

ERZ\_WN\_0002476

Erzeugung Wärme und Strom, Werknorm Grundlage für die  
Spezifikation der Leittechnik

gültig ab: 06.01.2026  
Reviewdatum: 06.01.2028  
verantwortlich: M4-EP2  
Status: Gültig  
Seite: 1

## Basisinformationen

Geltungsbereich/ gültig für	Diese Werknorm gilt für alle Anlagen oder Anlagenteile, die in der Betreiberverantwortung von M4-E liegen oder liegen werden.
Ziel und Zweck (2-3 Sätze)	Die Werknorm dient als Leitfaden zur einheitlichen Ausführung von Prozessleitsystemen für Erzeugungsanlagen der Mainova AG bei der Erstellung des Leistungsverzeichnisses
Inhalt (2-3 Sätze)	Die Werknorm beinhaltet Vorgaben zum Aufbau und Ausführung der Prozessleitsysteme für Kraftwerke
Bemerkungen/ Zusatzinformationen	
Regelungsersteller	Opp, Olaf
Ablauf Reviewfrist (Zeitraum)	24 Monate
Prüfung durch:	<input type="checkbox"/> Compliance/ Recht <input type="checkbox"/> ISMS/ Datenschutz <input type="checkbox"/> Personalrecht (Mitbestimmung BR)

## Inhalt

1. Regelungseigenschaften .....	3
1.1 Ziel/Zweck .....	3
1.2 Geltungsbereich .....	3
1.3 Inkrafttreten .....	3
2. Allgemein .....	3
3. Begriffsdefinition und Geltungsbereich .....	4
4. Prozessleitsystem .....	6
4.1 Prozessautomatisierung .....	6
4.2 Allgemeine Anforderungen .....	8
4.3 Redundanz .....	10
4.4 Funktionale Sicherheit von sicherheitstechnischen Systemen .....	11
4.5 IT-Sicherheit .....	12
5. Komponenten .....	13
5.1 Ein/- und Ausgabebaugruppen .....	13
5.2 Bediener PCs (Clients) .....	13
5.3 Engineering Stationen .....	13
5.4 Server PC Prozessdatenbank/ Meldungen/ Langzeitarchivierung .....	14
5.5 Monitore/ Großbildschirme .....	14
5.6 Systemauslastung, CPU und Netzwerk .....	14
5.7 Leittechnikschränke .....	15
6. Aufbau/ Programmierung/ Konfiguration Automatisierungsebenen .....	16
6.1 Prozess- und Blockleitebene .....	16
6.2 Gruppenleitebene .....	16
6.3 Einzelleitebene .....	16
7. Funktionen des Bedien- Beobachtungssystems .....	17
7.1 Dynamische Darstellung des Prozesses .....	17
7.2 Alarm Management .....	18
7.3 Führung der Bediener .....	18
8. Feldgerätevisualisierung .....	19
9. Schnittstellen/ Kopplung .....	19
10. Dokumentation .....	19
11. Beispiel Topologie Leitsystem .....	20
12. Mitgeltende Regelungen .....	20
13. Anhänge .....	20

## 1. Regelungseigenschaften

### 1.1 Ziel/Zweck

Diese Werknorm gilt für alle Anlagen oder Anlagenteile, die in der Betreiberverantwortung von M4-E liegen oder liegen werden.

Diese Anweisung beschreibt die Mindestanforderungen für Prozessleitsysteme in Bezug auf Systemaufbau, Programmierung und Bedienung für Kraftwerke als Grundlage/ Leitfaden für die Erstellung einer projektspezifischen, detaillierten Anfrage/ Ausschreibung- bzw. Bestellspezifikation (Leistungsverzeichnis/ Lastenheft).

### 1.2 Geltungsbereich

Diese Werksnorm gilt für alle Beschäftigten der Bereiche/ der Abteilungen M4-E.

### 1.3 Inkrafttreten

Diese Werksnorm tritt mit ihrer Veröffentlichung in Kraft.

## 2. Allgemein

Für die grundsätzlichen Anforderungen an die Qualität und die Funktionalität eines Prozessleitsystems ist diese Richtlinie maßgebend.

Grundlagen sind alle einschlägigen, gesetzlichen, behördlichen und gewerblichen Vorschriften und der anerkannte Stand der Technik, dokumentiert in VDE, VDI, TÜV, VGBE und den DIN-/EU-/IEC-Normen.

### 3. Begriffsdefinition und Geltungsbereich

Unter einem Prozessleitsystem werden die datenverarbeitenden Einrichtungen verstanden, die erforderlich sind, Produktionsvorgänge oder Teile davon digital zu erfassen, zu automatisieren, übersichtlich darzustellen und den steuernden menschlichen Eingriff zu unterstützen oder überhaupt erst zu ermöglichen.

Im Bereich der verfahrenstechnischen, energieerzeugenden oder –verteilenden Anlage bedeutet dies, dass

- Aktoren einer elektrischen Fernansteuerung zugänglich gemacht werden.
- Sensoren zur Überwachung und zur Bildung von Kriterien erfasst werden.
- Mit Steuerungen und Regelungen Sensoren und Aktoren zu automatisierten Funktionseinheiten verschaltet werden.
- Mit Bildschirmsystemen eine benutzerfreundliche Visualisierungs- und Eingriffsmöglichkeit geschaffen wird.
- Meldefunktionen den Menschen in seinen Entscheidungen unterstützen.
- Auswertefunktionen eine Analyse des Geschehenen ermöglichen.
- Übergeordnete oder externe Stellen Zugriff auf (ausgewählte) Daten bekommen.
- Unterschiedliche Anlagenteile miteinander vernetzt werden können.

Für komplexe Aufgabenstellungen, wie zum Beispiel der Automatisierung eines Großkraftwerkes, bietet sich der Einsatz eines durchgängigen Prozessleitsystems an, welches sämtliche leittechnischen Anforderungen der gesamten Anlage möglichst mit einer Systemtechnik löst, beginnend bei der Signalaufbereitung, fortgeführt in der Zusammenschaltung und Verarbeitung und endend in der Visualisierung.

Für kleine Anlagen oder verfahrenstechnisch abgeschlossene Bereiche einer Gesamtanlage mit einem geringen Signalaustauschbedarf, mit anderen Anlagenbereichen, wird häufig auf den Einsatz eines durchgängigen Prozessleitsystems verzichtet. Dies muss projektspezifisch nach der Wichtigkeit bzw. Kritikalität des jeweiligen Anlagenteils entschieden werden.

Dafür können die Anlagenbereiche mit gleicher SPS-Technik (**S**peicher**p**rogrammierbare **S**teuerung) automatisiert, visualisiert und miteinander verschaltet werden. Der Lieferant der jeweiligen eingesetzten SPS soll anlagenweit gleich gehalten werden.

Um dem Bediener eine durchgängige Anlagenführung zu ermöglichen, sollte daher die Bedienung und Beobachtung harmonisiert werden.

Im Bereich der Automatisierung wird unterschieden zwischen SCADA (Supervisory Control and Data Acquisition / Überwachungssteuerung und Datenerfassung) und PLS (Prozessleitsystem) oder auch DCS (Distributed Control System).

Der Terminus SCADA bezieht sich gewöhnlich auf dezentrale Systeme, die die gesamte Installation überwachen, [visualisieren](#) sowie steuern und regeln. Meist sind sie aus einem oder mehreren sogenannten Master Terminal Units (MTU, auch SCADA-Master oder SCADA-Server genannt) aufgebaut. Der größte Teil der Regelung wird automatisch durch [Fernbedienungsterminals](#) (Remote Terminal Units, RTU) oder durch [Speicherprogrammierbare Steuerungen](#) (SPS) durchgeführt. SCADA Systeme kommen oft zum Einsatz um übergeordnet auf mehrere verschiedene Leitsysteme Zugriff zu haben und so eine einheitliches Bedienen und Beobachten zu ermöglichen. Ein PLS/DCS ist ein verteiltes Automatisierungssystem, das zur Steuerung komplexer industrieller Prozesse entwickelt wurde. Es zeichnet sich durch seine Fähigkeit aus, große Datenmengen aus mehreren Quellen wie Sensoren, Aktoren und anderen Steuergeräten zu verarbeiten.

DCS-Systeme werden typischerweise in Branchen wie Öl und Gas, Chemie und Energieerzeugung eingesetzt. DCS-Steuerungssysteme bestehen aus mehreren Controllern, die mit einem zentralen Server oder Netzwerk verbunden sind. Jeder Controller ist für die Steuerung eines bestimmten Teils des Prozesses verantwortlich. Der zentrale Server bzw. das Netzwerk dient der Verwaltung und Koordination der Controller und sorgt so für eine reibungslose Zusammenarbeit.

Der Hauptvorteil von DCS-Automatisierungssystemen ist ihre Fähigkeit, große Datenmengen aus mehreren Quellen zu verarbeiten. Damit eignen sie sich ideal für die Steuerung komplexer Industrieprozesse. DCS-Systeme sind außerdem äußerst zuverlässig und verfügen über integrierte Redundanz, um sicherzustellen, dass das System auch dann weiter funktioniert, wenn eine oder mehrere Komponenten ausfallen.

Um dem Bediener eine durchgängige Anlagenführung zu ermöglichen, sollte daher die Bedienung und Beobachtung harmonisiert sein. Dies gilt ebenfalls für die Programmierenebene: Aus der Bedienebene soll jederzeit ein Zugriff auf die Programmierenebene möglich sein.

Im Folgenden werden die Anforderungen an ein Prozessleitsystem detailliert.

## 4. Prozessleitsystem

### 4.1 Prozessautomatisierung

Um den genannten Aufgaben gerecht zu werden, besteht die Prozessautomatisierung aus verschiedenen Ebenen:

- Im Bereich der Prozessautomatisierung werden verschiedene Ebenen unterschieden. Diese lassen sich in Form einer Pyramide darstellen. Diese basieren auf der IEC 62264.

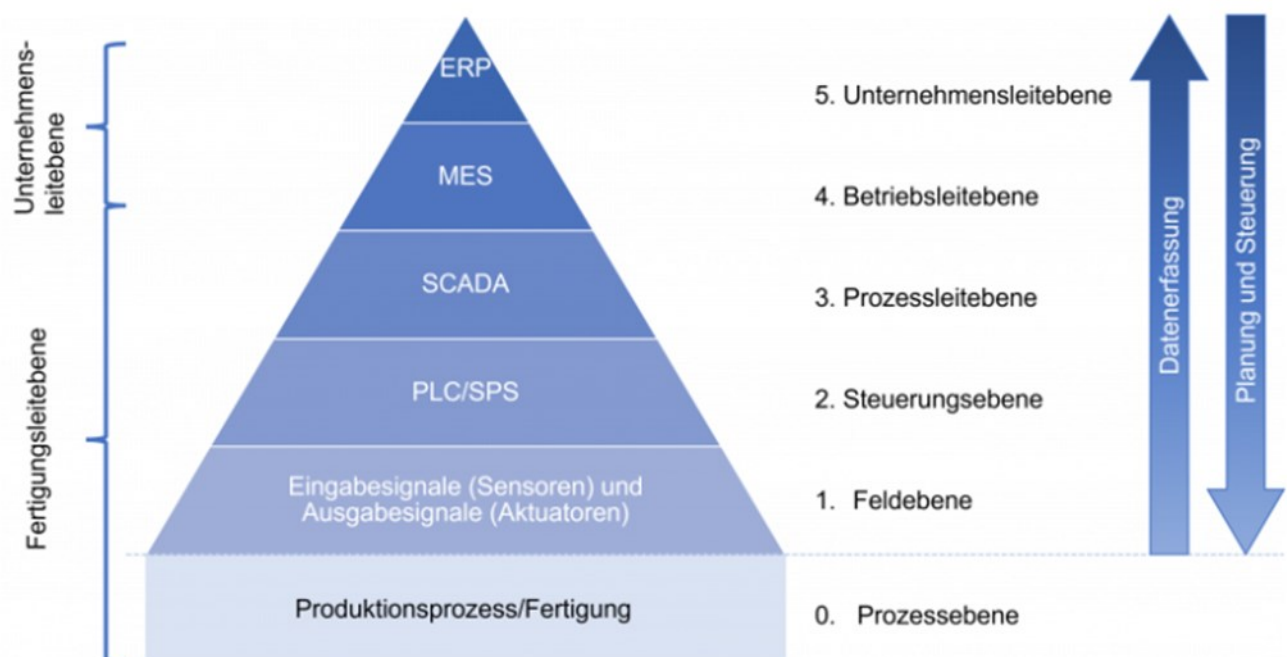


Bild 4.-1 IEC 62264 Ebenen (Level) der Prozessautomatisierung

- Ebene 0: Prozessebene**

Die Prozessebene ist die unterste Ebene auch Anlagenebene genannt. Hier findet die Fertigung, Herstellung statt.

- Ebene 1: Feldebene und Steuerungsebene.**

Zur Feldebene zählen Ein- und Ausgabegeräte, sowie Sensoren und Aktoren. Sensoren liefern dem Prozessleitsystem die erforderlichen Daten zum Ist-Status der Anlage. Dazu zählen Binärsignale, wie auch Analogwerte, beispielsweise Druck-, Temperatur-, Durchfluss- und Levelmessungen. Aktoren beeinflussen die Prozesse. Viele Sensoren und Aktoren können remote über ein HART (Highway Addressable Remote Transducer) Protokoll konfiguriert werden.

Die Anbindung der Feldebene an die Steuerungsebene erfolgt hartverdrahtet oder über Bus oder Feldbus (Beispiele: ,ProfiNet,, IEC 61850).

In der Steuerungsebene (SPS) werden Eingangssignale A/D gewandelt bzw. Ausgangssignale D/A gewandelt. Auf echtzeitfähigen SPS oder CPU-Baugruppen sind Programme geladen, wie Steuerungen und Regelungen, Schritketten und logische Verknüpfungen. Damit wird ein hochautomatisierter und - verfügbarer Betrieb der Anlage ermöglicht. Redundante Architekturen erhöhen die Verfügbarkeit der

Anlage. Sicherheitsrelevante Funktionen (Failsafe) werden mit speziellen Baugruppen, Ablaufstrukturen und Protokollen realisiert, welche stand-alone oder integriert sein können. Im Automatikbetrieb sollte die Anlage auch ohne Eingriffe vom PLS weiter betrieben und im Zweifel selbständig in einen sicheren Zustand fahren. Die Steuerungsebene kommuniziert über einen redundanten Automationsbus mit der PLS-Ebene.

- **Ebene2: Prozessleitsysteme (PLS).**

In dieser Ebene erfolgt die Bedien- und Beobachtung (BuB) der Anlage die Meldeverarbeitung und Protokollierung, die Archivierung der Daten sowie das Engineering.

Lediglich Kleinstlösungen sind als Einplatzsysteme ausgelegt. Erfolgt die Bedienung an mehreren Plätzen, dann ist eine Client Server Struktur vorteilhaft. Stand der Technik sind PLS, die webbasiert aufgebaut sind.

Das Langzeitarchiv befindet sich auf einem „Network Attached Storage“ NAS, ebenso das Meldearchiv. Das PLS überwacht alle intelligenten Baugruppen sowie die Kommunikation und stellt den aktuellen Status graphisch übersichtlich dar. Im Falle von Abweichungen und Störungen werden diese auch als Meldungen angezeigt. Die Darstellung der archivierten Signale und Werte erfolgt in Form von Protokollen und Standard Tabellen Dateien.

Applikation Server kommunizieren mit den Web-Clients über einen Applikations-Bus und den SPS/CPU über den Automationsbus. Applikation Server sind redundant ausgelegt; der Redundanzpartner besitzt das identische Prozessabbild des aktiven Applikation Servers. Daten werden zentral vorgehalten, damit ist ein effizientes, paralleles Engineering möglich. Das Engineering kann von jedem Bedienplatz erfolgen. Limitierungen bestehen lediglich durch die Anzahl der Lizenzen. Die Engineeringdaten sind immer „As-Built“. In der PLS-Ebene werden Lösungen zur Kopplung mit anderen Anlagen angeboten. So ist ein Multi-Unit Betrieb möglich. SPS/CPU anderer Anlagen lassen sich über geeignete Protokolle einbinden. Ebenso kann das PLS anderen Systemen Daten zur Verfügung stellen, beispielsweise als OPC-Server. Damit können verschiedene, lokal verteilte Warten verschiedener PLS-Lieferanten zu einer zentralen Warte zusammengelegt werden.

Datenübertragungssysteme sind Automations- wie auch Applikationsbus und als Industrial Ethernet mit einer Übertragungsgeschwindigkeit  $\geq 1$  Gbit/sec und im Design mindestens Ein-fehlertolerant ausgelegt. Die Verfügbarkeit und Sicherheit der Anlage kann durch eine geeignete Netztopologie verbessert werden. Der Datenaustausch mit SPSen oder Applikationsserver anderer Anlagen kann über Buskoppler oder Kommunikationsserver erfolgen. Nebenanlagen können über Black-Box Kopplungen eingebunden werden. Unter Berücksichtigung der IT Sicherheitsrichtlinie kann eine Verbindung zum Büronetzwerk wie auch ins Internet zu Servicezwecken als Fernwartungsschnittstelle eingerichtet werden.

- **Ebene 3: Betriebsleitebene (MES/Manufacturing Execution System):**

Anforderungen an höhere Verfügbarkeit sowie die Suche nach Optimierungsmöglichkeiten werden auf dieser Ebene forciert. Daten werden in Cloud-Servern gespeichert und mit Algorithmen ausgewertet. Basierend auf den gesammelten Daten können zum einen eine vorausschauende Wartung (predictive Maintenance) wie auch eine Wartung nach dem echten Verschleiß und nicht nach vordefinierten Wartungsintervallen berechnet werden oder zum anderen eine Verfügbarkeitsplanung für das Kraftwerk selbst (Kraftwerkeinsatzplanung).

- **Ebene 4: ERP (Enterprise-Resource-Planning)**

wird hier nicht näher betrachtet.

## 4.2 Allgemeine Anforderungen

Folgende Anforderungen werden an das Prozessleitsystem gestellt:

- Es kommt nur ein VGB-S-170-konformes System zum Einsatz, das bereits auf dem Markt etabliert ist. Das Prozessleitsystem ist zeitdeterministisch aufgebaut und hat eine Datenbasis für alle beteiligten Systeme. Die Bussysteme und die dafür erforderlichen Komponenten sind redundant und als Ring auszulegen. Die Auslegung der Bussysteme ist so auszugestalten, dass es bei Schalthandlungen zu keinen Verzögerungen der Befehlsgabe kommt und entsprechende Reserven vorhanden sind.
- Ein hoher Grad an Automatisierung und Verfügbarkeit der Automatisierungslösungen erlauben zentrale Bedienung und Engineering von verteilten Erzeugeranlagen (Multi-Unit). Die Systemarchitektur ermöglicht ein paralleles Multiengineering.
- Die Strukturierung der Anlage, Einstellungen, die Automatisierungslogik und die Bedien- und Beobachtungsfunktionen sowie eine umfassende Diagnostik erfolgt in einer integrierten Umgebung.
- Das Betriebssystem, Aufbau und Handling kann auf Microsoft® basieren, andere Systeme wie z.B. Linux sind auch möglich.
- Das Engineering greift auf eine zentrale gemeinsame Datenbasis für die Automatisierung und die Bedien- und Beobachtungsfunktionen zurück. Diese Strukturierung erfolgt sowohl für die Automatisierung als auch für die Bedien- und Beobachtungsfunktionen über eine gemeinsame Programmiersoftware, die auf entsprechende vom Hersteller festgelegte standardisierte Funktionsbausteine bzw. Bibliotheken nach VGB-S-170 zugreift.
- Das System ermöglicht ein aufwandsminimiertes Engineering. So sollte eine Online-Erweiterung der I/O im Rahmen der Kanalreserve, wie auch Steckplatzreserve flexibel und ohne Einschränkungen möglich sein. Neuhinzugefügte oder geänderte I/O werden automatisch erkannt. Das System schlägt eine Konfiguration vor, welche im Bereich Energieerzeugung üblich ist. Alternativ kann eine Konfiguration immer auch individuell erfolgen.
- Ein Einlesen von standardisierten I/O-Listen soll möglich sein. Die Listen beinhalten alle relevanten Daten zu den I/O-Signalen und -Werten, Grenzwerte und Meldungen.
- Feldgeräte mit HART-Funktionalität sind einzubinden. Die korrespondierende GSD-Datei beinhaltet relevante Information und Einstellmöglichkeiten, damit ist eine Konfiguration des Devices remote möglich ist. Das System soll auch eine GSD-Datei zur Verfügung stellen welche sich generisch, universell an die Anforderungen anpassen lässt. Die Zugriffe „Lesen“ und „Schreiben“ soll performant sein und im Sekundenbereich liegen.
- Das Engineering der Automatisierungsfunktionen erfolgt über ein grafisches Planungs-Tool. Dort werden hierarchische Baumstrukturen mit Knoten erzeugt, die Ablaufstrukturen zugeordnet werden. Zusätzlich zu den Bausteinen der Bibliothek kann der Anwender auch eigene Bausteine erstellen. Diese sollten aus einer Verschaltung einzelner Bibliothekbausteine bestehen. Der Grad der Individualisierung soll durch die Notwendigkeit der Aktualisierung der Systemsoftware - im Rahmen der Pflege und Erweiterung der Funktionalität - limitiert sein. Zur Verringerung der Komplexität können nicht benötigte Ein- oder Ausgänge an den Bausteinen der Bibliothek unsichtbar beschaltet werden. Werden Funktionen einzelner Bausteine nicht benötigt, sollten diese auch aus Performancegründen nicht in die SPS geladen werden. Systemseitig werden zugehörige Funktionsbausteine nach der Anlagenstruktur in den Plänen generiert. Die Verbindung der Ein- und Ausgänge kann manuell geschehen. Systemseitig erfolgt eine automatische Entflechtung.
- Das System bietet alle Funktionsbausteine, die einen hoch automatisierten Betrieb ermöglichen. So soll im Betrieb die Automatisierung, die Anforderung des Unitmasters umsetzen und entsprechend nach Vorgabe produzieren. Schrittketten ermöglichen ein automatisiertes An- und Abfahren, Steuerungen und Regelkreise einen optimalen Betrieb und



eine schnelle Reaktion auf Störungen. Eine adaptive Regelung ermöglicht einem optimierten Betrieb, das System passt die Regelparameter für einzelne Lastbereiche optimal ein. Damit können Transienten schneller gefahren werden. Basierend auf einer grundsätzlichen Strukturierung ermöglicht das System Änderungen und Erweiterungen online durchzuführen.

- Änderungen werden mit der Speicherung sofort in die SPS übertragen und können dort aktiviert werden. Ein zeitaufwändiges „Mapping“ ist nicht erlaubt.
- Im Engineering der Automatisierung wie auch BuB (Bedienen und Beobachten) steht eine „UnDo“-Funktion zur Verfügung. Über die Rückgängig Taste kann der Anwender Eingaben zurückspringen.
- Dynamisierte Funktionspläne zeigen Werte und Zustände im Plan an und unterstützen bei der Fehlersuche. Werte und Signale lassen sich auch über mehrere Pläne einfach durch Auswahl des Konnektors aufrufen und verfolgen. Werte von Baustein-Ports können auch mit Ersatzwerten überschrieben werden. Aktive Ersatzwerte sind automatisch farblich gekennzeichnet und werden zusätzlich in einer Liste geführt.
- Alle Pläne sind im Layout gemäß den Mainova-Anforderungen zu individualisieren.
- Im Engineering werden basierend auf der hierarchischen Struktur der Automatisierungsfunktionen Anlagenbilder automatisch oder manuell erzeugt, basierend auf den grafischen Symbolen der eingesetzten Bibliothekbausteinen/Piktogrammen. Diese können im Anlagenbild frei platziert werden. Diese grafischen Symbole korrespondieren mit den Funktionsbausteinen und beinhalten Face Plates für die Bedienung sowie Einzelbilder mit Status- und Diagnoseanzeigen. Änderungen der Automatisierungsfunktionen bedingen automatisch auch Änderungen in den korrespondierenden Bildern des BuB.
- Die Engineering-Umgebung beinhaltet ein Versionsmanagement für Zwischen- und Hauptversionen. Dazu steht eine Back-up Möglichkeit zur Verfügung, die es erlaubt Kopien von Zwischen- und Hauptversionen außerhalb des Systems zu speichern.
- Im Falle einer sicherheitsgerichteten Abschaltung der Anlage ist es für das Servicepersonal unerlässlich, die Ursache der Abschaltung eindeutig zu identifizieren. Zu diesem Zweck stellt das Leitsystem verschiedene Diagnosewerkzeuge bereit, darunter das Störablaufprotokoll sowie Erstwertmeldungen. Da einzelne Auslösesignale oft nur durch wenige Millisekunden voneinander getrennt sind, ist eine präzise zeitliche Erfassung erforderlich. Diese Signale werden daher mithilfe von Digitaleingabebaugruppen mit einer Auflösung von einer Millisekunde hochgenau erfasst. Die Ausgabe der erfassten Daten erfolgt über das SOE-Protokoll (Sequence of Events) oder die Erstwertmeldung.
- Die systemseitig gespeicherte Dokumentation des Anlagenengineerings und der Systemkonfiguration entspricht stets dem aktuellen ‚As-Built‘-Stand und erfüllt die Anforderungen gemäß VGB-S-170. Dies sind z.B. Funktionspläne, Grenzwert- und Sollwertlisten, Passwortphilosophy etc.
- Das System soll Nutzerorientiert sein, eine Online-Hilfe Funktion kontextabhängig und über ein Suchfenster dem Nutzer eine effiziente Alternative zur papiergebundenen Systemdokumentation bieten. Tutorials zeigen dem Nutzer einzelne, nicht alltägliche Tätigkeiten wie Anlegen eines Projekts, Einfügen eines Automatisierungsservers oder einer zusätzlichen I/O-Baugruppe. Ziel ist es, das Engineering sämtlicher Funktionen in einer möglichst einheitlichen Umgebung mit konsistentem Aussehen und Handhabung durchzuführen.
- Das Engineering greift auf eine zentrale gemeinsame Datenbasis für die Automatisierung und die Bedien- und Beobachtungsfunktionen zurück. Diese Strukturierung erfolgt sowohl für die Automatisierung als auch für die Bedien- und Beobachtungsfunktionen über eine gemeinsame Programmiersoftware, die auf entsprechende vom Hersteller festgelegte standardisierte Funktionsbausteine bzw. Bibliotheken nach VGB-S-170 zugreift. Das System ermöglicht dadurch ein aufwandsminimiertes Engineering.

- So sollte eine Online-Erweiterung der I/O im Rahmen der Kanalreserve, wie auch Steckplatzreserve flexibel und ohne Einschränkungen möglich sein. Neu hinzugefügte oder geänderte I/O werden automatisch erkannt. Das System schlägt eine Konfiguration vor, welche im Bereich der Energieerzeugung üblich ist.
- Der Signalaustausch soll unabhängig von der Struktur des Datenübertragungssystems und so programmierbar sein, dass alle Signale an jeder Systemkomponenten uneingeschränkt zur Verfügung stehen. Zwischenkopplungen sollten so weit wie möglich vermieden werden.
- Einheitliche Verbindungstechnik wie z.B. Zugfederklemmen/ Push-In (Schraubklemmen sind zu vermeiden) ist anzuwenden.
- Verfahrenstechnische Redundanzen sind im Prozessleitsystem abzubilden und in den Schrankkonzepten zu berücksichtigen.
- Die Ankopplung der einzelnen Systemkomponenten an das Datenübertragungssystem muss rückwirkungsfrei erfolgen, so dass der Ausfall einer Einheit die Signalübertragung zwischen den übrigen Einheiten nicht beeinträchtigt.
- Das Datenübertragungssystem muss in der Lage sein, Signale in Echtzeit zu übertragen (zeitfolgerichtig, ereignisgesteuert, Auflösung im Millisekundenbereich). Für die Zeitsynchronisierung über alle Prozessleitsystemkomponenten ist eine Funkuhr mit Quarzausfallüberbrückung und/ oder eine GPS-Uhr einzusetzen).
- Das Datenübertragungssystem ist so auszulegen, dass eine problemlose Erweiterung oder Reduktion der Peripherie - und gegebenenfalls des Datenübertragungssystems selbst - möglich ist, ohne dass sich die im Betrieb befindlichen Anlagenkomponenten stillgesetzt werden müssen oder deren Verfügbarkeit eingeschränkt wird.
- Die Automatisierung ist hierarchisch mit Funktionsplan (FUP) und Funktionsgruppen zu strukturieren. Die einzelnen Hierarchieebenen sind autark abzubilden. (siehe auch Kapitel Aufbau/ Programmierung/ Konfiguration Automatisierungsebenen).
- Beistellung aller notwendigen Engineering- Werkzeuge für die Wartung und Pflege des Prozessleitsystems (Hotfixes, Updates, Servicepacks, etc.) - möglicherweise auch über Serviceverträge.
- Alle leittechnischen Komponenten müssen, soweit möglich und sinnvoll, im Rahmen des Gesamtkonzeptes einheitlichen und untereinander gleichwertigen Anforderungen an Ausrüstung, Ausgestaltung, Sicherheit, Verfügbarkeit und Bedienbarkeit gerecht werden.
- Einbau, Ausbau und Austausch beliebiger einzelner Komponenten muss im laufenden Anlagenbetrieb ohne weitere Störung des Prozesses oder der Leitanlage möglich sein.
- Eine Hardwarereserve (Steckplätze, Kanalreserve etc.) von 20% nach Abnahme ist zu gewährleisten. Die Reserve ist über das ganze System zu verteilen.

## 4.3 Redundanz

- Alle Automatisierungskomponenten müssen redundant einsetzbar sein. Erfolgt die Automatisierung weitgehend in intelligenten Zentraleinheiten mit wenig intelligenten Ein-/Ausgabebaugruppen, sind die Zentraleinheiten redundant auszuführen. Der redundante Einsatz der Schaltkomponenten muss bedarfsgerecht festgelegt werden.
- Mögliche Aufstellung von redundanten Systemen in getrennten Brandabschnitten ist projektspezifisch abzuklären.
- Um eine höchstmögliche Verfügbarkeit des Leitsystems sicherzustellen, ist das Datenübertragungssystem mit allen Ankopplungskomponenten an die Automatisierungseinheiten (Automatisierungs- und Visualisierungsbussysteme) redundant auszuführen.

- Die Umschaltung zwischen redundanten Komponenten muss automatisch, unterbrechungs- und stoßfrei erfolgen. Störungen in der Redundanz sowie Redundanzumschaltungen und deren Ursachen sind zu detektieren und zu melden.

## 4.4 Funktionale Sicherheit von sicherheitstechnischen Systemen

Errichtung und Betrieb von Anlagen mit Gefährdungspotential unterliegen der internationalen Norm IEC 61511, dem Standard für die funktionale Sicherheit sicherheitstechnischer Systeme.

Die Beschreibung der Vorgehensweise zur Realisierung der funktionalen Sicherheit folgt hier dem Sicherheitslebenszyklus (Safety Lifecycle) der Anlage, der in folgende drei Phasen gegliedert ist: Analysephase, Realisierungsphase sowie Betriebs- und Wartungsphase.

Generell sind alle diese Phasen und die damit verbundenen Tätigkeiten für die funktionale Sicherheit zu dokumentieren.

### Analysephase

Im Rahmen einer Risikoanalyse werden zunächst alle vorhandenen Risiken identifiziert. Für jedes erkannte Risiko muss anschließend ermittelt werden, ob dieses der Reduzierung bedarf. Ist dies der Fall, so muss die jeweils erforderliche Risikoreduzierung quantifiziert werden. Dies geschieht durch den Einsatz von Risikobewertungsmethoden, anhand derer die erforderlichen SIL-Anforderungen bestimmt werden.

Eine niedrige SIL-Anforderung (SIL 1) bedeutet hierbei, dass nur eine geringe Risikoreduzierung notwendig ist. Ein höherer SIL (zum Beispiel SIL 3) erfordert ein entsprechend größeres Maß an Risikoreduzierung.

Sowohl zur Identifizierung von Risiken als auch zur Quantifizierung der gegebenenfalls nötigen Risikoreduzierung stehen diverse Verfahren zur Verfügung, die üblicherweise mit Softwareunterstützung zur Anwendung kommen. Die Identifikation von Risiken wird häufig mit Hilfe der „Hazard and Operability Study“ (kurz HAZOP) durchgeführt. Um die erforderliche Risikoreduzierung zu quantifizieren (SIL-Ermittlung), sind unter anderen Risikographen, LOPA („Layer of Protection Analysis“) und Risikomatrix gebräuchliche Methoden.

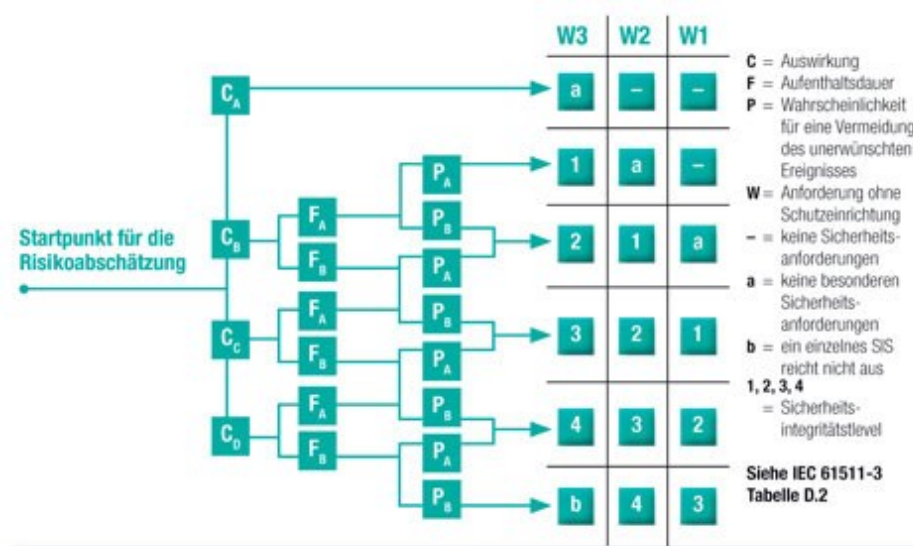


Bild 4-3 Der Risikograph

Entsprechend der Risikoermittlung sind Maßnahmen nach IEC61511, 61513 und 62061 in der Anlage und im Prozessleitsystem zur Reduktion des Risikos erforderlich. Ein wesentliches Ergebnis der Analyse ist die Spezifikation der Sicherheitsanforderungen (Safety Requirement Spezifikation, SRS), die alle Sicherheitsfunktionen (Safety Instrumented Functions, SIF) einschließlich der an sie gestellten Anforderungen aufzeigt und den geforderten Safety Integrated Level (SIL) vorgibt.

- **Realisierungsphase**

Die SRS ist die Grundlage für die weitere Anlagenplanung, insbesondere für die Auslegung des sicherheitstechnischen Systems (SIS) und dessen Sicherheitsfunktionen sowie für weitere Maßnahmen zur Risikominderung. Sie ist maßgebend für die Auswahl des SIS sowie der Hardware und Software zur Realisierung der Sicherheitsfunktionen.

Das System bietet zur Realisierung spezielle Hardwarekomponenten sowie eine sichere Datenübertragung. Es umfasst außerdem einen eigenen Runtime-Container auf der SPS, spezielle Funktionsbausteine und eine dedizierte Engineering-Umgebung. Diese ist vom TÜV zertifiziert für Sicherheitsanwendungen bis SIL 3 gemäß IEC 61508. - „State of the Art“ Prozessleitsysteme bieten dies in einer „Safety Integrated“ Umgebung.

Failsafe Eingabebaugruppen können auf der I/O-Ebene zusammen mit Non-Failsafe Baugruppen betrieben werden. Gleiches gilt für den Feldbus wie auch die SPS. Im Engineering sind die Anforderungen für Failsafe voll integriert. Das Engineering erfolgt in gleicher Weise graphisch in Funktionsplänen. Für die Failsafe-Anwendung wird im Engineering eine Bibliothek eingefügt. Das Engineering Tool des Prozessleitsystems bietet ein integriertes Safety Matrix Engineering Tool. Ein Online- und ein Offline-Betrieb muss möglich sein.

Somit werden sicherheitsgerichtete Abschaltungen einzelner Aggregate bei gefährlichen Abweichungen bis zum gesicherten Shutdown durch Auslösung des MFT (Master Fuel Trip) gewährleistet.

Die Genauigkeit der Erfassung der relevanten Eingangssignale muss eine Millisekunde betragen.

- **Betriebs- und Wartungsphase.**

Mit einem Tool lassen sich im Betrieb die Zustände der Safety Matrix (Verriegelungsmatrix) im Onlinebetrieb visualisieren.

## 4.5 IT-Sicherheit

Der IT- Sicherheit muss unbedingt Folge geleistet werden. Deswegen wird hier auf separate Werknormen und Richtlinien verwiesen, die zu beachten sind.

Siehe hierzu:

- VR7.05.01 Informationssicherheitsrichtlinie
- OT/ IT Security Lastenheft

## 5. Komponenten

### 5.1 Ein/- und Ausgabebaugruppen

Jeder einzelne Analog- und Binärwert aus dem Prozess ist in einer Analog- bzw. Binärwertaufbereitungsbaugruppe zu erfassen und zu verarbeiten. Die Aufbereitungsbaugruppen sollen die folgenden Merkmale besitzen:

- Eignung zum Anschluss und Parametrierung von HART-Messumformern ohne Beeinträchtigung der Verarbeitungsfunktion auch während der Parametrierung über die Messsignalleitung.
- Die Messwertumformer- bzw. Geberversorgung erfolgt grundsätzlich über die Messsignalleitung (2-Draht-Technik) aus der entsprechenden Eingabebaugruppe.
- Die Speisung der 2-Draht-Messumformer muss kurzschlussfest und selektiv sein.
- Die Geberversorgung muss für fremdgespeiste Signalquellen bei sonst unveränderter Funktionalität abschaltbar sein.
- Messgeräte mit externer Spannungsversorgung werden standardmäßig mit 24V DC ( $\pm 20\%$ ) fremdversorgt. In Ausnahmefällen ist 230V AC zulässig.
- Die Rückwirkungsfreiheit auf andere Kanäle u.a. durch Einzelabsicherung ist zu gewährleisten.
- Jeder Geberanschluss ist auf Drahtbruch, Kurzschluss und Speisungsausfall zu überwachen und Störungen sind zu melden.
- Die Aufbereitungsbaugruppen sind auf ihre Funktionalität zu überwachen und Störungen zu melden.
- Jede Messung und jede ihrer Verarbeitungsfunktionen muss über das Datenübertragungssystem online, unterbrechungsfrei und zeitnah generiert, gelöscht, verändert und simuliert werden können.
- Alle Binärsignale sind am Systemeingang mit einem Zeitstempel zu markieren. Das gilt auch für alle verarbeiteten Signale sowie von Analogwerten abgeleitete Grenzwerte im System.

### 5.2 Bediener PCs (Clients)

Arbeitsplatzrechner und/ oder KVM-Extender (Keyboard, Video, Mouse) sind mit 4-fach Multi-Monitor-Karte zum Anschluss von vier Monitoren auszurüsten. Die Bedienung erfolgt mittels kabelgebundener festangeschlossener Tastatur und Maus. Alle KVM-Komponenten sind IP basierend auszuführen. Komponentenausfälle oder Störungen des Rechners (Platte, Netzteil etc.) sind im Bediensystem zur Anzeige zu bringen und zu melden.

Jeder Arbeitsplatz ist mit zeitlich unbegrenzten Herstellerlizenz und den zugehörigen Lizenznachweisen auszustatten.

### 5.3 Engineering Stationen

Engineering User Software Lizenzen sind vorkonfiguriert mit zeitlich unbegrenzten Herstellerlizenz und den zugehörigen Lizenznachweisen auszustatten. Ein Umschalten von der Engineering-Ebene auf die Bediener Ebene muss jederzeit möglich sein. Generell müssen die Zugriffsberechtigungen auf Bedien-/ bzw. Engineering Stationen projektspezifisch festgelegt werden (Passwort bezogen und/ oder Passwort bezogen mit Personen bezogenen Ausweis).

## 5.4 Server PC Prozessdatenbank/ Meldungen/ Langzeitarchivierung

Eine Vorhaltung einer Prozessdatenbank ist Grundbedingung.

- Für Ereignisse, Störungen und Abweichungen werden Meldungen erstellt. Das Engineering von Meldungen im System erfolgt vereinfacht durch das Einlesen von Daten aus einer Tabelle oder auch einzeln. Meldungen werden visualisiert über die Meldefolgeanzeige MFA in der oberen Bildmitte. Über eine projektierte Taste in der Fußzeile gelangt der Anwender vom BUB in die Meldungsverarbeitung. Dort gibt es verschiedene Darstellungen für Meldungen gleichen Typs (Kommen, Kommen quittiert, Kommen Gehen, nicht quittiert, Archiv) auf korrespondierenden Meldeseiten. Von dort lassen sich ebenso Protokolle mit archivierten Signalzuständen zusammenstellen, darstellen, drucken und als Datei exportieren. Die Meldeverarbeitung soll in der Systemauslegung der Anlage einen Meldeschwall verarbeiten, ohne Meldungen zu verlieren. Dabei soll sich die Aktualisierungszeiten der Bilder nicht mehr als verdoppeln, ebenso die Signallaufzeit für Bedienungen von der Bedienaktion bis zur Klemme der Ausgabebaugruppe.
- Meldungen, binäre und analoge Signale können nach Auswahl gespeichert werden. Bei Kleinkonfigurationen sind die Archive auf den Automatisierungsservern installiert, größere Prozessleitsysteme verfügen über eine ausgelagerte Speicherung, NAS (Network Attached Storage).
- Gespeicherte Daten aus dem Archiv lassen sich im System in verschiedenen Weisen darstellen: Als Kurvenbild, Protokoll und in Tabellenform im MS-Excel Format zur weiteren Verarbeitung, wie auch schreibgeschützt im PDF-Format. Dazu gibt es fest projektierte Tabellen wie auch Kurven und ebenso vom Anwender frei projektierbare Kurven- und Tabellendarstellungen.
- Daten für Langzeitarchivierung werden auf einen Datenspeicher ausgelagert (Swapping Out), zur Ansicht können diese wieder in den Systemspeicher eingelesen werden. Die Archivierung von Meldungen und Analogwerten mit Einsatz einer NAS erfolgt redundant - nach Raid Level 1 (Bei dem Archiv handelt es sich um ein Umlaufarchiv). Dabei ist die Kapazität so auszulegen, dass Archivdaten mindestens zehn Jahre zurückliegend verfügbar sind.

## 5.5 Monitore/ Großbildschirme

Mindestanforderungen an alle Monitore und Displays:

- Ausführung: State of the Art
- Geeignet für den 24 / 7 Stunden-Einsatz
- Hohe Helligkeits- und Kontrastwerte.
- Signaleingänge: HDMI, Displayport
- Audio, integrierte Lautsprecher

## 5.6 Systemauslastung, CPU und Netzwerk

- Das Baugruppenspektrum ist zu minimieren. Stehen in zentralteilbasierten Systemen mehrere CPU-Typen zur Auswahl, so ist nur diejenige einzusetzen, die am stärksten belasteten Teilsystem noch die geforderte Leistungsreserve erbringt.
- Zentrale Komponenten (CPUs, Kommunikationsprozessoren, etc.) sind, wenn technisch möglich so auszuwählen, dass sowohl geringe Anforderungen an Sicherheit (SIL 1) wie auch hohe Anforderungen (SIL 3, z.B. im Kesselschutz) abgedeckt werden.

- In zentralteilbasierten Systemen sollen redundante CPU's und alle Anwenderbaugruppen in Automatisierungsschränken eingebaut werden.
- Die gesamte Systemauslastung innerhalb der Automatisierungseinheiten darf zu keinem Zeitpunkt 60% überschreiten (Überprüfung muss System intern möglich/ ersichtlich sein).
- Die Belastung der Busse (z.B. Ethernet) darf niemals 30% überschreiten (Überprüfung muss System intern möglich/ ersichtlich sein).

- 

- Ersatzteile, Serviceunterstützung und Lieferbarkeit von Hardwarekomponenten und Serviceunterstützung der gesamten Software (auch 3rd Party) muss für noch mindestens 15 Jahre gegeben sein. Dies hat der Lieferant entsprechend vor der Realisierung zu bestätigen.

In diesem Zeitraum ist die sichere Funktionalität des Systems zu gewährleisten. Im Falle eines Defekts von Baugruppen auf der EA-Ebene sind steckplatzkompatible Ersatzbaugruppen verfügbar. Für alle anderen Produkte und Komponenten sind funktionskompatible Ersatzteile freigegeben und erhältlich. Werden Betriebssysteme abgekündigt, ersetzt der Lieferant diese durch jeweilige Nachfolgeprodukte (Dies kann zum Tausch von Rechnern führen).

Funktionskompatible Nachfolgeprodukte und -komponenten außerhalb der EA-Ebene garantieren den Betrieb der Anlage.

- Die betriebliche Sicherheit der Anlage muss über die Systemlaufzeit gegeben sein. Erkannte Sicherheitslücken in den Betriebssystemen, die von Herstellern beseitigt wurden, müssen zeitnah kommuniziert und dem Auftraggeber zur Verfügung gestellt werden.

## 5.7 Leittechniksschränke

Alle Systemkomponenten sind in Standardschränken einzubauen. Es wird zwischen folgenden Schrankarten unterschieden:

- Elektronikschränke für Automatisierung
- Elektronikschränke für Hilfselektronik
- Spannungsversorgungsschränke
- Koppelschränke
- Rechner/ Serverschränke
- Hilfsschränke.

Nähere Beschreibung ist aus der ERZ WN 00135 zu entnehmen.

Für anzubietende Reserve- und Verschleißteile im Bereich der Elektrotechnik und Leittechnik ist folgender Umfang zu berücksichtigen:

Als Reserveteile für die Elektro- und Leittechnik sollen 20 % der eingebauten Komponenten (z.B. Baugruppen, Netzteile, Spezialkomponenten, etc.) vorgesehen werden.

## 6. Aufbau/ Programmierung/ Konfiguration Automatisierungsebenen

Die Funktion der Automatisierung ist so zu verwirklichen, dass:

- ein vollautomatischer Betrieb (u.a. An- und Abfahren, Laständerungen, Stillstand und Störungen) gegeben ist.
- zentrale Prozessüberwachungen und -steuerungen ausschließlich über Bildschirme und Großbildwand möglich ist.
- die Aufgaben, die ein Bediener im Leitstand ausführt, in allen Betriebsphasen durchgeführt werden können.
- die Anlage über ein Blockleitprogramm und Regelung gefahren werden kann.
- der Bediener im Leitstand in allen Betriebsphasen die Möglichkeit hat, in die Automatik einzugreifen.

Die Funktionen sind standardisiert und in klaren Strukturen aufzubauen. Sie erfolgt in hierarchischer Form durch verschiedene Funktionsbausteine in verschiedenen Automatisierungsebenen wie folgt:

### 6.1 Prozess- und Blockleitebene

Diese obere Ebene beinhaltet Sollwertführungs- und Steuereinrichtungen, die auf die nächstgelegene (untere) Gruppenleitebene Einfluss nehmen. Z.B. werden hier in dieser Ebene bedient und beobachtet, Blockregelungen und Meldungsüberwachung vollzogen.

Sämtliche Betriebsarten der Anlagen wie An- und Abfahren, Laständerung und Stillstand werden hier koordiniert.

### 6.2 Gruppenleitebene

In dieser Ebene werden Gruppen- und Untergruppensteuerungen, Betriebsautomatiken und Führungsregelungen verwirklicht. Es können mehrere Ebenen aufgeteilt werden in Bezug auf die verfahrenstechnischen Systeme. In dieser Gruppenleitebene muss ein Handeingriff möglich sein.

### 6.3 Einzelleitebene

Bei dieser Ebene werden die Antriebssteuerungen, Einzelregelungen, die Signalaufbereitung und den Schutz/ Verriegelung verwirklicht. Handeingriffe auf die Einzelleitebene müssen auch hier möglich sein.

Generell gilt noch zu Programmierung und Konfigurierung:

- Alle leittechnischen Funktionen wie Freigaben, Automatikbefehle, Schutzverriegelungen, Funktionsgruppensteuerungen, Vorwahlen, Antriebssteuerungen, Regelungen und andere Hilfsfunktionen sind über einen dynamischen Prozess FUP (FunktionsPlan) sichtbar für den Anlagenfahrer durchzuführen. Für die Hauptfunktionsbausteine muss ein standardisierter, vorkonfektionierter Signalaustausch im Prozessbedien- und Beobachtungssystem vorhanden sein.
- Alle Regelungs- und Steuerfunktionen sind so zu konfigurieren, dass in allen stationären und nicht stationären Betriebszuständen der Anlage die Sollzustände der Prozessgrößen sicher erhalten bleiben. Das ordnungsgemäße Verhalten der Regelkreise auf Sollwert- und Störgrößen sprünge ist nachzuweisen. Die zugesicherten Eigenschaften sind durch Nachweismessungen zu belegen, in Bezug auf Regelgüte (Überschwingweite und Ausregelzeit).

Zusätzlich sollte die Konfigurationssoftware folgende Möglichkeiten besitzen:



- Jedes Gebersignal muss mit analogen bzw. binären Filterfunktionen korrigierbar sein (z.B. lineare und nichtlineare analoge Filterfunktionen, Radizierung, Nullpunktunterdrückung, Druck- und/oder Temperaturkorrektur, Schwellwertvorgabe, einstellbare Änderungsrate usw.).
- Ein „manipuliertes“ oder korrigiertes Messsignal darf sich in der Bedienbarkeit nicht von einem „rohen“ Messwert unterscheiden. Es muss aber ersichtlich sein, dass es manipuliert/ simuliert ist (forced signal).
- Die Analogsignalverarbeitung muss Grenzwertvergaben mit maximal möglicher Anzahl erlauben.
- Die Verarbeitung von Grenzwerten, binären Messungen oder gebildeten Signalen als Meldung muss steuerbar sein (Priorität, Unterdrückungssignal usw.).
- Alle Messwerte sind über das Datenübertragungssystem den übrigen Leitsystemkomponenten zur Verarbeitung anzubieten.
- Jede Messung sollte von jedem Bedienplatz bedien- und beobachtbar sein unabhängig von Signalform und Ursprung.
- Es kommen standardisierte Funktionsbausteine nach DIN EN 61131 zum Einsatz. Alle eingestellten prozessabhängigen Werte und Parameter müssen im Funktionsplan (FUP) dokumentiert sein.
- Funktionsmakros für Steuer- und Regelfunktionen.  
Es müssen projektierbare Eingänge für Schutz, Automatik, Freigaben und Handansteuerung (BuB- Bedienung, Vor- Ort Bedienung) mit einstellbarer Priorität vorhanden sein.
- Sämtliche Funktionen wie Sollwerte, Gruppensteuerungen, Analogwerte (Grenzwerte), Antriebssteuerung bzw. -regelung und jede ihrer Verarbeitungsfunktionen etc. muss über das Bussystem online, unterbrechungsfrei und zeitnah generiert, gelöscht, verändert und simuliert werden können.
- Bei Hardwarestörungen innerhalb eines Regelkreises muss die Umschaltung von Automatik- auf Handbetrieb automatisch erfolgen. Zur gleichartigen Behandlung bei Prozessstörungen muss ein zusätzlicher konfigurierbarer Funktionseingang vorhanden sein.
- Die Zeiten der Antriebssteuerbefehle sind einstellbar auszuführen, so dass auch langsam schaltende Antriebe sicher geschaltet werden.
- Die Antriebslaufzeiten sind zu überwachen.
- Die Standard-Prozessschnittstelle zwischen Softwarebaustein und Hardware muss mit freien Signalen beeinfluss- bzw. überschreibbar sein (Bsp.: Aus zwei externen Endschaltern wird eine Rückmeldung für einen Antrieb gebildet).
- Für die Prioritätensteuerung von Hand-, Automatik- und Schutzsignalen gelten die im „Konzept der Automatisierung“ festgelegten Regeln.
- Einstellbare Abtastzeiten von 100 bis 1000ms haben sich in verfahrenstechnischen Bereichen als ausreichend erwiesen. Für schnellste Regelungen (Turbine, Netz) sind Zykluszeiten von 1ms gefordert. Dies wird meistens mit einem untergeordneten Leitsystem für die Turbinenregelung verwirklicht (Stichwort: Zykluszeiten).
- Der Informationsgehalt von Antrieben oder der Schaltanlage sollte/muss vollständig über autarke Signale (nicht errechnete Signale) abgebildet werden. (z.B.: Eine Endposition eines Antriebes/ Ventils solle mit einem Endlagenschalter abgebildet werden und nicht über die Laufzeit).

## 7. Funktionen des Bedien- Beobachtungssystems

### 7.1 Dynamische Darstellung des Prozesses

- Der Prozess ist mit Hilfe von genormten Symbolen und Farben darzustellen.
- Prozessgrößen können in Prozessbildern, Trends, Kennlinien- bzw. Kurvenbildern angezeigt werden. Neben Zahlenwerten mit Einheiten sollen auch Darstellung von Balken- und Zeigerdarstellungen möglich sein.
- Dynamische Funktionspläne (FUP) sind mit Anzeige der Prozesswerte und Status auszuführen.
- Zustandswerte sind mit einheitlichen Farbcodierungen auszuführen. Änderungen über Farbumschlag oder blinken darstellen. Farbcodierungen können auch nach lokalen beim Betreiber üblichen Ausführung angepasst werden.
- Der Bediener sollte sich frei konfigurierbare Kurvenbilder (Trends) anlegen können (mit jeweils mindestens 6 Kurven). Die Konfiguration bzw. Zusammenstellung sollte einfach per Drag & Drop erfolgen können. Auch sollten errechnete Zwischenergebnisse/ Sollwerte aus Kalkulationsblöcke in den Kurvenbildern darstellbar sein.
- Darstellungen in Fenstertechnik (Window pop-up).
- Zugriff auf Standard MS-Office Pakete wie Word und/ oder Excel sollte User- und Rechteabhängig möglich sein zwecks Berichterstellung.

## 7.2 Alarm Management

- Systemweite Erfassung aller Prozessstörungen und Störungen/ Fehler in den Systemen des Leitsystems.
- Sinnvolle Verdichtung und Reduktion von Meldungen in Abhängigkeit des Anlagenzustandes.
- Erstwertmeldung und Meldefolgeunterdrückung.
- Stillstandsunterdrückung, z. B. Druck Min nur aktiv, wenn Pumpe läuft, (nach Ablauf einer Anfahrüberbrückung).
- Navigationsmöglichkeit zu den zugeordneten Prozessbildern je Alarm.
- Langzeitspeicherung der Alarme
- Optische und akustische Alarme, quittierbar.
- Alarmzeilen sollen unverdeckbar sein, nach Funktion sortierbar.
- Alarmierung/ Meldung von nicht erfüllten Kriterien bei Sequenzabläufen.
- Liste der Alarme auf allen Visualisierungssysteme mit KKS, Alarmtext- und Zustand (mit Farbunterschied), sortiertem Zeitstempel.

## 7.3 Führung der Bediener

- Hierarchische Struktur der Prozessbilder in Bereichen, Gruppen und Details.
- Navigationsmöglichkeiten zu den zugehörigen Anzeigen.

## 8. Feldgerätevisualisierung

Standardisierte Oberflächen und Tools für eine effizientere Inbetriebnahme und Betrieb sind zu berücksichtigen (z.B. zu viele Schulungen mit unterschiedlichen Tools).

Parallel zur Messwertverarbeitung im Leitsystem muss eine Serviceebene für die Feldinstrumentierung vorhanden sein, die eine zentrale Parametrierung, Diagnose und Inbetriebnahme ermöglicht. Ein Diagnose- und Serviceplatz für Feldgeräte sollte eingerichtet werden, bei dem die Funktionalitäten herstellerspezifischer Engineering- und Diagnosetools in das Engineering-System des Leitsystems integriert sind. Z.B. Bereitstellung der notwendigen Dienste wie Signalrangierung, Zugriffe für

- Feldbusse
- HART Protocol
- Ethernet etc.

## 9. Schnittstellen/ Kopplung

Das System verfügt über performante Schnittstellen zur Anbindung von Dezentralen Steuerungen (Blackboxen), Schaltanlagen, Integration anderer Anlagen wie auch Möglichkeiten zur Integration in übergeordnete Anlagen. Je nach Anforderung zur einfachen Übertragung von Daten oder auch zeitgestempelten Signalen und Werte. Dazu zählen: Die Anbindung können über Modbus TCP/RTU, SIMATIC S7-300, S7-400 S7-1200/1500 Interface, Multi-Unit Kommunikation, OPC UA Server und Client. Über ein generisches Prozessbus Interface können auch andere Komponenten verknüpft werden. Es ist darauf zu achten, dass möglichst standardisierte Schnittstellen eingesetzt werden. Selbst programmierte Schnittstellen und Protokolle sind zu vermeiden.

Internet-Verbindungen (siehe auch Verbundrichtlinie VR 7.05.01 Informationssicherheit) sind, wenn möglich über Bürokommunikation zu bilden (separate PCs mit Firewall und sicher VPN-Verbindung. Direkte Glasfaserverbindung (Punkt zu Punkt) sind soweit möglich vorzuziehen. Verbindungen über Sendemasten (z.B.) LTE sind zu vermeiden.

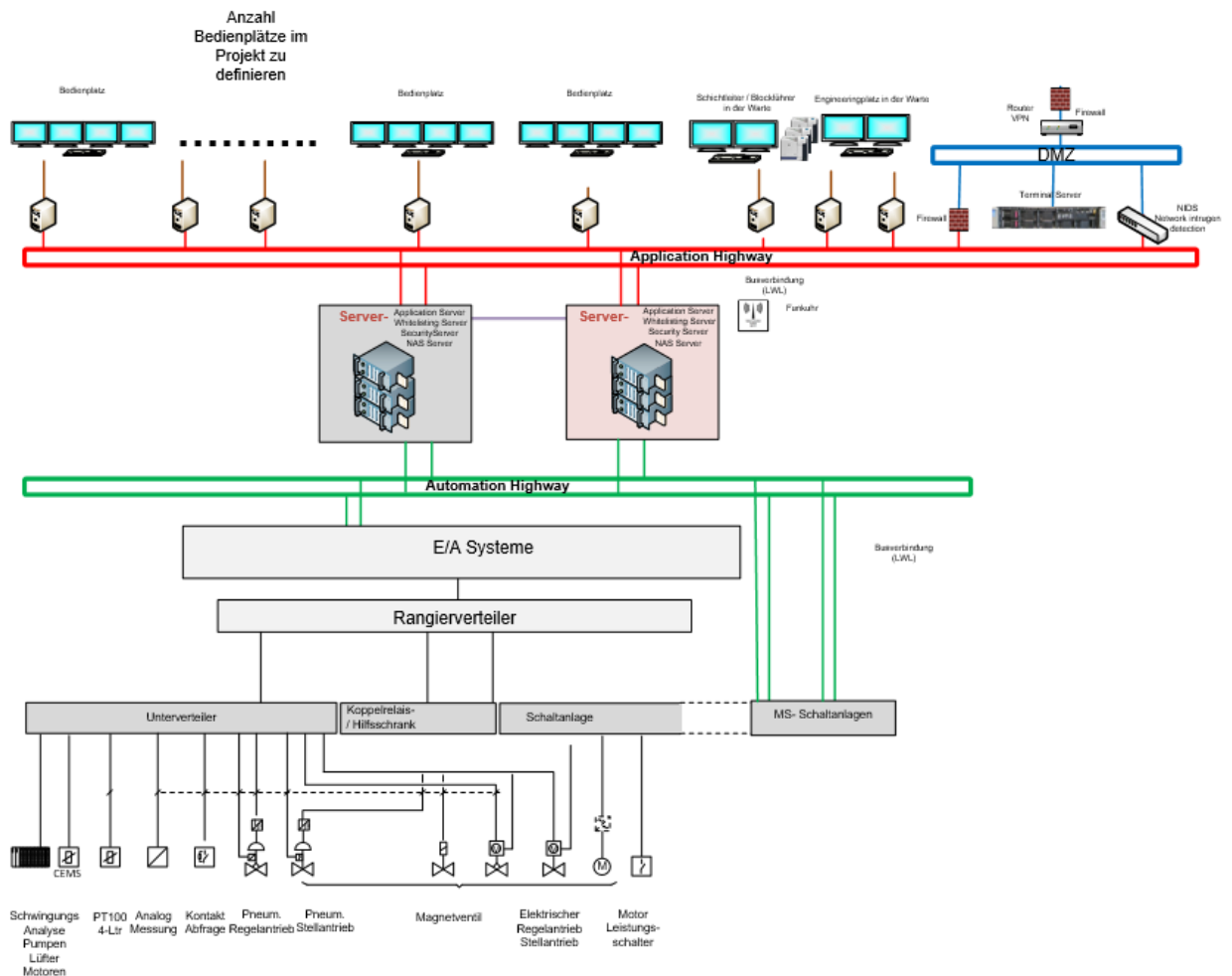
## 10. Dokumentation

Eine effektive Betriebs- und Prozessführung kann nur durch einen schnellen Zugriff auf die vollständige und aktuelle Dokumentation gewährleistet werden, in dieser befinden sich:

- Funktionale Abläufe und Bausteinbeschreibungen
- Gerätetechnische Beschreibung
- Regelkreisbeschreibung, -schemata
- Betriebshandbuch vom Leitsystem Patchmanagement
- Wartungsanweisungen
- Messstellenliste

## 11. Beispiel Topologie Leitsystem

### Typisches Layout Leitsystem



## 12. Mitgeltende Regelungen

- 0001315 Werknorm elektrische Anlagen und elektrische Tätigkeiten
- 0000709 Informationssicherheitsrichtlinie VR7.05.01
- 0002478 Werknorm Anbindung von Anlagen in das übergeordnete Kraftwerksnetz
- VGB-Standard VGB-S-170
- OT/IT-Security Lastenheft

## 13. Anhänge

- Keine