Qualitätsmanagementsysteme - Anforderungen

ISO 11064-5:2008-07 Ergonomische Gestaltung von Leitzentralen - Teil 5: Anzeigen und Stellteile

ISO 13849-1:2006-11 Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 1: Allgemeine Gestaltungsleitsätze

ISO 10418:2003-10 Erdöl- und Erdgasindustrie - Offshore Produktionsanlagen - Analyse, Auslegung, Installation und Prüfung von grundlegenden Sicherheitssystemen von Verfahren oberhalb der Wasseroberfläche

- **International Society of Automation** (ISA)

ISA/ANSI 84.00.01:2004-09 Functional safety of safety instrumented systems for the process industry sector - Part 1 Framework, Definitions, System, Hardware and Software Requirements

ISA/ANSI 84.00.02:2004-09 Functional Safety: Safety Instrumented Systems for the Process Industry Sector — Part 2: Guidelines for the Application of ANSI/ISA 84.00.01 2004 Part 1 (IEC 61511-1 Mod) Hardware and Software Requirements

ISA/ANSI 84.00.03:2004-09 Functional Safety: Safety Instrumented Systems for the Process Industry Sector - Part 3: Guidance for the Determination of the Required Safety Integrity Levels - Informative

ANSI/ISA 88.00.0X Batch Control Part 1: Models and Terminology; Part 3: General and Site Recipe Models and Representation; Part 4: Batch Production Records (in diesem Dokument als ISA S88 bezeichnet)

ANSI/ISA 95.00.0X Enterprise-Control System Integration Parts 1-5

- **Europäische Kommission**

Mit der CE-Kennzeichnung (Conformité Européenne) erklärt der Hersteller, dass das Produkt den geltenden Anforderungen der EU-Richtlinien genügt:

- Geräte für explosionsgefährdete Bereiche, Richtlinie 2014/34/EU
- Richtlinie 2014/30/EU über die elektromagnetische Verträglichkeit (EMV)
- Niederspannungsrichtlinie 2014/35/EU
- Maschinenrichtlinie 2006/42/EG

EU-Richtlinien über gute Herstellungspraxis, Teil 4, Anhang 11; (2011)

- **US-amerikanische Regierung**

US Food and Drug Administration (FDA) 21 CFR Part 11[11] – Electronic Records: Electronic Signatures (ERES)

- **International Society for Pharmaceutical Engineering (ISPE)**

Good Automated Manufacturing Practice (GAMP). GAMP 5 A Risk-Based Approach to Compliant GxP[12] Computerized Systems

- **EEMUA**

EEMUA 201 (Ed.2:2010) Process plant control desks utilizing human-computer interfaces: a guide to design, operational and human-computer interface issues

- **NAMUR**

NAMUR NE 91 Anforderungen an Systeme für anlagennahes Asset Management

NAMUR NE 105 Anforderungen an die Integration von Feldbusgeräten in Engineering-Tools für Feldgeräte

NAMUR NE 107 bzw. VDI/VDE/NAMUR/WIB 2650 Selbstüberwachung und Diagnose von Feldgeräten

- **Sonstige**

Modbus RTU:2002-12 MODBUS over serial line specification and implementation guide V1.0 (Modbus Organization)

[11] CFR = Code of Federal Regulations der US-amerikanischen Regierung.

[12] GxP ist ein allgemeiner Begriff für "gute (beliebige...) Praxis"

41 Definitionen

Dieses Kapitel enthält Definitionen für Akronyme, Abkürzungen, Wörter und Begriffe, die im vorliegenden Dokument verwendet werden.

41.1 Akronyme und Abkürzungen

CAD	Rechnerunterstütztes Konstruieren (Computer Aided Design)
CAE	Rechnerunterstützte Entwicklung (Computer Aided Engineering)
CFC	Continuous Function Chart
CPU	Zentrale Steuereinheit (Central Processing Unit)
PLS	Prozessleitsystem
DHCP	Dynamic Host Configuration Protocol
DOL	Direkteinschaltung (Direct On Line)
DMZ	Demilitarisierte Zonen
ECC	Error Correcting Code-Speicher
EDDL	Elektronische Gerätebeschreibungssprache (Electronic Device Description Language, IEC 61804)
EIA	Electronic Industries Association
EMV	Elektromagnetische Verträglichkeit
EMS	Elektromagnetische Störung
ERP	Enterprise Resource Planning
ES	Engineering-Station
FDI	Feldgeräte-Integration (Field Device Integration)
GPS	Global Positioning System
HART	Highway Addressable Remote Transducer
HMI	Mensch-Maschine-Schnittstelle (Human Machine Interface)
E/A	Eingabe/Ausgabe
IEC	International Electrotechnical Commission
AWL	Anweisungsliste
IPsec	Internet Protocol Security
ISA	The Instrumentation, Systems, and Automation Society
ITP	Industrial Twisted Pair
MAC	Media-Access-Control-Adresse
MES	Manufacturing Execution Systems
MQTT	Message Queue Telemetry Transport Protokoll
MTA	Vorkonfigurierte Abschlussbaugruppe/-komponente (Marshalled Termination Assembly)
MTBF	Mittlere Betriebsdauer zwischen Ausfällen (Mean Time Between Failures)

NAT	Network Address Translation
NAPT	Network Address & Port Translation
OLE	Objektverknüpfung und -einbettung (Object Linking and Embedding)
OPC	OLE für Prozesssteuerung
OPC UA	OPC Unified Architecture
OS	Operator-Station
PC	Personalcomputer (X86-64- oder x64-basierte Computer-Architektur)
P&I-Fließschema	Prozess- und Instrumentenfließschema
PID	Proportional-Integral-Differential
PG	Panzergewinde (Stahlpanzerrohrgewinde-Norm für Schraubgewinde - DIN 40430)
PO	Prozessobjekt
PSU	Stromversorgungseinheit (Power Supply Unit)
RAID	Redundante Anordnung unabhängiger Festplatten (Redundant Array Independent Disks)
RFI	Funkfrequenzstörung (Radio Frequency Interference)
R-LAD	Relais-Kontaktplan (Relay Ladder Logic)
RIO	Abgesetzte Ein-/Ausgabe (Remote Input/Output)
RTD	Widerstandsthermometer (Resistance Temperature Detector)
RTX	Real Time Extension für Microsoft Windows
SFC	Ablaufsprache (Sequential Function Chart)
SIF	Integrierte Sicherheitsfunktion
SIL	Sicherheitsintegritätsstufe
SQL	Structured Query Language
ST	Strukturierter Text
STO	Standardisiertes technologisches Objekt
TCP/IP	Transmission Control Protocol/Internet Protocol
VSD	Regelantrieb (Variable Speed Drive)
VPN	Virtuelles privates Netz
WLAN	Wireless-LAN

Telemetrie

DSL	Digitaler Teilnehmeranschluss (Digital Subscriber Link)
FMS/PROFIBUS DP	Fieldbus Message of PROFIBUS Decentralized Peripherals
GOOSE	Generic Object Oriented Substation Events (IEC 61850-8-1)
GPRS	Allgemeiner paketorientierter Funkdienst (General Packet Radio Service)
GPS	Global Positioning System

IED	Intelligentes elektronisches Gerät (Intelligent Electronic Device, IEC/TR 61850-1)
IP	Internet-Protokoll
ISDN	Dienstintegrierendes digitales Netz (Integrated Services Digital Network)
IWLAN	Industrial Wireless Local Area Network
MMS	Nachrichtenprotokoll für Fertigungszwecke (Manufacturing Message Protocol, ISO 8802-3)
PSTN	Festnetz (Public Switched Telephone Network)
RTU	Fernbedienungsterminal (Remote Telemetry Unit)
UMTS	Universal Mobile Telecommunications System
WAN	Wide Area Network

41.2 Wörter und Begriffe

Alarmprotokollierung, Alarmaufzeichnung (Alarm Logging): Editor für die Konfiguration des Meldungssystems in der Operator-Station und Anwendung für die Anzeige, Archivierung und Abwicklung von Meldungen.

Archiv: Ablage historischer Messwerte und Meldungen in der Operator-Station, sodass diese Daten langfristig wieder abgerufen werden können.

AS-Interface: Das Actuator Sensor Interface ist ein Vernetzungssystem für im Feld montierte binäre Sensoren und Stellglieder.

Akustischer Melder (Audible Signal Device): Signalhorn, Hupe, Glocke, Summer oder ähnliches Gerät, das anzeigt, dass ein neuer Alarm oder eine Meldung bei der Operator-Station angekommen ist.

Verfügbarkeit: Die Wahrscheinlichkeit, dass ein System seine vorgesehene Funktion erfüllen kann, wenn dies erforderlich ist.

Bausteine: Bausteine sind einzelne Bestandteile der Controller-Software-Konfiguration eines Benutzers, die durch spezifische Funktion, Struktur und spezifischen Zweck gekennzeichnet sind.

Bus: Ein Leitweg für elektrische Signale, der den Austausch von Daten zwischen verschiedenen Komponenten eines Computers oder Systems ermöglicht.

CPU: Die zentrale Einheit des Controllers, in der das Benutzerprogramm gespeichert ist und verarbeitet wird und in der das Betriebssystem und Kommunikationsschnittstellen enthalten sind.

CFC (Continuous Function Chart): Eine höhere grafische Sprache mit Funktionsbausteinen für die Projektierung kontinuierlicher Regelungssysteme.

FDI (Field Device Integration)**:** eine Technologie, die eine einheitliche Geräteintegration für alle Leitsysteme, Feldgeräte und Protokolle erlaubt.

GSD (General Station Description): Kommunikationsmerkmale eines Profibus-Gerätes sind immer in einer GSD-Datei beschrieben.

GSDML (General Station Description Markup Language): Die Funktionalität eines Profinet-IO-Feldgerätes ist immer in einer GSD-Datei beschrieben.

MRP (Media Redundancy Protocol): Mit dem MRP kann über eine Ringtopologie eine redundante PROFINET Kommunikation ohne Switches realisiert werden.

Plan (Chart): Das Dokument, in dem die Automatisierungsfunktionen mit dem CFC Tool oder dem SFC Tool erstellt werden können.

Leitung: Logische Gruppierung von Kommunikationsanlagen, die die Sicherheit darin enthaltener Kanäle schützt.

Kommunikationsverbindung: Die Hardware und Software für die Übertragung und den Empfang digitaler Informationen über ein Kommunikationssystem wie z.B. einen Bus.

Konfigurierbar, projektierbar: Die Möglichkeit der Auswahl und Verknüpfung von Standard-Hardware-Modulen (Baugruppen, Bausteinen) zu einem System; oder die Möglichkeit der Änderung der Funktionalität oder Bemessung von Software-Funktionen durch Änderung von Parametern ohne Änderung oder Neugenerierung von Software.

Konfiguration, Projektierung: Die physikalische Installation von Hardware-Modulen zur Erfüllung von Systemanforderungen; oder die Auswahl von Software-Optionen zur Erfüllung von Systemanforderungen.

CSV (Comma Separated Values): ASCII-Textformat zur Speicherung von Tabellendaten.

Zyklus: Im Controller, die Ausführung von Algorithmen durch diesen, und die Übertragung von Ausgabewerten an Geräte.

Internet-Sicherheitskonzept (Cybersecurity): Maßnahmen, die zur Verhinderung einer unbefugten Nutzung von kritischen Systemen oder Informationen sowie zur Verhinderung von DoS-Angriffen, Änderungen, Offenbarung, Umsatzeinbußen oder Zerstörung im Zusammenhang mit derartigen Systemen und Informationen erforderlich sind.

DCF77: Langwellenzeitsignal und Normalfrequenz-Funkstation der Physikalisch-Technischen Bundesanstalt (PTB).

Diskrete Regelung: Regelung, bei der Eingaben, Algorithmen und Ausgaben auf logischen Werten (wahr oder falsch) basieren.

Dezentrale Peripherie: Feldgeräte oder analoge und digitale Baugruppen, die abgesetzt von ihrem zentralen Controller installiert sind.

Engineering-Workstation (ES): Computer-Ausrüstung, die einen PC, einen Monitor, eine Tastatur und ein zugehöriges Zeigegerät umfasst und von technisch-versiertem Personal zur Projektierung des Leitsystems verwendet wird.

Ethernet: Hardware-Typenstandard für die Datenübertragung mit Coax-, Twisted Pair- oder LWL-Kabeln bzw. für die drahtlose Datenübertragung meist mit 10 Mbit/s (siehe Fast Ethernet).

Bildbaustein (Faceplate): Ein grafisches Element auf dem Bildschirm der Operator-Station, das z.B. ein analoges Steuerinstrument, einen festverdrahteten Drucktaster oder einen Schalter darstellt und die Beobachtung und Bedienung des Geräts durch den Operator ermöglicht.

Fast Ethernet: Schnellere Version von Ethernet mit Übertragungsraten von 100 Mbit/s (IEEE 802.3u-1995).

Fehlertolerantes System: Ein System, in dem alle wesentlichen Komponenten (wie z.B. CPU, Stromversorgungen, Racks) doppelt vorhanden sind, sodass bei Auftreten eines Fehlers das Reservegerät die Funktion vom Hauptgerät ohne Unterbrechung der Steuerung übernehmen kann.

Foundation Fieldbus: Der Feldbusstandard der ISA/IEC Foundation bezieht sich auf ein Kommunikationssystem für im Feld montierte Mess- und Steuerungsgeräte. (IEC 61784 und IEC 61158).

Funktionsplan (FUP): Ein Steuerbaustein gemäß IEC 61131-3.

Gigabit Ethernet: Ethernet mit Übertragungsraten von 1000 Mbit/s.

GPS (Global Positioning System): Satellitengestütztes System, das exakte Positionen überall auf der Erde sowie die Uhrzeit liefert.

HMI (Human Machine Interface) (Mensch-Maschine-Schnittstelle): Das grafische Schnittstellenprogramm, das es einem Operator ermöglicht, mit einem Prozess zu interagieren und Prozesse zu steuern.

Instanz: Eine Kopie eines Funktionsbausteins, die für die Steuerungsprojektierung einer ähnlichen Anwendung wiederverwendet wird.

Anweisungsliste (AWL): Eine Textprogrammiersprache, die der Maschinensprache ähnelt und der Norm IEC 61131-3 entspricht.

Ungültiger Wert: Der Zustand eines Variablenwerts, der anzeigt, dass die gemessene oder berechnete Menge außerhalb des zulässigen Bereichs liegt, nicht messbar oder nicht berechenbar ist.

Kontaktplan (KOP): Grafische Darstellung der Automatisierungsaufgabe mit Relaissymbolen gemäß IEC 61131-3.

Lifebeat Monitoring (Lebensüberwachung): Ein Programm auf der Operator-Station, das den Controller, Server und Operator-Stationen überwacht und ein Anlagenbild mit dem Status liefert.

Protokolle: Dateien oder Ausdrucke von Informationen in chronologischer Reihenfolge.

Modus, Betriebsart: Betriebszustand von Steuerbausteinen wie z.B. manuell, automatisch oder Kaskade.

Baugruppe, Baustein, Modul: Eine Gruppe miteinander verbundener Komponenten, die ein erkennbares Gerät, Instrument oder Ausrüstungselement darstellen. Eine Baugruppe kann abgeschaltet, als komplette Einheit entfernt und durch ein Ersatzteil ersetzt werden. Sie hat definierbare Leistungsmerkmale, die ihre Prüfung als Einheit ermöglichen.

OPC (Object Linking and Embedding for Process Control): Software-Anwendung, die einen bidirektionalen Datenfluss zwischen zwei getrennten Anwendungen ermöglicht.

Operator-Station (OS): Elektronische Ausrüstung auf der sich die Mensch-Maschine-Schnittstelle befindet, die mindestens einen Monitor, eine Tastatur und ein Zeigegerät umfasst und durch einen Operator zum Beobachten und Bedienen des ihm zugewiesenen Prozesses oder der ihm zugewiesenen Fertigungseinheiten verwendet wird.

R1 System Redundancy: ein modulares PROFINET-Gerät mit redundanter Kommunikationsschnittstelle baut mehr als eine Kommunikationsbeziehung zu einem redundanten Controller auf.

S2 System Redundancy: ein PROFINET-Gerät mit einfacher Kommunikationsschnittstelle baut mehr als eine Kommunikationsbeziehung zu einem redundanten Controller auf.

SPS (Speicherprogrammierbare Steuerung): Wird für die diskrete und kontinuierliche Steuerung in Verarbeitungs- und Produktionsanlagen verwendet.

PROFIBUS: Feldbus entsprechend EN 50170 Vol. 2 PROFIBUS (DIN 19245; Bussystem für industrielle Anwendung auf Basis von PROFIBUS).

Plug and Play: Die Fähigkeit von Hardware-Geräten, sich gegenüber dem System automatisch selbst zu identifizieren. Wird das Gerät eingeschaltet, so wird ihm automatisch eine eindeutige Kennung zugewiesen, ohne dass dafür DIP-Schalter gesetzt werden müssen.

Punkt: Eine Prozessvariable, die von einem Eingangssignal abgeleitet oder in einer Prozessberechnung errechnet wird.

Prozessobjekt: Eine Sammlung von Variablen und Parametern, die eine Steuerungs-/Regelungsfunktion ausführt (z.B. Motor, Sperrventil, PID-Regler), die aus mehr als einem E/A-Punkt bestehen kann.

Redundant: Ein System/Subsystem mit zwei Modulen, die bei Auftreten eines Fehlers eine automatische Umschaltung (Ersatzschaltung) ohne Ausfall der Systemfunktion durchführen.

Regelung: Die Funktionen Prozessmessung, Ausführung von Regelungsalgorithmen und Regelung eines Gerätestellglieds, durch die die selbsttätige Regelung eines Anlagenprozesses bereitgestellt wird.

Zuverlässigkeit: Die Wahrscheinlichkeit, dass das System oder die Komponente seinen bzw. ihren vorgesehenen Zweck für eine bestimmte Zeit erfüllt, gemessen meist als „Mean Time Between Failures" (mittlerer Ausfallabstand).

Strukturierter Text (ST): Eine höhere Sprache entsprechend IEC 1131-3 und ähnlich Pascal für die Programmierung komplexer oder kundenspezifischer Steuerungs-/Regelungsaufgaben im Controller.

Selbst diagnostizierend: Die Fähigkeit eines elektronischen Geräts, seinen eigenen Status selbst zu überwachen und Fehler anzuzeigen, die im Gerät selbst auftreten.

Sicherheit: Systemzugriffskontrolle durch Tastensperre, Passwort, elektronische Karte oder gleichwertiges Verfahren.

Ablaufsteuerung: Eine Art diskrete Steuerung, die sequentielle Prozesse abwickelt.

Sequential Function Chart (SFC): Eine höhere grafische Projektierungssprache für Ablaufsteuerungsanwendungen.

Systembus: Das Netz, das für die Kommunikation zwischen Steuerungen und HMI-Servern verwendet wird.

Variable: Eine Sammlung von Attributen, die einen Regelkreis, eine Prozessvariable, eine gemessene Eingabe, einen berechneten Wert oder eine Kombination derselben sowie alle zugehörigen Steuerungs-/Regelungs- und Ausgabealgorithmen spezifiziert. Jede Variable ist eindeutig.

Variablenkennung: Der eindeutige alphanumerische Code, der Eingängen, Ausgängen, Gerätepositionen und Steuerbausteinen zugewiesen wird. Die Variablenkennung kann die Anlagenbereichskennung enthalten.

Terminalbus: Das Netz für die Kommunikation zwischen HMI-Clients und HMI-Servern.

Zeitsynchronisation: Time Synch wird durch die Operator-Station bereitgestellt, um sicherzustellen, dass alle SPS und Operator-Stationen auf dem Bus mit der gleichen Uhrzeit arbeiten.

Virtualisierung: Virtualisierung bezieht sich auf die ausführbare Abbildung eines oder mehrerer Computer auf einem realen Computer.

Zone: Gruppierung logischer oder physischer Anlagen, die denselben Sicherheitsanforderungen unterliegen.

42 Warenzeichen

Microsoft®, Windows®, Windows Server®, Windows 7®, Windows XP®, Internet Explorer®, SQL Server®, Excel®, Access®, ActiveX®, Visual Basic® sind entweder eingetragene Warenzeichen oder Warenzeichen der Microsoft Corporation.

OLE, DCO, COM sind von Microsoft entwickelte Technologien, die die Verknüpfung und Einbettung von Objekten ermöglichen.

Adobe®, PostScript® und Acrobat® sind eingetragene Warenzeichen von Adobe Systems, Incorporated.

BATCHML wurde vom World Batch Forum (WBF) spezifiziert.

AutoCAD® ist ein eingetragenes Warenzeichen von Autodesk, Incorporated.

X Window System ist ein Warenzeichen von The Open Group

SAP®, Sybase®, Crystal Reports® sind Warenzeichen oder eingetragene Warenzeichen der SAP AG in Deutschland und zahlreichen anderen Ländern oder eines SAP-Tochterunternehmens.

HTML, XML sind Warenzeichen, eingetragene Warenzeichen oder Oberbegriffe des Massachusetts Institute of Technology (MIT), des European Research Consortium for Informatics and Mathematics (ERCIM) oder der Keio University.

PROFIBUS ist ein Warenzeichen der PROFIBUS User Organization.

HART® ist ein eingetragenes Warenzeichen der HART Communication Foundation.

McAfee, Virusscan® sind eingetragene Warenzeichen von McAfee Inc.

OfficeScan® ist ein Warenzeichen oder eingetragenes Warenzeichen von Trend Micro Incorporated.

Symantec AntiVirus™, Norton® ist ein Warenzeichen oder eingetragenes Warenzeichen der Symantec Corporation oder deren Tochterunternehmen.

Foundation™ Fieldbus ist ein Warenzeichen der Fieldbus Foundation

GAMP® ist ein eingetragenes Warenzeichen der International Society for Pharmaceutical Engineering.

TÜV® ist das Warenzeichen der TÜV-Organisationen und der TÜV-Interessenvertretung (VdTÜV).