(19) Deutsches Patent- und Markenamt

(10) **DE 10 2022 114 543 A1** 2022.12.22

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2022 114 543.3**
(22) Anmeldetag: **09.06.2022**
(43) Offenlegungstag: **22.12.2022**

(51) Int Cl.: ***G05B 19/418*** (2006.01)

(30) Unionspriorität:

63/211,535	**16.06.2021**	**US**
17/502,926	**15.10.2021**	**US**

(71) Anmelder:
FISHER-ROSEMOUNT SYSTEMS, INC., Round Rock, TX, US

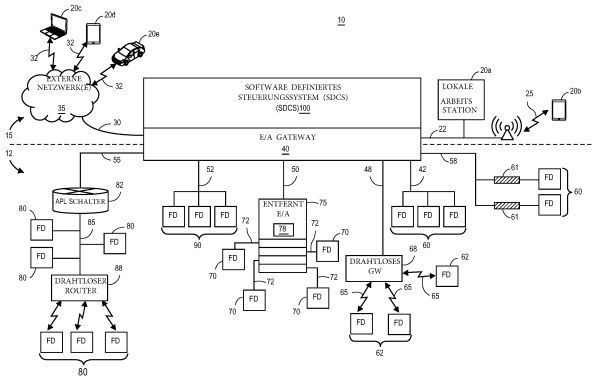
(74) Vertreter:
Meissner Bolte Patentanwälte Rechtsanwälte Partnerschaft mbB, 80538 München, DE

(72) Erfinder:
Amaro, Anthony jr., Cedar Park, TX, US; Nixon, Mark J., Thorndale, TX, US

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **SYSTEME UND VERFAHREN ZUR ZUORDNUNG VON MODULEN IN EINEM SOFTWAREDEFINIERTEN STEUERUNGSSYSTEM FÜR INDUSTRIELLE PROZESSANLAGEN**

(57) Zusammenfassung: Ein Prozesssteuerungssystem beinhaltet eine Vielzahl von Feldgeräten, die zur Steuerung eines Prozesses in einer Prozessanlage arbeiten. Eine Kommunikationsinfrastruktur koppelt die Vielzahl von Feldgeräten an ein Software-definiertes Steuerungssystem (SDCS), das Daten von den Feldgeräten empfängt und Anweisungen an die Feldgeräte sendet. Ein Datencluster, der das SDCS ausführt, beinhaltet eine Vielzahl von Rechenknoten, von denen jeder einen Prozessor, der ein Betriebssystem ausführt, einen Speicher und eine Kommunikationsressource beinhaltet, die mit einem oder mehreren anderen Rechenknoten im Datencluster verbunden ist. Eine Vielzahl von instanziierten Containern, von denen jeder eine isolierte Ausführungsumgebung innerhalb des Betriebssystems des Rechenknotens darstellt, auf dem der Container instanziiert ist, arbeiten zusammen, um die Ausführung einer Steuerstrategie im SDCS zu erleichtern. Mindestens einer der Container im SDCS ist an eine Komponente im SDCS angeheftet.



Beschreibung

TECHNISCHES GEBIET

[0001] Die vorliegende Anmeldung bezieht sich allgemein auf industrielle Prozesssteuerungssysteme von industriellen Prozessanlagen und insbesondere auf industrielle Prozesssteuerungssysteme, die Software-definiert sind.

STAND DER TECHNIK

[0002] Derzeitig verkaufte industrielle Prozesssteuerungssysteme, wie sie in Chemie-, Erdöl-, Industrie- oder anderen Prozessanlagen zur Herstellung, Veredelung, Umwandlung, Erzeugung oder Produktion von physischen Materialien oder Produkten verwendet werden, beinhalten typischerweise eine oder mehrere Prozesssteuerungen, die über physische Schichten, die analog, digital oder kombiniert analog/digital sein können, mit einem oder mehreren Feldgeräten kommunikativ gekoppelt sind oder eine oder mehrere drahtlose Kommunikationsverbindungen oder Netzwerke beinhalten können. Die Feldgeräte, bei denen es sich beispielsweise um Ventile, Stellungsregler, Schalter und Transmitter (z.B. Temperatur-, Druck-, Füllstands- und Durchflusssensoren) handeln kann, befinden sich in der Prozessumgebung der industriellen Prozessanlage (die hier austauschbar als „Feldumgebung“ oder „Anlagenumgebung“ der industriellen Prozessanlage bezeichnet wird) und führen im Allgemeinen physische Prozesssteuerungsfunktionen aus, wie z.B. das Öffnen oder Schließen von Ventilen, das Messen von Prozess- und/oder Umgebungsparametern wie Durchfluss, Temperatur oder Druck usw., um einen oder mehrere Prozesse zu steuern, die innerhalb der Prozessanlage oder des Systems ablaufen. Intelligente Feldgeräte, wie z.B. Feldgeräte, die dem bekannten FOUNDATION® Fieldbus Protokoll entsprechen, können auch Steuerungsberechnungen, Alarmfunktionen und andere Steuerungsfunktionen ausführen, die üblicherweise in der Steuerung implementiert sind. Die Prozesssteuerungen, die sich ebenfalls typischerweise in der Assetumgebung befinden, aber auch in einer mit der Anlage verbundenen geschützten Backend-Umgebung liegen können, empfangen Signale, die auf von den Feldgeräten durchgeführte Prozessmessungen und/oder andere die Feldgeräte betreffende Informationen hinweisen, und führen eine Steuerungsroutine oder Anwendung aus, die z.B. verschiedene Steuerungsmodule betreibt, die verschiedene Steuerungsalgorithmen verwenden, eine Steuerungsentscheidung treffen, Prozesssteuersignale auf der Grundlage der empfangenen Informationen erzeugen und mit den Steuerungsmodulen oder Blöcken, die in den Feldgeräten ausgeführt werden, koordinieren, wie z.B. HART®, WirelessHART® und FOUNDATION® Fieldbus Feldgeräte.

[0003] Andere Arten von Feldgeräten können z.B. spektrometrische Geräte sein, die für die Qualitätskontrolle und die Verifizierung der Reinheit verwendet werden können, z.B. in speziellen chemischen und pharmazeutischen Prozessanlagen. Beispiele für spektrometrische Feldgeräte sind NIR- (Nahinfrarot), UV-VIS- (ultraviolett-sichtbar) und Raman-Spektrometer, um nur einige zu nennen. Spektrometrische Feldgeräte können von Steuerungen oder Gerätemanagern gesteuert oder verwaltet werden, die den spektrometrischen Geräten typischerweise mitteilen, wann sie Daten sammeln sollen, wann sie die gesammelten Daten übertragen sollen, usw.

[0004] E/A-Geräte, die zwischen den Feldgeräten und den Steuerungen angeordnet sind, ermöglichen die Kommunikation zwischen ihnen. Beispielsweise senden Steuerungsmodule in einer Prozesssteuerung die Steuersignale an eine Vielzahl von verschiedenen Eingabe-/Ausgabegeräten (E/A-Geräte), die diese Steuersignale dann über spezielle Kommunikationsleitungen oder -verbindungen (physische Kommunikationsschichten) an die eigentlichen Feldgeräte senden, um dadurch den Betrieb mindestens eines Bereichs der Prozessanlage oder des Systems zu steuern, z.B. um mindestens einen Bereich eines oder mehrerer industrieller Prozesse (z.B. physische Prozesse) zu steuern, die innerhalb der Anlage oder des Systems laufen oder ausgeführt werden. In einem anderen Beispiel übermitteln spektrometrische Manager oder Steuerungen Anweisungen an verschiedene E/A-Geräte, die dann die Anweisungen über die speziellen Kommunikationsleitungen oder -verbindungen an physische spektrometrische Geräte in der industriellen Prozessanlage senden. Als Reaktion auf die Anweisungen übermitteln die spektrometrischen Geräte die gesammelten Daten über einen ähnlichen umgekehrten Weg über die E/A-Geräte an die Manager/Steuerungen und/oder an andere Empfängergeräte im Prozesssteuerungssystem. Die E/A-Geräte, die sich ebenfalls typischerweise in der Assetumgebung befinden, sind in der Regel zwischen einer Steuerung und einem oder mehreren Feldgeräten angeordnet und ermöglichen die Kommunikation dazwischen, z.B. durch Umwandlung elektrischer Signale in digitale Werte und umgekehrt. Verschiedene E/A-Geräte sind vorgesehen, um Feldgeräte zu unterstützen, die verschiedene spezielle Kommunikationsprotokolle verwenden. Insbesondere ist zwischen einer Steuerung und jedem Feldgerät, das ein bestimmtes Kommunikationsprotokoll verwendet, ein anderes E/A-Gerät vorgesehen, so dass ein erstes E/A-Gerät zur Unterstützung von HART-Feldgeräten, ein zweites E/A-Gerät zur Unterstützung von Fieldbus-Feldgeräten, ein drittes E/A-Gerät zur Unterstützung von Profibus-Feldgeräten usw. verwendet wird. Feldgeräte, Steuerungen und E/A-Geräte werden im Allgemeinen als „Prozess-Steuerungseinrichtungen“ bezeichnet und befinden sich im Allgemeinen in

einer Feldumgebung eines Prozesssteuerungssystems oder einer Anlage, sind dort angeordnet oder installiert.

[0005] Darüber hinaus werden die Informationen aus den Feldgeräten und ihren jeweiligen Steuerungen über die Steuerungen über eine Datenautobahn oder ein Kommunikationsnetzwerk an ein oder mehrere andere Hardwaregeräte weitergegeben, wie z.B. Bediener-Workstations, Personalcomputer oder Computergeräte, Datenhistoriker, Berichtsgeneratoren, zentralisierte Datenbanken oder andere zentralisierte administrative Computergeräte, die sich typischerweise in Steuerungsräumen oder an anderen Orten befinden, die von der raueren und/oder gefährlichen Feldumgebung der Anlage entfernt sind, z.B. in einer Backend-Umgebung der Prozessanlage. Jedes dieser Hardware-Geräte ist typischerweise in der Prozessanlage oder in einem Bereich der Prozessanlage zentralisiert. Auf diesen Hardwaregeräten laufen Anwendungen, die es einem Bediener beispielsweise ermöglichen, Funktionen zur Steuerung eines Prozesses und/oder zum Betrieb der Prozessanlage auszuführen, wie z.B. das Ändern von Einstellungen der Prozesssteuerungsroutine, das Modifizieren des Betriebs der Steuerungsmodule innerhalb der Steuerungen oder der Feldgeräte, das Anzeigen des aktuellen Prozesszustands, das Anzeigen von Alarmen, die von Feldgeräten und Steuerungen erzeugt werden, das Simulieren des Prozessbetriebs zum Zwecke der Schulung von Personal oder des Testens von Prozesssteuerungssoftware, das Führen und Aktualisieren einer Konfigurationsdatenbank usw. Die von den Hardware-Geräten und Prozesssteuerungen genutzte Datenautobahn kann einen verdrahteten Kommunikationspfad, einen drahtlosen Kommunikationspfad oder eine Kombination aus verdrahteten und drahtlosen Kommunikationspfaden beinhalten und verwendet typischerweise ein paketbasiertes Kommunikationsprotokoll und ein nichtzeitsensitives Kommunikationsprotokoll, wie ein Ethernet- oder IP-Protokoll.

[0006] Das DeltaVTM Steuerungssystem, das von Emerson Prozess Management vertrieben wird, beinhaltet beispielsweise mehrere Anwendungen, die in verschiedenen Geräten gespeichert sind und von diesen ausgeführt werden, die sich an unterschiedlichen Orten innerhalb einer Prozessanlage befinden. Eine Konfigurationsanwendung, die sich auf einer oder mehreren Workstations oder Computergeräten befindet, ermöglicht es dem Nutzer, Prozesssteuerungsmodule zu erstellen oder zu ändern und diese Prozesssteuerungsmodule über eine Datenautobahn auf dedizierte verteilte Steuerungen herunterzuladen. Typischerweise bestehen diese Steuerungsmodule aus kommunikativ miteinander verbundenen Funktionsblöcken, bei denen es sich um Objekte in einem objektorientierten Programmierprotokoll handeln kann, die Funktionen innerhalb des Steuerschemas auf der Grundlage von Eingaben ausführen und Ausgänge an andere Funktionsblöcke innerhalb des Steuerschemas liefern. Die Konfigurationsanwendung kann es einem Konfigurationstechniker auch ermöglichen, Bedienerschnittstellen zu erstellen oder zu ändern, die von einer Anzeigeanwendung verwendet werden, um Daten für einen Bediener anzuzeigen und es dem Bediener zu ermöglichen, Einstellungen, wie z.B. Sollwerte, innerhalb der Prozesssteuerungsroutinen zu ändern. Jede dedizierte Steuerung und in einigen Fällen ein oder mehrere Feldgeräte speichern und führen eine entsprechende Steuerungsanwendung aus, die das ihr zugewiesene und heruntergeladene Steuerungsmodul ausführt, um die tatsächliche Prozesssteuerungsfunktionalität zu implementieren. Die Anzeigeanwendungen, die auf einem oder mehreren Bedienerarbeitsplätzen (oder auf einem oder mehreren entfernten Computergeräten, die in kommunikativer Verbindung mit den Bedienerarbeitsplätzen und der Datenautobahn stehen) ausgeführt werden können, empfangen Daten von der Steuerungsanwendung über die Datenautobahn und zeigen diese Daten Prozesssteuerungssystemdesignern, Bedienern oder Nutzern über die Nutzerschnittstellen an und können eine beliebige Anzahl verschiedener Ansichten bereitstellen, z. B. die Ansicht eines Bedieners, eines Ingenieurs, eines Technikers usw. Eine Datenhistoriker-Anwendung wird typischerweise in einem Datenhistoriker-Gerät gespeichert und von diesem ausgeführt, das einige oder alle über die Datenautobahn bereitgestellten Daten sammelt und speichert, während eine Konfigurationsdatenbasis-Anwendung in einem weiteren, an die Datenautobahn angeschlossenen Computer laufen kann, um die aktuelle Prozess-Steuerungsroutine Konfiguration und damit verbundene Daten zu speichern. Alternativ kann sich die Konfigurationsdatenbasis auch auf demselben Arbeitsplatz wie die Konfigurationsanwendung befinden.

[0007] Da sich verteilte industrielle Prozesssteuerungssysteme im Laufe der Zeit weiterentwickelt haben, wurden verschiedene Hardware-, Kommunikations- und Netzwerktechnologien entwickelt und hinzugefügt. Folglich beinhalten die heutigen Prozesssteuerungssysteme typischerweise eine Vielzahl unflexibler und hardwarezentrierter Geräte, wie z.B. dedizierte Bedienerkonsolen, Konfigurationsstationen, speziell angefertigte Steuerungen und E/A-Karten, um nur einige zu nennen. Diese Vielzahl verschiedener Arten von Hardware-Geräten innerhalb eines Prozesssteuerungssystems erfordert mehrere Ebenen der Konfiguration und der Beschreibung des zugrundeliegenden Systems für den Nutzer, was in der Regel zu höheren Kosten für die anfängliche Entwicklung und für das Änderungsmanagement führt. Darüber hinaus sind Prozessanlageninstallationen und -erweiterungen aufgrund ihrer Abhängigkeit von

speziell angefertigter Hardware leicht von Kostenüberschreitungen und Verzögerungen in der Lieferkette betroffen.

[0008] Der Sektor Informationstechnologie (IT) leidet unter ähnlichen Problemen, wenn auch in einem allgemeineren Sinne. Im IT-Sektor geht der Trend in letzter Zeit dahin, die Schichten der Infrastruktur, einschließlich der physischen Hardwareanforderungen, von der nutzerabhängigen Geschäftslogik zu abstrahieren, um eine flexible Hardwareinstallation zu ermöglichen. In der Regel entwerfen, diktieren oder legen IT-Administratoren in IT-Systemen die Hardwareanforderungen fest, die für die Implementierung der vom Nutzer gewünschten Geschäftslogik erforderlich sind, und passen die Hardware-Plattformkonfigurationen und -nutzungen an, wenn sich die Anforderungen der Geschäftslogik ändern.

ZUSAMMENFASSUNG

[0009] Ein industrielles, Software-definiertes Prozesssteuerungssystem (SDCS) bietet eine neuartige Architektur für ein Prozesssteuerungssystem einer industriellen Prozessanlage, die Software und Hardware des Prozesssteuerungssystems weitgehend entkoppelt. Im Allgemeinen wird die Geschäftslogik der Prozesssteuerungssystem-Automatisierung als logische Abstraktionen auf Software- und Hardware-Computer-Ressourcen implementiert. Die Verwaltung dieser Ressourcen für die industrielle Prozesssteuerung kann in einer hyperkonvergenten Computersystem-Infrastrukturumgebung implementiert werden, in der die Software-definierten (SD) Komponenten oder Elemente durch das Software-definierte Prozesssteuerungssystem verwaltet und verteilt werden, wobei einige oder alle der hier beschriebenen Techniken verwendet werden. Vorteilhafterweise verwaltet das Software-definierte Prozesssteuerungssystem dynamisch und automatisch Software- und Hardwareressourcen, um dynamische Anforderungen der Geschäftslogik des Prozesssteuerungssystems im Hinblick auf dynamisch auftretende Bedingungen des Prozesssteuerungssystems und der industriellen Prozessanlage (z.B. reaktiv und/oder vorausschauend) während der Laufzeit des Software-definierten Prozesssteuerungssystems zu unterstützen.

[0010] Das Software-definierte Prozesssteuerungssystem (SDCS) kann eine Software-definierte Netzwerkschicht, eine Software-definierte Anwendungsschicht und eine Software-definierte Speicherschicht beinhalten, die von einer physischen Schicht unterstützt werden. Die physische Schicht kann im SDCS beinhalten sein oder auch nicht. Im Allgemeinen beinhaltet die physische Schicht Hardware-Schnittstellen (z.B. eine oder mehrere Netzwerkschnittstellen oder Ports), über die das SDCS kommunikativ mit der Feldumgebung der industriellen Prozessanlage und den darin befindlichen physischen Geräten oder physischen Komponenten verbunden ist. Die Hardware-Schnittstellen können zum Beispiel Ein-/Ausgabe-Schnittstellen (E/A) beinhalten. Die physische Schicht kann auch Routing-Komponenten beinhalten, die über Software und/oder Hardware implementiert werden können, um Daten zu und von bestimmten Schnittstellenports zu leiten. In einigen Ausführungsformen beinhaltet das SDCS die physische Schicht, und in einigen Ausführungsformen schließt das SDCS die physische Schicht aus und ist kommunikativ mit einer anderen Gruppe von Rechengeräten oder einer Rechenplattform verbunden, die die physische Schicht bereitstellt.

[0011] Die Software-definierte Netzwerkschicht des SDCS beinhaltet eine Rechenplattform mit einem oder mehreren Datenverarbeitungsclustern, die zumindest teilweise, wenn nicht sogar vollständig, über das Internet vernetzt sind. Jeder Cluster kann einen oder mehrere Knoten beinhalten, die zumindest teilweise über entsprechende Netzwerkressourcen miteinander vernetzt sind, und jeder Knoten beinhaltet einen entsprechenden Satz von Prozessor- und/oder Prozessor-Kernressourcen und Speicherressourcen. Ein Knoten kann zum Beispiel auf einem Computer oder einem Server implementiert sein. Ein Computer oder Server kann mehrere Prozessoren beinhalten, und ein Prozessor kann mehrere Kerne beinhalten.

[0012] In der SD-Netzwerkschicht überwacht und verwaltet ein Software-definiertes Betriebssystem die Erstellung von Komponenten der Software-definierten Anwendungsschicht und die Nutzung oder Auslastung (sowohl einzeln als auch gemeinsam) der verfügbaren (und sich möglicherweise dynamisch ändernden Hardware- und Software-Ressourcen) der Rechenplattform Knoten während des Starts und der Laufzeit des SDCS. Zum Beispiel weist das SD-Betriebssystem Komponenten der Anwendungsschicht an, auf bestimmten Knoten der Rechenplattform ausgeführt zu werden und/oder bestimmte Prozessor-Ressourcen, Rechenkern-Ressourcen und/oder Speicher-Ressourcen der Knoten der Rechenplattform zu nutzen. Im Allgemeinen stellt das SD-Betriebssystem der SD-Netzwerkschicht Unterstützungsdienste bereit, von denen einige von SD-Anwendungsschicht-Komponenten in Anspruch genommen werden, die die SD-Anwendungsschicht-Komponenten gemäß der Geschäftslogik des Prozesssteuerungssystems, dem Zeitplan und den Leistungsanforderungen in Abstimmung mit der Überwachung und Verwaltung der Hardware- und Software-Ressourcen des Knotens zur Unterstützung der Software-definierten Anwendungsschicht-Komponenten verschiedenen Knoten zuweisen, zuordnen, neu anordnen, neu zuordnen, einen Lastausgleich vornehmen usw. Darüber hinaus kop-

pelt und verwaltet die Software-definierte Netzwerkschicht kommunikativ die Vernetzung oder Lieferung von Daten zwischen Software-definierten Anwendungsschicht-Komponenten und ihren jeweiligen Endpunkten, bei denen es sich um andere Software-definierte Anwendungsschicht-Komponenten, Geräte in der Prozessanlagen Feldumgebung, Geräte der Nutzer Schnittstelle, externe Systeme usw. handeln kann.

[0013] Die Software-definierte Anwendungsschicht beinhaltet die Geschäftslogik des Prozesssteuerungssystems, die typischerweise über Container, virtuelle Maschinen oder andere geeignete gekapselte Ausführungsumgebungen implementiert wird. Beispielsweise kann die Geschäftslogik des Prozesssteuerungssystems als eine Reihe von Anwendungsschichtdiensten implementiert werden, wobei die Anwendungsschichtdienste jeweils für bestimmte Sätze von Geschäftslogik konfiguriert werden können und jede Instanz eines konfigurierten Dienstes in einer eigenen gekapselten Ausführungsumgebung ausgeführt werden kann. SDCS Anwendungsschichtdienste können z.B. Prozesssteuerungs-Steuerungen, Nutzer-Schnittstellen, Diagnostik, Analytik, E/A Networking und Historiker beinhalten, um nur einige zu nennen. SD Anwendungsschichtdienste können mit Steuerungsroutinen, Tags, Gerätekennungen, Gerätesignalkennungen, Parametern, Werten usw. konfiguriert werden, um konfigurierte Instanzen von Diensten zu bilden, die jeweils in einer entsprechenden gekapselten Ausführungsumgebung (z.B. konfigurierte Container, virtuelle Maschinen usw.) ausgeführt werden können. Die konfigurierten gekapselten Ausführungsumgebungen werden von der SD Netzwerkschicht zugeordnet oder zugewiesen (und in einigen Fällen neu zugewiesen oder neu wiederzugewiesen, basierend auf dynamisch auftretenden Bedingungen innerhalb der industriellen Prozessanlage), um auf entsprechenden Software- und/oder Hardware-Ressourcen des Knotens der Rechenplattform ausgeführt zu werden.

[0014] Die Software-definierte Speicherschicht beinhaltet Prozesssteuerungssystem-Datenspeicher, die von der Software-definierten Anwendungsschicht genutzt werden können. Ähnlich wie die Software-definierte Anwendungsschicht stellt die Software-definierte Speicherschicht logische Speichereinheiten oder -orte zur Verwendung durch die Anwendungen der SD-Anwendungsschicht bereit, und die logischen Speichereinheiten werden von der SD-Netzwerkschicht verschiedenen Ressourcen des Knotens der Rechenplattform zugewiesen und/oder zugeordnet (und in einigen Fällen neu zugewiesen und/oder neu zugeordnet). Darüber hinaus kann die SD-Netzwerkschicht, falls gewünscht, für Redundanz verschiedener logischer Speichereinheiten sorgen.

[0015] Ein Verfahren und System zur Steuerung einer industriellen Prozesssteuerungsanlage verwendet die SDCS Anwendungsschichtdienste, um die Prozesssteuerung unter Verwendung von Software-definierten Steuerungen, Software-definierten Eingabe-/Ausgabe-Ressourcen, Software-definiertem Speicher und/oder Software-definiertem Netzwerk zu erleichtern. Die SDCS Anwendungsschicht beinhaltet einen oder mehrere Container, die einen oder mehrere Dienste ausführen. Ein Orchestrator arbeitet als Teil einer hyperkonvergenten Infrastruktur, um die Instanziierung des einen oder der mehreren Container zu steuern und den Lastausgleich und die Fehlertoleranz durch Duplizierung und/oder Verschiebung (z.B. Re-Instanziierung) von Containern zwischen verschiedenen Hardware-Ressourcen zu erleichtern. So können beispielsweise einzelne Container, die entsprechende Dienste ausführen, zwischen Hardware-Ressourcen verschoben werden, wenn die Hardware-Ressourcen (z.B. Prozessoren, Prozessor-Kerne, Speichergeräte, Netzwerkkapazitäten) ausgelastet sind, um sicherzustellen, dass alle Dienste nominell/bestimmungsgemäß arbeiten. Als weiteres Beispiel können mehrere Kopien eines bestimmten Containers (d.h. mehrere Kopien eines Dienstes, der einen bestimmten Bereich der Prozessanlage bedient) auf verschiedenen Hardware-Ressourcen instanziiert werden, um sicherzustellen, dass die Steuerung auf eine andere Kopie des Containers übergehen kann, wenn eine einzelne Kopie des Containers instabil oder nicht verfügbar wird oder eine Hardware-Ressource ausfällt. Zu den auf diese Weise implementierten und vom Orchestrator kontrollierten Diensten können E/A-Serverdienste, Steuerungsdienste, Historiker, Subsysteme (z.B. Batch-Steuerung, kontinuierliche Steuerung, Ereignissteuerung, Alarm-Subsysteme, Diagnose-Subsysteme usw.), Netzwerkdienste (z.B. Software-Firewalls) und jeder andere containerisierte Dienst im SDCS gehören. Die Hardware-Ressourcen, über die Hardware-Diversität zwischen identischen Containern implementiert werden kann, beinhalten Datencluster, Energieversorgungen, Serverknoten, Prozessoren, Prozessorkerne, Speichergeräte usw., und können das dynamische Hinzufügen oder Entfernen von Hardware-Ressourcen je nach Bedarf oder Anforderung ermöglichen.

[0016] Ein weiterer Aspekt des hier beschriebenen Systems beinhaltet verschachtelte Rechencontainer, die innerhalb des SDCS arbeiten. Während jeder der auf einem Rechenknoten instanziierten Container eine isolierte Ausführungsumgebung darstellt, die innerhalb des Betriebssystems des Rechenknotens ausgeführt wird, kann ein bestimmter Container innerhalb eines anderen Containers instanziiert werden und/oder einen oder mehrere Container beinhalten. So ist es z.B. möglich, physische oder logische Hierarchien innerhalb der Prozessanlage zu replizieren und damit die physischen und logischen Anord-

nungen von Elementen innerhalb der Prozessanlage in der SDCS zu duplizieren. Zum Beispiel, Assetsbereiche, Einheiten innerhalb von Bereichen und Prozessmodule innerhalb von Einheiten können in verschachtelten Containern des SDCS repliziert werden.

[0017] Darüber hinaus können in dem hier beschriebenen SDCS Container an andere Elemente der Prozesssteuerungsumgebung angeheftet werden. Durch das Anheften eines Containers an ein anderes Element des Prozesssteuerungssystems oder der Anlage kann ein Konfigurationstechniker oder Betreiber sicherstellen, dass bestimmte Parameter eingehalten werden, auch wenn der Orchestrator eine gewisse Autonomie genießt. Beispielsweise können Container an Rechenressourcen, an Speicherressourcen, an Netzwerkressourcen, an Energieversorgungsressourcen usw. angeheftet werden, um sicherzustellen, dass bestimmte Aspekte der Fehlertoleranz beibehalten werden, auch wenn Container zum Zwecke des Lastausgleichs „verschoben“ werden (z.B. kann ein Container auf Rechenressourcen verbleiben, die an eine bestimmte Energieversorgung gekoppelt sind, auch wenn der Container zwischen Rechenressourcen verschoben werden kann, die an die Energieversorgung gekoppelt sind). Container können auch mit anderen Containern oder Gruppen von Containern verbunden sein (so dass sie zusammen verschoben/instanziiert werden), unabhängig davon, ob sie verschachtelt sind oder nicht, oder sie können mit der Hardware in der Prozesssteuerungsanlage selbst verbunden sein (z.B. so dass ein bestimmter Steuerungscontainer mit einer bestimmten Einheit der Prozesssteuerungshardware verbunden ist).

[0018] In einem Betriebsbeispiel kann ein E/A-Serverdienst der SDCS Schnittstellen mit mehreren containerisierten Steuerungsdiensten haben, die jeweils die gleiche Steuerungsroutine implementieren, um den gleichen Bereich der gleichen Anlage zu steuern. Der E/A-Serverdienst kann jedem der containerisierten Steuerungsdienste dieselben Steuerungseingängen zur Verfügung stellen (z.B. die Steuerungsausgänge, die Messungen darstellen, die von Feldgeräten gewonnen und von den Feldgeräten an den E/A-Serverdienst übermittelt wurden). Jeder containerisierte Steuerungsdienst führt dieselbe Steuerungsroutine aus, um einen Satz von Steuerungsausgängen zu erzeugen. Der E/A-Serverdienst empfängt jeden Satz von Steuerungsausgängen und leitet einen „aktiven“ Satz von Steuerungsausgängen an die entsprechenden Feldgeräte weiter. Die Ausgabesätze der anderen Steuerungsdienste müssen nicht an die Feldgeräte übermittelt werden. Der E/A-Serverdienst und andere Dienste im System, wie z.B. ein Orchestratordienst, können die Leistung und die Ressourcennutzung im Steuerungssystem kontinuierlich auswerten und die Steuerungsdienste gegebenenfalls dynamisch aktivieren und deaktivieren, um die Leistung zu optimieren. Falls gewünscht, kann der E/A-Serverdienst containerisiert werden. Außerdem kann es mehr als eine Instanz desselben containerisierten E/A-Serverdienstes geben. In einer solchen Implementierung kann eine einzelne dieser Instanzen als „aktiv“ betrachtet werden und als voll funktionsfähiger Vermittler für den E/A-Verkehr zwischen Feldgeräten und containerisierten Steuerungsdiensten fungieren. Die „inaktiven“ E/A-Serverdienste können denselben E/A-Verkehr empfangen, den der „aktive“ E/A-Serverdienst empfängt, und können dieselbe Logik für den E/A-Verkehr implementieren. Falls gewünscht, leiten die „inaktiven“ E/A-Serverdienste den E/A-Verkehr jedoch nicht weiter; oder wenn sie es doch tun, wird er vom Zieldienst oder -gerät nicht empfangen und bearbeitet (z.B. kann ein Netzwerkschalter den Verkehr empfangen und feststellen, dass es sich um „inaktiven“ E/A-Verkehr handelt, und ihn daher möglicherweise nicht an sein Ziel weiterleiten).

[0019] Containerisierte Steuerungsdienste und containerisierte E/A-Serverdienste können auf physische Ressourcen in einer Anlage oder anderswo in beliebiger Weise verteilt werden. Falls gewünscht, sind ein oder mehrere der implementierten Container nicht dauerhaft an einen bestimmten Computer-Cluster oder Knoten/Server gebunden, auf dem sie gerade ausgeführt werden. Die Container können dynamisch (z.B. in oder nahezu in Echtzeit, während der Ausführung) instanziiert, gelöscht und auf verschiedenen Computern neu instanziiert werden, wenn dies gewünscht wird, um Rechen- und Netzwerklasten auszugleichen und Ineffizienzen bei der Berechnung oder im Netzwerk zu verringern (z.B. wenn eine bestimmte physische Ressource Computerisch oder durch Netzwerkverkehr übermäßig belastet wird). Darüber hinaus kann die Gesamtzahl der Instanzen eines bestimmten Containers je nach Bedarf dynamisch reduziert oder erhöht werden, und jede dieser Instanzen (die z.B. alle den gleichen Steuerungsdienst implementieren) kann je nach Bedarf aktiviert oder deaktiviert werden. Dieses „Jonglieren“ zwischen Containern kann hilfreich sein, wenn die Rechen- und Netzwerkauslastung der physischen Ressourcen stark variiert. Jeder Steuerungsdienst kann in einem eigenen Container untergebracht werden, wodurch eine relativ isolierte, konsistente und vorhersehbare Umgebung geschaffen wird, in der jeder Steuerungsdienst implementiert wird, unabhängig von der breiteren Softwareumgebung auf dem Knoten, der die Container implementiert. Ein Container kann zum Beispiel Software-Abhängigkeiten und Software-Bibliotheken beinhalten, die für einen bestimmten Steuerungsdienst benötigt werden. Ohne Container wäre es möglicherweise erforderlich, jeden einzelnen Knoten, auf dem der Steuerungsdienst ausgeführt wird, ordnungsgemäß zu konfigurieren, um eine konsistente Umge-

bung für den Steuerungsdienst zu gewährleisten. Und wenn ein bestimmter Knoten in der Lage sein muss, verschiedene Arten von Diensten zu implementieren (die jeweils unterschiedliche Umgebungsanforderungen haben können), kann die Gewährleistung einer ordnungsgemäßen Konfiguration des Knotens komplex werden. Im Gegensatz dazu ermöglichen der beschriebene Steuerungsdienstcontainer, dass jeder Steuerungsdienst in jedem beliebigen Knoten einfach instanziiert und zwischen Knoten/Servern oder Rechenclustern (z.B. durch den E/A-Serverdienst) leicht verschoben werden kann.

[0020] Ein weiterer Aspekt des hier beschriebenen Systems beinhaltet Sicherheitsdienste innerhalb des SDCS. In der SD Netzwerkschicht kann ein SD Netzwerkdienst das logische oder virtuelle Netzwerk, das vom logischen Prozesssteuerungssystem verwendet wird, verwalten und managen. Der SD-Netzwerkdienst kann Instanzen von Netzwerk-Geräten, wie z.B. virtuelle Router, virtuelle Firewalls, virtuelle Switches, virtuelle Schnittstellen, virtuelle Datendioden, usw., und Instanzen von Netzwerkdiensten, wie z.B. Paketprüfdienste, Zugriffssteuerungsdienste, Autorisierungsdienste, Autentifizierungsdienste, Verschlüsselungsdienste, Zertifizierungsautoritätsdienste, Schlüsselverwaltungsdienste, usw., im SDCS einrichten und verwalten.

[0021] Zum Beispiel kann der SD-Netzwerkdienst einen Dienst für rollenbasierte Autorisierung innerhalb des SDCS bereitstellen. Wenn ein Nutzer eine Autorisierung für den Zugriff auf einen Dienst (z.B. ein Steuerungsdienst) innerhalb des SDCS anfordert, kann der Autorisierungsdienst auf der Grundlage der Anforderung eine Autorisierungsstufe des Nutzers bestimmen und feststellen, ob der Nutzer berechtigt ist, auf den anderen Dienst zuzugreifen. Genauer gesagt kann der Autorisierungsdienst eine Mindestautorisierungsstufe für den Zugriff auf den Steuerungsdienst bestimmen und feststellen, ob die Autorisierungsstufe des Nutzers die Mindestautorisierungsstufe erreicht oder überschreitet. Wenn der Nutzer nicht autorisiert ist, kann der Autorisierungsdienst den Zugriff auf den Steuerungsdienst verhindern.

[0022] Der SD-Netzwerkdienst kann auch einen Zertifizierungsautoritätsdienst einrichten. Der Zertifizierungsautoritätsdienst kann digitale Zertifikate für physische oder logische Assets zur Authentifizierung der physischen oder logischen Assets generieren. Die Zertifikate können anzeigen, dass der Zertifizierungsautoritätsdienst die Identität des physischen oder logischen Assets verifiziert hat, so dass die Identität nicht jedes Mal verifiziert werden muss, wenn der physische oder logische Asset mit Diensten oder Knoten des SDCS kommuniziert.

[0023] Das SDCS kann auch einen Suchdienst beinhalten, der über einen Container auf einem Rechenknoten des SDCS ausgeführt wird. Wenn ein physisches oder logisches Asset einem Netzwerk in der Prozessanlage beitritt, meldet das physische oder logische Asset seine Anwesenheit. Der Suchdienst erzeugt und speichert dann eine Aufzeichnung der Identität, der Fähigkeiten und/oder des Standorts jedes physischen oder logischen Assets in der Prozessanlage, die während der Laufzeit der Prozessanlage genutzt werden kann, um zumindest einen Bereich des industriellen Prozesses zu steuern. Auf diese Weise kann der Suchdienst bei der Inbetriebnahme von physischen Assets innerhalb der Prozessanlage, wie z.B. Feldgeräten, sowie bei der Inbetriebnahme von logischen Assets, wie z.B. Containern, Diensten und Microdienste, helfen. Physische oder logische Assets im SDCS können automatisch nach ihrer Entdeckung ohne manuelle Eingabe in Betrieb genommen werden.

[0024] Der Suchdienst kann auch eine Fehlerbehebung durchführen, wenn die Aufzeichnung der physischen oder logischen Assets in der Prozessanlage beschädigt oder zerstört ist, indem er eine Anfrage an alle physischen oder logischen Assets im Netzwerk sendet, um ihre Anwesenheit zu melden. Auf diese Weise kann der Datensatz der physischen oder logischen Assets automatisch wiederhergestellt werden, ohne dass die Informationen über die einzelnen physischen oder logischen Assets in der Prozessanlage manuell eingegeben werden müssen.

[0025] Im Gegensatz zu aktuellen Prozesssteuerungs-Datenaustauschstandards wie OPC, bei denen das System höchstens die Fähigkeiten identifiziert, die von einem physischen oder logischen Asset bekannt gegeben werden (hier auch als „primäre Variablen“ bezeichnet), ist der hier beschriebene Suchdienst so konfiguriert, dass er automatisch zusätzliche Fähigkeiten des physischen oder logischen Assets ableitet, die dem Suchdienst nicht bekannt gegeben werden, wenn das physische oder logische Asset ermittelt wird (hier auch als „kontextuelle Variablen“ bezeichnet). Zu den zusätzlichen Fähigkeiten können zusätzliche Parameter oder Dienste gehören, die von dem physischen oder logischen Asset bereitgestellt werden, oder Dienste, die für die Kommunikation mit dem physischen oder logischen Asset konfiguriert sind. Der Suchdienst kann dann einem anderen Knoten oder Dienst im SDCS, der Informationen über das physische oder logische Asset anfordert, einen Hinweis auf die Fähigkeiten des physischen oder logischen Assets geben. Auf diese Weise kann der Suchdienst einen vollständigeren Datensatz über die physischen oder logischen Assets in der Prozessanlage und ihre jeweiligen Fähigkeiten speichern als frühere Prozesssteuerungssysteme. Dementsprechend können Knoten und Dienste im SDCS detaillierte Informationen

über die Fähigkeiten der physischen oder logischen Assets in der Prozessanlage vom Suchdienst erhalten, ohne die physischen oder logischen Assets direkt abfragen zu müssen, um zusätzliche Fähigkeiten zu identifizieren.

[0026] Um einen Nutzer bei der Visualisierung des Laufzeitbetriebs des SDCS zu unterstützen, kann ein Visualisierungsdienst Schnittstellen mit dem Orchestrator und einer Konfigurationsdatenbasis herstellen, um Konfigurationsdaten und aktuelle Laufzeitbetriebsdaten zu erhalten, die die momentan bestehenden oder in Betrieb befindlichen Beziehungen zwischen verschiedenen logischen Elementen des Steuerungssystems, wie Steuer- und Subsystemcontainern, sowohl untereinander als auch mit physischen Elementen im System definieren. Der Visualisierungsdienst kann eine beliebige Anzahl verschiedener Nutzer-Displays erstellen, die diese Beziehungen (wie sie momentan im SDCS konfiguriert sind und funktionieren) veranschaulichen und die auch wichtige Leistungs- oder „Gesundheitsparameter oder Zustandsparameter“ für eines oder mehrere der angezeigten logischen und/oder physischen Elemente liefern. So kann der Visualisierungsdienst beispielsweise eine Laufzeit-Betriebshierarchie erstellen, die in einer hierarchischen Ansicht zeigt, wie verschiedene logische Elemente, wie z.B. Steuerungscontainer und deren Untereinheiten, ineinander verschachtelt und aneinander angeheftet sind. Diese Hierarchie kann auch die Art und Weise veranschaulichen, in der verschiedene logische Elemente an verschiedene physische Elemente des Steuerungssystems angeheftet sind oder einfach in ihnen ausgeführt werden. Die Hierarchiedarstellung kann es einem Nutzer auch ermöglichen, verschiedene logische Elemente zu anderen logischen Elementen oder zu physischen Elementen innerhalb des Systems zu verschieben oder dynamisch neu zuzuordnen. Darüber hinaus kann der Visualisierungsdienst eine Anzeige erstellen und präsentieren, die die physische Hardware (z.B. Server, Knoten, Rechencluster, Prozessoren usw.) innerhalb des Steuerungssystems und die logischen Elemente (z.B. Steuerungscontainer, Container von Drittanbietern, Subsystemcontainer usw.) darstellt, die momentan auf diesen physischen Elementen ausgeführt werden. Die Anzeige kann auch Leistungs- oder Zustandsindizes beinhalten, die verschiedene Leistungs- und/oder Zustandsmessungen für die physischen und logischen Elemente innerhalb der Anzeige angeben. In anderen Fällen kann der Visualisierungsdienst eine Anzeige erstellen und präsentieren, die verschiedene logische Elemente und die Art und Weise, wie diese logischen Elemente ineinander verschachtelt oder aneinander angeheftet sind, sowie die physischen Elemente, die momentan zur Ausführung jedes der logischen Elemente während der aktuellen Laufzeit des Steuerungssystems verwendet werden, veranschaulicht. Diese Anzeigen können auch verschiedene Leistungskennzahlen für die verschiedenen logischen und physischen Elemente anzeigen, so dass ein Nutzer den aktuellen Betrieb und den Betriebszustand des Steuerungssystems oder verschiedener Bereiche desselben leicht erkennen oder visualisieren kann.

Figurenliste

Fig. 1 zeigt ein Blockdiagramm einer beispielhaften physischen industriellen Prozessanlage, die ein Software-definiertes Steuerungssystem (SDCS) beinhaltet;

Fig. 2 zeigt ein Blockdiagramm eines beispielhaften Software-definierten Steuerungssystems, das in die industrielle Prozessanlage von **Fig. 1** integriert werden kann;

Fig. 3 ist ein Blockdiagramm, das die Prinzipien der Fehlertoleranz und des Lastausgleichs illustriert;

Fig. 4A ist ein Blockdiagramm, das den Lastausgleich konzeptionell veranschaulicht;

Fig. 4B ist ein Blockdiagramm, das die Implementierung von Prioritätscontainern und des Lastausgleichs auf Containerebene veranschaulicht;

Fig. 5A ist ein Blockdiagramm, das die Implementierung von Fehlertoleranz auf Containerebene illustriert;

Fig. 5B ist ein Blockdiagramm, das eine Implementierung von Fehlertoleranz auf Serverebene veranschaulicht;

Fig. 6 ist eine Beispiel-Datenstruktur, die von einem Orchestrator verwaltet wird, um instanziierte Dienste und Container zu verfolgen;

Fig. 7 ist ein Blockdiagramm, das einen Software-definierten Speicherdienst darstellt;

Fig. 8 ist ein Blockdiagramm, das die logische und physische hierarchische Anordnung einer Prozessanlage zeigt;

Fig. 9 ist ein Blockdiagramm, das eine beispielhafte Implementierung von verschachtelten Containern in einem Prozesssteuerungssystem zeigt;

Fig. 10 ist ein Blockdiagramm, das die Verwendung von verschachtelten Containern für Fehlertoleranz und Lastausgleich illustriert;

Fig. 11 ist ein Blockdiagramm, das individuell instanziierte Container in einem verschachtelten hierarchischen System veranschaulicht;

Fig. 12 ist ein Blockdiagramm, das ein weiteres Beispiel für die Verschachtelung von Containern zeigt;

Fig. 13 ist ein Blockdiagramm, das ein erstes Beispiel für das Anheften von Containern in einem Prozesssteuerungssystem darstellt;

Fig. 14 ist ein Blockdiagramm, das ein zweites Beispiel für das Anheften von Containern in einem Prozesssteuerungssystem veranschaulicht;

Fig. 15 ist ein Blockdiagramm eines E/A-Netzwerks mit containerisierten Diensten zur Implementierung der Steuerung von Bereichen der in **Fig. 1** dargestellten Anlage;

Fig. 16 ist ein Blockdiagramm eines Computerclusters mit physischen Ressourcen (z.B. Computern, Servern, Netzwerkgeräten usw.), auf denen einer oder mehrere der verschiedenen hier beschriebenen Container, Mikrocontainer, Dienste und/oder Routinen implementiert, dynamisch zugewiesen und die Last ausgeglichen werden können, um die Nutzung und Leistung der Computerressourcen zu optimieren;

Fig. 17 zeigt eine beispielhafte Ausführungsform eines physischen Servers, auf dem containerisierte Dienste, wie die in **Fig. 15** und **Fig. 16** gezeigten, implementiert werden können;

Fig. 18 ist ein Flussdiagramm eines Verfahrens zur Implementierung eines E/A-Serverdienstes, wie einer der in **Fig. 15-17** gezeigten;

Fig. 19 ist ein Flussdiagramm eines Verfahrens zur Bewertung und zum Übergang zwischen containerisierten Steuerungsdienste, wie eine der in **Fig. 15-17** gezeigten;

Fig. 20 zeigt ein Blockdiagramm von Beispielcontainern, Diensten und/oder Subsystemen, die im SDCS von **Fig. 1** beinhaltet sind und sich auf die Netzwerksicherheit beziehen;

Fig. 21 zeigt ein weiteres Blockdiagramm von beispielhaften Containern, Diensten und/oder Subsystemen, die im SDCS von **Fig. 1** beinhaltet sind und sich auf die Netzwerksicherheit beziehen;

Fig. 22 zeigt ein Blockdiagramm eines Beispielcontainers, der zur Ausführung eines virtuellen Routers innerhalb des SDCS von **Fig. 1** konfiguriert ist;

Fig. 23 zeigt ein Blockdiagramm beispielhafter virtueller Firewalls, die jeweils mit einem entsprechenden Steuerungsdienst verbunden sind und einen Satz von Firewall-Regeln beinhalten, die für den zugehörigen Steuerungsdienst spezifisch sind;

Fig. 24 zeigt ein Blockdiagramm eines Beispielcontainers, der für die Ausführung einer virtuellen Steuerung konfiguriert ist und einen verschachtelten Container beinhaltet, der für die Ausführung eines Sicherheitsdienstes für die virtuelle Steuerung konfiguriert ist;

Fig. 25 zeigt ein weiteres Blockdiagramm eines Beispielcontainers, der zur Ausführung eines virtuellen Routers innerhalb des SDCS von **Fig. 1** konfiguriert ist, wobei der virtuelle Router verschachtelte Container beinhaltet, die zur Ausführung eines virtuellen Feld-Gateways, einer virtuellen Datendiode bzw. eines virtuellen Edge-Gateways konfiguriert sind;

Fig. 26 zeigt ein Blockdiagramm eines Beispielcontainers, der für die Ausführung eines Zertifizierungsautoritätsdienstes konfiguriert ist;

Fig. 27 zeigt ein Blockdiagramm von Beispielcontainern, Diensten und/oder Subsystemen, die im SDCS von **Fig. 1** beinhaltet sind und die für die Ausführung von Authentifizierungs- und Autorisierungsdiensten konfiguriert sind;

Fig. 28 zeigt ein Blockdiagramm eines Beispielcontainers, der für die Ausführung eines Speicherdienstes konfiguriert ist;

Fig. 29 zeigt ein Flussdiagramm, das ein Beispielverfahren zur Sicherung eines Prozesssteuerungssystems einer Prozessanlage darstellt;

Fig. 30 zeigt ein Flussdiagramm, das ein Beispiel für ein Verfahren zur rollenbasierten Autorisierung in einem Software-definierten Prozesssteuerungssystem (SDCS) darstellt;

Fig. 31 zeigt ein Flussdiagramm, das ein Beispielverfahren zur Erzeugung eines digitalen Zertifikats durch einen Zertifizierungsautoritätsdienst zur Authentifizierung eines physischen oder logischen Assets einer Prozessanlage darstellt;

Fig. 32 zeigt ein Flussdiagramm, das ein Beispielverfahren zur Authentifizierung eines physischen oder logischen Assets einer Prozessanlage darstellt;

Fig. 33 zeigt ein Blockdiagramm von beispielhaften Containern, Diensten und/oder Subsystemen, die im SDCS von **Fig. 1** beinhaltet sind und sich auf die Erkennung beziehen;

Fig. 34 zeigt ein Blockdiagramm eines Beispielcontainers, der zur Ausführung eines Suchdienstes konfiguriert ist;

Fig. 35 zeigt ein Blockdiagramm eines Beispiel-Containers, der für die Ausführung eines Kontext-Wörterbuchdienstes konfiguriert ist;

Fig. 36 zeigt ein Blockdiagramm eines Beispielkontextes, der in einen Kontext-Wörterbuch-Container aufgenommen werden kann;

Fig. 37 zeigt ein Flussdiagramm, das ein Beispielverfahren zur Bereitstellung von Discovery-Software als Dienst in einer Prozessanlage darstellt;

Fig. 38 zeigt ein Flussdiagramm, das ein Beispielverfahren zum Ableiten von Informationen über ein physisches oder logisches Asset einer Prozessanlage unter Verwendung eines Kontextwörterbuchs darstellt;

Fig. 39 zeigt ein Flussdiagramm, das ein Beispielverfahren für die Zuordnung eines Satzes von Fähigkeiten zu jedem Typ eines physischen oder logischen Assets in einer Prozessanlage und die Bestimmung der Fähigkeiten eines ermittelten physischen oder logischen Assets darstellt;

Fig. 40 zeigt ein Flussdiagramm, das ein Beispiel für ein Verfahren zur Fehlerbehebung bei erkannten Objekten in einer Prozessanlage darstellt;

Fig. 41 zeigt ein Flussdiagramm, das ein Beispiel für ein Verfahren zur automatischen Inbetriebnahme eines SDCS darstellt;

Fig. 42 zeigt ein Diagramm eines Visualisierungsdienstes oder Dienstprogramms, das mit einer Konfigurationsdatenbank und einem Orchestrator verbunden ist und dazu verwendet werden kann, einem Nutzer aktuelle logische und physische Konfigurations- und Laufzeitinformationen sowie verschiedene Leistungsindikatoren in Verbindung mit logischen und physischen Elementen des Systems zu liefern;

Fig. 43 zeigt eine erste Bildschirmanzeige, die von dem Visualisierungsdienst von **Fig. 42** dargestellt werden kann, um in einer hierarchischen Ansicht die Konfigurations- und Laufzeitinteraktionen von logischen und physischen Elementen in einem Steuerungssystem zu veranschaulichen;

Fig. 44 zeigt eine zweite Bildschirmanzeige, die vom Visualisierungsdienst von **Fig. 42** dargestellt werden kann, um die konfigurierten- und Laufzeit-Interaktionen logischer Elemente zu veranschaulichen, die momentan auf einem bestimmten Satz physischer Elemente im Steuerungssystem implementiert sind;

Fig. 45 zeigt eine dritte Bildschirmanzeige, die vom Visualisierungsdienst von **Fig. 42** dargestellt werden kann, um konfigurierte- und Laufzeit-Interaktionen von physischen Elementen zu veranschaulichen, die mit einem bestimmten oder ausgewählten Satz von logischen Elementen im Steuerungssystem verbunden sind, und

Fig. 46 zeigt eine vierte Bildschirmanzeige, die von dem Visualisierungsdienst von **Fig. 42** dargestellt werden kann, um konfigurierte- und Laufzeit-Interaktionen von logischen und physischen Elementen im Steuerungssystem zusätzlich zu verschiedenen Leistungsindikatoren für jedes Element zu veranschaulichen.

DETAILLIERTE BESCHREIBUNG

[0027] Fig. 1 zeigt ein Blockdiagramm einer beispielhaften physischen industriellen Prozessanlage 10 mit einem beispielhaften Software-definierten Steuerungssystem (SDCS) 100. Die Prozessanlage 10 beinhaltet eine Feldumgebung 12 (z.B. den Prozessanlagenboden), die mit einer Backend-Umgebung 15 kommunikativ verbunden ist. Die Backend-Umgebung 15 der Anlage 10 ist in der Regel von den rauen Bedingungen und Materialien der Feldumgebung 12 abgeschirmt und kann beispielsweise einen separaten Raum, ein Gebäude oder einen Ort auf dem Gelände in der Nähe der Feldumgebung 12, eine beliebige Anzahl von Geräten, die sich entfernt vom Standort der Anlage befinden, und/oder eine beliebige Anzahl von Anwendungen, die entfernt auf Geräten oder Systemen ausgeführt werden, die sich entfernt vom Standort der Anlage befinden, beinhalten. Die Backend-Umgebung 15 beinhaltet das SDCS 100 und typischerweise auch eine oder mehrere physische Arbeitsstationen und/oder Nutzer-Schnittstellen 20a-20e, die kommunikativ mit dem SDCS 100 verbunden sind. Eine oder mehrere Bediener- und/oder Konfigurations-Arbeitsstationen 20a können sich beispielsweise vor Ort in der Anlage 10 in einem abgeschirmten Raum befinden und über eine kabelgebundene Daten- oder Kommunikationsverbindung 22 (z.B. Ethernet oder eine andere geeignete kabelgebundene Verbindung) mit dem SDCS 100 verbunden sei und ein oder mehrere Bedienertablets 20b, die vom Personal vor Ort verwendet werden, können über eine drahtlose Verbindung 25 (z.B. Wi-Fi, WirelessHART, eine Mobilfunkverbindung wie 4G LTE, 5G oder 6G oder eine andere Art von geeigneter drahtloser Verbindung) und eine drahtgebundene Verbindung 22 mit dem SDCS 100 verbunden sein. Andere mit der Prozessanlage 10 verbundene Nutzer-Schnittstellen 20c-20e können außerhalb der Anlage 10 angeordnet sein und über letzte-Meile-Verbindungen 30 und/oder drahtlose Verbindungen 32 und/oder über ein oder mehrere private und/oder öffentliche Netzwerke 35 mit dem SDCS 100 kommunizieren. Beispielsweise können Laptops 20c, mobile Geräte 20d und/oder prozessanlagenbezogene Anwendungen, die in Laptops 20c, mobilen Geräten 20d und/oder Fahrzeugsystemen 20e ausgeführt werden, über entsprechende drahtlose Verbindungen 32, ein oder mehrere öffentliche und/oder private Daten- oder Kommunikationsnetze 35 und eine direkte oder letzte Meile-Verbindung 30 zum SDCS 100 (bei der es sich typischerweise, aber nicht notwendigerweise, um eine kabelgebundene Verbindung handelt) kommunikativ mit dem SDCS 100 verbunden sein. Die ferngesteuerten Nutzer-

Schnittstellen und Geräte 20c-20e können beispielsweise von Assetbedienern, Konfigurationsingenieuren und/oder anderem Personal genutzt werden, das mit der industriellen Prozessanlage 10 und ihren Komponenten in Verbindung steht.

[0028] Wie in **Fig. 1** dargestellt, ist das SDCS 100 über ein E/A (Eingang/Ausgang) Schnittstellensystem oder Gateway 40 mit den Komponenten der Feldumgebung 12 verbunden. Im Allgemeinen beinhaltet der feldseitige Bereich des E/A-Schnittstellensystems 40 eine Reihe von physischen Ports oder physischen Hardware-Schnittstellen, über die verschiedene Arten von E/A-Daten an/von in der Feldumgebung angeordneten Komponenten geliefert werden und die mit verschiedenen Arten von Prozessanlage-Kommunikationsverbindungen oder Datenverbindungen 42-58, über die die E/A-Daten geliefert werden, verbunden sind und/oder diese unterstützen. Das E/A-Schnittstellensystem 40 konvertiert und/oder leitet physische E/A, die über die Verbindungen 42-58 von Komponenten der Feldumgebung 12 empfangen werden, an Empfängerkomponenten des SDCS 100 (in **Fig. 1** nicht dargestellt) weiter, und umgekehrt konvertiert das E/A-Schnittstellensystem 40 die vom SDCS 100 erzeugte Kommunikation in entsprechende physische E/A und leitet die physische E/A an entsprechende Empfängerkomponenten, die innerhalb der Feldumgebung 12 angeordnet sind, z.B. über entsprechende Verbindungen 42-58. Als solches wird das E/A-Schnittstellensystem 40 hier austauschbar als „E/A-Gateway“ 40 bezeichnet. In der in **Fig. 1** dargestellten Ausführungsform werden das SDCS 100 und mindestens ein Bereich des E/A-Gateways 40 unter Verwendung eines gemeinsamen Satzes von Hardware- und Software-Rechenressourcen, z.B. einer gleichen Rechenplattform, implementiert. Das heißt, in der in **Fig. 1** dargestellten Ausführungsform teilen sich das SDCS 100 und mindestens ein Bereich des E/A-Gateways 40 (z.B. die Bereiche des E/A-Gateways 40, die Konvertierung, Routing, Switching usw. durchführen) zumindest einige Rechenhardware- und Softwareressourcen; das E/A-Gateway 40 beinhaltet jedoch darüber hinaus die physischen E/A-Ports oder E/A-Hardware-Schnittstellen zu den Daten- oder Kommunikationsverbindungen 42-58. In anderen Ausführungsformen können das SDCS 100 und das E/A Gateway 40 jedoch auf separaten, kommunikativ verbundenen Rechenplattformen implementiert sein, von denen jede einen separaten Satz von Hardware- und Software-Rechenressourcen nutzt, wie z.B. in **Fig. 2** dargestellt.

[0029] Was nun die Feldumgebung 12 betrifft, so zeigt **Fig. 1** verschiedene physische Komponenten und/oder Geräte (z.B. Prozesssteuerungseinrichtungen, Feldgeräte, Netzwerkelemente usw.), die darin angeordnet, installiert und miteinander verbunden sind und den industriellen Prozess (z.B. den physischen Prozess) während der Laufzeit der Anlage 10 steuern, indem sie z.B. miteinander kommunizieren und physisch arbeiten, um Roh- oder Eingangsmaterialien in gewünschte Produkte oder Ausgangsmaterialien umzuwandeln. Die verschiedenen Feldgeräte 60, 62, 70, 80, 90 und andere Feldkomponenten 68, 72, 82 können über das E/A-Gateway 40 Prozess-E/A an/von dem SDCS 100 kommunizieren, indem sie verschiedene Arten von Prozess-E/A verwenden.

[0030] Zum Beispiel können ein oder mehrere verdrahtete Feldgeräte (FDs) 60 in der Feldumgebung 12 angeordnet sein und über standardmäßige (z.B. traditionelle) verdrahtete physische E/A-Typen wie Analogausgang (AO), Analogeingang (AI), Diskreter Ausgang (DO), Diskreter Eingang (DI), usw. kommunizieren. Zu den verdrahteten Feldgeräten 60 können beispielsweise Ventile, Aktoren, Pumpen, Sensoren usw. gehören, die Datensignale erzeugen und Steuersignale empfangen, um damit ihre jeweiligen physischen Operationen in der Anlage 10 zu steuern sowie Status-, Diagnose- und andere Informationen bereitzustellen. Verdrahtete Feldgeräte 60 können über verdrahtete Verbindungen 42 mit dem E/A-Gateway 40 kommunizieren, wobei jedes bekannte verdrahtete Protokoll der Industrieautomatisierung wie 4-20 mA, Feldbus, Profibus, Modbus, HART usw. verwendet wird. Als solches kann das E/A-Gateway 40 entsprechende E/A-Karten oder Geräte (nicht abgebildet) beinhalten, die die über die Verbindungen 42 empfangene und gesendete Kommunikation bedienen. Zusätzlich oder alternativ können in einigen Konfigurationen ein oder mehrere verdrahtete Feldgeräte 60 direkt mit einer separaten E/A-Karte oder einem Gerät 61 verbunden sein, und die Kommunikation zu/von den separaten E/A-Karten oder Geräten 61 kann über eine Datenautobahn 58, wie z.B. ein Ethernet oder ein anderes geeignetes Transportmedium mit hoher Bandbreite, vom/-zum E/A Gateway 40 geliefert werden.

[0031] Die Feldumgebung 12 kann ein oder mehrere drahtlose Feldgeräte 62 beinhalten, von denen einige intrinsisch drahtlos und einige verdrahtete Feldgeräte sein können, die mit entsprechenden drahtlosen Adaptern verbunden sind. Die drahtlosen Feldgeräte und Adapter 62 können über jedes bekannte drahtlose Protokoll für die industrielle Automatisierung, wie z. B. WirelessHART, oder ein allgemeines drahtloses Protokoll, wie z. B. Wi-Fi, 4G LTE, 5G, 6G usw. über die jeweiligen drahtlosen Verbindungen 65 kommunizieren. Ein oder mehrere drahtlose Gateways 68 können die von den drahtlosen Geräten 62 über die drahtlosen Verbindungen 65 empfangenen drahtlosen Signale in drahtgebundene Signale umwandeln, die über eine oder mehrere Verbindungen 48 an das E/A-Gateway 40 geliefert werden, und können vom E/A-Gateway 40 über die Verbindungen 48 empfangene Signale in drahtlose

Signale umwandeln und die drahtlosen Signale über die drahtlosen Verbindungen 65 an die entsprechenden Empfängergeräte 62 übertragen. So können die Verbindungen 48 einen drahtlosen E/A-Typ unterstützen, und das E/A-Gateway 40 kann entsprechende drahtlose E/A-Karten oder Geräte (nicht dargestellt) beinhalten, die die über die Verbindungen 48 gesendeten und empfangenen Kommunikationen bedienen. In einer (in **Fig. 1** nicht gezeigten) Ausführungsform können zumindest einige der Links 48 direkt mit einer entsprechenden drahtlosen E/A-Karte oder einem Gerät verbunden sein, die bzw. das wiederum über eine Datenautobahn kommunikativ mit dem E/A-Gateway 40 verbunden sein kann (z.B. in ähnlicher Weise wie drahtgebundene Geräte 60 und E/A-Karten/Geräte 61), wobei die Datenautobahn in der Datenautobahn 58 beinhalten sein kann oder eine andere Datenautobahn sein kann.

[0032] Die Prozessanlage 10 kann eine Reihe von Feldgeräten 70 beinhalten, die über entsprechende Terminals 72, eine oder mehrere ferngesteuerte- oder Rangier-E/A-Schränke oder -Systeme 75 und eine oder mehrere Verbindungen 50 mit dem E/A Gateway 40 kommunikativ verbunden sind. Das heißt, jedes der Feldgeräte 70 kann unter Verwendung eines standardmäßigen oder herkömmlichen drahtgebundenen E/A-Typs (z. B. AO, DO, AI, DI usw.) über eine entsprechende physische Verbindung und ein Terminal 72 mit dem ferngesteuerten-Rangier-E/A-System 75 kommunizieren. Ein oder mehrere Prozessoren 78 des dezentralen E/A-Systems 75 können als lokaler Schalter des dezentralen E/A-Systems 75 dienen und somit die Kommunikation zu/von den physischen Terminals 72 (und den jeweils angeschlossenen Feldgeräten 70) und dem E/A-Schnittstellensystem 40, z.B. über Verbindungen 50, schalten oder weiterleiten. Dementsprechend können die Links 50 einen marshalled- oder entfernten-E/A-Typ unterstützen, und das E/A-Gateway 40 kann entsprechende E/A-Karten oder Geräte beinhalten, um die über die Links 50 gelieferten Kommunikationen zu bedienen. In einer (in **Fig. 1** nicht gezeigten) Ausführungsform können zumindest einige der Links 50 direkt mit einer jeweiligen entfernten E/A-Karte oder einem Gerät verbunden sein, die bzw. das wiederum mit dem E/A-Gateway 40 kommunikativ verbunden sein kann, und die Kommunikation zu/von der entfernten E/A-Karte oder dem Gerät kann von/zu dem E/A-Gateway 40 über eine Datenautobahn, über eine Datenautobahn (z.B. in ähnlicher Weise wie bei kabelgebundenen Geräten 60 und E/A-Karten/Geräten 61), wobei die Datenautobahn in der Datenautobahn 58 beinhalten sein kann oder eine andere Datenautobahn sein kann.

[0033] In einigen Implementierungen beinhaltet die Prozessanlage 10 eine Reihe von drahtgebundenen und/oder drahtlosen Feldgeräten 80, die über einen APL-Schalter 82 (Advanced Physical Layer) mit dem E/A-Gateway 40 kommunizieren. Im Allgemeinen liefern der APL-Schalter 82 und seine Verbindungen 85 Energie an die Feldgeräte 80 und in einigen Fällen an andere Geräte wie den drahtlosen Router 88, z.B. in einer Weise, die den gesetzlichen Energie-Sicherheitsanforderungen der gefährlichen Feldumgebung 12 entspricht. Typischerweise sorgen die APLkompatiblen Verbindungen 85 für den Datentransport zu/von den Feldgeräten 80 und dem drahtlosen Router 88 über Transportmedien und Paketprotokolle mit hoher Bandbreite, wie z.B. Ethernet und IP-Protokolle, oder andere geeignete Transportmedien und Paketprotokolle mit hoher Bandbreite. Einige der Feldgeräte 80 können Feldgeräte der nächsten Generation oder APL-kompatible Feldgeräte sein, und einige der Feldgeräte 80 können Standardfeldgeräte sein, die über entsprechende APL-Adapter mit den Links 85 verbunden sind. Ähnlich wie die Links 85 können auch die Links 55, die den APL-Schalter 82 und das E/A-Gateway 40 kommunikativ verbinden, APL-kompatible Transportmedien und/oder Paketprotokolle verwenden, wie z.B. Ethernet- und IP-Protokolle mit hoher Bandbreite, und somit können die Links 55 einen APL-E/A-Typ unterstützen. Folglich kann das E/A-Gateway 40 entsprechende E/A-Karten oder -Geräte beinhalten, um die über die Verbindungen 55 gelieferte Kommunikation zu bedienen.

[0034] In einigen Konfigurationen kann der APL-Schalter 82 oder ein anderer APL-Schalter (nicht gezeigt), der kommunikativ mit dem E/A-Gateway 40 verbunden ist, eine direkte Verbindung zu einem Remote-E/A-Bus herstellen, wie z.B. dem Remote-E/A-Bus, der in den Remote-E/A-Schränken oder Rangier- oder marshallingsystemen 75 beinhaltet ist, oder einem anderen Remote-E/A-Bus, der in einem anderen Remote-E/A-Schrank oder Rangiersystem (nicht gezeigt) beinhaltet ist. In diesen Konfigurationen kann der APL-Schalter Energie an den dezentralen E/A-Schrank oder das Rangier- oder marshalling-System liefern.

[0035] In einigen Konfigurationen kann die Prozessanlage 10 eine Reihe von Feldgeräten 90 beinhalten, die über Standard- oder Nicht-APL-Ethernet-Verbindungen 52 mit dem E/A-Gateway 40 kommunizieren. Beispielsweise können die Feldgeräte 90 über das E/A-Gateway 40 mit dem SDCS 100 kommunizieren, indem sie ein industrielles Steuerungs-IP-Protokoll, wie z.B. HART-IP oder ein anderes geeignetes industrielles Steuerungs-IP-Protokoll, über eine oder mehrere Ethernet-Verbindungen 52 mit hoher Bandbreite verwenden, die von der gefährlichen Feldumgebung 12 abgeschirmt sind, aber die Feldgeräte 90 nicht mit Energie versorgen. Als solche unterstützen die Verbindungen 52 einen Standard-Ethernet- oder Paket-E/A-Typ, und das E/A-Gateway 40 kann entsprechende E/A-Karten oder Geräte beinhalten, um die über die Verbindungen 52 gelie-

ferte Kommunikation zu bedienen. In einer (in **Fig. 1** nicht gezeigten) Ausführungsform können zumindest einige der Links 52 direkt mit einer entsprechenden IP-kompatiblen (Standard-Ethernet) E/A-Karte oder einem Gerät verbunden sein, die bzw. das wiederum über eine Datenautobahn (z.B. in ähnlicher Weise wie drahtgebundene Geräte 60 und E/A-Karten/Geräte 61) mit dem E/A-Gateway 40 kommunikativ verbunden sein kann, die in der Datenautobahn 58 beinhalten sein kann oder eine andere Datenautobahn sein kann.

[0036] Natürlich sind die in **Fig. 1** gezeigten Feldgeräte 60, 62, 70, 80, 90 und Feldkomponenten 68, 72, 82 nur beispielhaft. Andere Typen von Feldgeräten und Feldkomponenten der industriellen Prozessanlage 10 können zusätzlich oder alternativ in der Prozessanlage 10 verwendet werden und über das E/A Gateway 40 mit dem SDCS 100 kommunizieren, indem geeignete Verbindungen, Protokolle und Prozess E/A Typen verwendet werden.

[0037] **Fig. 2** zeigt ein Blockdiagramm der Architektur eines beispielhaften Software-definierten Steuerungssystems (SDCS) 200, das in der industriellen Prozessanlage von **Fig. 1** beinhalten sein kann. Zum Beispiel kann zumindest ein Bereich der Architektur 200 von dem SDCS 100 von **Fig. 1** verwendet werden. Allgemein gesprochen und wie unten beschrieben, verwendet das SDCS 200 eine geschichtete Architektur, in der die Geschäftslogik des SDCS 200 von der physischen Rechenplattform des SDCS 200 abstrahiert ist. Zur Vereinfachung der Diskussion wird das SDCS 200 unter gleichzeitiger Bezugnahme auf verschiedene Bereiche der industriellen Prozessanlage 10 von **Fig. 1** beschrieben; dies dient jedoch nur der Veranschaulichung und ist nicht einschränkend.

[0038] **Fig. 2** zeigt das SDCS 200 in kommunikativer Verbindung mit der Feldumgebung 12 über ein E/A-Schnittstellensystem oder E/A-Gateway 202, das im Gegensatz zum E/A-Schnittstellensystem 40 von **Fig. 1** eine Reihe von Hardware- und Software-Rechenressourcen verwendet, die sich von denen unterscheiden, die vom SDCS 200 genutzt werden. Die vom E/A Schnittstellensystem 202 bereitgestellten Funktionen 202a, wie z.B. das Vermitteln, Weiterleiten und Konvertieren der zwischen dem SDCS 200 und den in der Feldumgebung 12 der Prozessanlage 10 angeordneten Geräten oder Komponenten gelieferten Kommunikationen, werden z.B. durch die Nutzung der Hardware- und/oder Software-Rechenressourcen des E/A Gateway 202 ausgeführt. Als solche werden diese Funktionen 202a hier kategorisch und gemeinsam als „Netzwerkschalter“ 202a bezeichnet. Die vom Netzwerkschalter 202a genutzten Software- und Hardware-Ressourcen können auf einem oder mehreren Speichern und Prozessoren des E/A Gateway 202 implementiert sein. Der Netzwerkschalter 202a kann zum Beispiel auf einem oder mehreren Servern, in einer Bank von vernetzten Computergeräten, einem Cloud-Computing-System, einem oder mehreren Datenclustern usw. implementiert sein. Ähnlich wie das Schnittstellensystem 40 von **Fig. 1** beinhaltet das E/A-Schnittstellensystem 202 jedoch eine Reihe von physischen Ports oder Schnittstellen 202b, über die verschiedene Arten von E/A-Verbindungen 42-58 physische E/A vom SDCS 200 zu Komponenten der Feldumgebung 12 und umgekehrt liefern. Das E/A-Schnittstellensystem 202 und das SDCS 200 können über eine oder mehrere Verbindungen 205 kommunikativ verbunden sein, bei denen es sich typischerweise um Daten- oder Kommunikationsverbindungen mit hoher Bandbreite handelt.

[0039] Wie in **Fig. 2** gezeigt, beinhaltet die Architektur des SDCS 200 eine Rechenplattform 208 aus Hardware- und Software-Ressourcen, die die höheren Schichten der Architektur unterstützen. Dementsprechend wird die Rechenplattform 208 hier austauschbar als „physische Schicht 208“ des SDCS 200 bezeichnet, da sie physische Prozessoren, Prozessorkerne, Speicher und Netzwerkschnittstellen beinhaltet. Die physische Schicht 208 der Rechenplattform oder des SDCS beinhaltet eine Reihe von Datenzentrums-Clustern C1, C2, ..., Cn, von denen jeder eine entsprechende Anzahl von Knoten beinhaltet, wobei die Knoten innerhalb jedes Datenzentrums-Clusters zumindest teilweise, wenn nicht sogar vollständig, miteinander verbunden sein können. Jeder Knoten eines jeden Datenzentrums-Clusters beinhaltet einen oder mehrere Prozessoren und/oder Prozessor-Kerne, einen oder mehrere Speicher und entsprechende Netzwerkressourcen, wie eine oder mehrere physische Kommunikationsschnittstellen, die den Knoten mit einem oder mehreren anderen Knoten des Daten-Clusters kommunikativ verbinden. Ein Knoten kann beispielsweise auf einem einzelnen Server implementiert sein oder auf einer Bank oder einer Gruppe von Servern implementiert sein.

[0040] Zusätzlich ist jeder Datenzentrums-Cluster mit einem oder mehreren anderen Datenzentrums-Clustern der Plattform 208 kommunikativ verbunden oder vernetzt. Daher wird in dieser Beschreibung die Rechenplattform 208 des SDCS 200 auch als „Datenzentrums-Cluster“, „Rechenplattform Knoten“ oder „Knoten“ 208 bezeichnet. In **Fig. 2** kann das SDCS Hyper Converged Infrastructure (HCI)-Betriebssystem (OS) 210 (das hier austauschbar als „SD HCI OS“ 210 bezeichnet wird) des SDCS 200 verschiedene Knoten 208 zuweisen, bestimmen oder zuordnen, um die jeweiligen Rollen zur Unterstützung des SDCS 200 auszuführen, wie z.B. Rechenleistung (z.B. über die jeweiligen Prozessoren und/oder Rechenkerne des Knotens) oder Datenspeicherung (z.B. über die jeweiligen Speicher des Knotens). Knoten 208, die zur Durchführung von

Rechenaktivitäten des SDCS 200 zugewiesen, bestimmt oder zugeordnet sind, werden hier als „Rechenknoten“ oder „rechnende Knoten“ bezeichnet. Entsprechend werden die Knoten 208, die für die Durchführung von Speicheraktivitäten des SDCS 200 zugewiesen, bestimmt oder zugeordnet sind, hier als „Speicherknoten“ bezeichnet. Ein einzelner Knoten 208 kann nur als Rechenknoten, nur als Speicherknoten oder sowohl als Rechenknoten als auch als Speicherknoten verwendet werden, und die Rolle(n) jedes einzelnen Knotens 208 kann/-können sich im Laufe der Zeit dynamisch ändern, zum Beispiel auf Anweisung des SD HCI OS 210. Vorteilhafterweise ist die Rechenplattform 208 skalierbar, so dass einzelne Knoten 208 und/oder einzelne Cluster Cx leicht hinzugefügt, entfernt, ausgetauscht usw. werden können, wenn dies zur Unterstützung des Software-definierten Prozesssteuerungssystems 200 erforderlich ist, insbesondere in Übereinstimmung mit den Anforderungen der anderen, höheren Schichten des SDCS 200.

[0041] Das SDCS Hyper Converged Infrastructure (HCI)-Betriebssystem 210 wird auf der Rechenplattform 208 ausgeführt und kann auf der Grundlage jedes geeigneten Allzweck-HCI-Betriebssystems (OS) wie Microsoft Azure Stack, VMWare HCI, Nutanix AOS, Kubernetes Orchestration, einschließlich Linux Containers (LXC/LXD), Docker Containers, Kata Containers usw. aufgebaut sein. Als solches bietet das SDCS HCI OS 210 eine Reihe von Rechen-, Speicher- und Netzwerkunterstützungsdiensten in einer Weise, die allgemeinen HCI-Betriebssystemen ähnelt. Im Gegensatz zu allgemeinen HCI-Betriebssystemen reagieren diese SD HCI OS-Supportdienste im SDCS 200 jedoch vorteilhafterweise dynamisch auf das logische oder abstrahierte Prozesssteuerungssystem des SDCS 200, z.B. auf die Softwarekomponenten der Anwendungsschicht 212 des SDCS 200. Das heißt, wenn sich die Leistung, der Ressourcenbedarf und die Konfigurationen der verschiedenen Anwendungsschichtdienste, Subsysteme und anderen Softwarekomponenten der Anwendungsschicht 212 dynamisch ändern (und/oder von den Diensten innerhalb der Anwendungsschicht 212 dynamisch vorhergesagt wird, dass sie sich ändern), kann das SDCS HCI-Betriebssystem 210 automatisch und reaktionsschnell die Nutzung der Hardware- und/oder Software-Ressourcen 208 des SDCS 200 anpassen und/oder verwalten, um den Bedarf und die Anforderungen des SDCS 200 für die Datenverarbeitung, die Speicherung und die Vernetzung sowie für andere Funktionalitäten im Zusammenhang mit der industriellen Prozesssteuerung zu unterstützen. Zu diesem Zweck kann das SD HCI-Betriebssystem 210 eine Reihe von Unterstützungsdiensten beinhalten, darunter zum Beispiel einen Software-definierten (SD) Computing (oder Compute) Dienst 215, einen SD Speicherdienst 218, einen SD Netzwerkdienst 220, einen SD Orchestratordienst 222 und optional einen oder mehrere andere SDCS HCI OS Unterstützungsdienste und/oder Funktionen 225. In einer Ausführungsform beinhaltet das SDCS HCI-Betriebssystem 210 eine Allzweck-HCI-Betriebssystemplattform (z.B., Microsoft Azure Stack, VMWare HCI, etc.), die insbesondere so angepasst wurde, dass sie den SD Computing-Dienst 215, den SD Speicherdienst 218, den SD Netzwerkdienst 220, den SD Orchestratordienst 222 und die anderen SDCS HCI OS Unterstützungsdienste und/oder -funktionen 225 beinhaltet, wobei die Menge der Unterstützungsdienste 215-225 automatisch auf die SDCS Anwendungssoftwarekomponenten 212 des Software-definierten Steuerungssystems 200 reagiert und diese insbesondere unterstützt. Allgemein gesprochen werden das SD HCI OS 210 und die SD Unterstützungsdienste 212-225, die das SD HCI OS 210 bereitstellt, hier gemeinsam und allgemein als die „Software-definierte Netzwerkschicht“ 210 des SDCS 200 bezeichnet.

[0042] Da das SDCS HCI OS 210 insbesondere die Zuweisung der Hardware- und Software-Ressourcen des Knotens der physischen Schicht 208 über die SDCS HCI OS-Unterstützungsdienste 215-225 verwaltet, können die SDCS HCI OS-Unterstützungsdienste 215-225 als Schnittstellendienste zwischen dem SDCS HCI OS 210 und den übergeordneten Diensten, Subsystemen und anderen Softwarekomponenten der Anwendungsschicht 212 des SDCS 200 dienen und/oder einen Rahmen für die übergeordneten Dienste, Subsysteme und anderen Softwarekomponenten der Anwendungsschicht 212 bieten. Als solche können die Softwarekomponenten der SDCS Anwendungsschicht 212 mit dem SD HCI OS 210 (und in einigen Fällen insbesondere mit einem oder mehreren seiner SD-spezifischen Unterstützungsdienste 215, 218, 220, 222, 225) über eine Reihe von Anwendungsprogrammierschnittstellen (APIs) 228, entweder über einen HCI-Adapter 230 (hier auch als „HCI-Adapter Schicht“ 230 bezeichnet) und eine andere Reihe von APIs 232 oder direkt (in **Fig. 2** nicht dargestellt) verbunden sein. Die HCI-Adapter Schicht 230 ermöglicht der SDCS Anwendungsschicht 212 den Zugriff auf die Unterstützungsdienste 215, 218, 220, 222, 225 und bleibt dabei unabhängig von den Besonderheiten des allgemeinen HCI-Betriebssystems (z.B. Microsoft Azure Stack, VMWare HCI, etc.), das mit solchen SD-spezifischen Diensten 215-225 angepasst wurde, um das SD HCI OS 210 zu bilden. Dementsprechend transformiert oder übersetzt der HCI-Adapter 230 die von der SDCS-Anwendungsschicht 212 genutzten APIs 228 in eine Reihe von APIs 232, die dem angepassten oder adaptierten Allzweck-HC-Betriebssystem 210 des SDCS 200 bekannt oder dazu kompatibel sind.

[0043] Im Gegensatz zu verallgemeinerten, geschichteten IT (Informationstechnologie)-Systemarchitekturen, bei denen geschäftslogische Anwendungen von der Hardware- und Software-Rechenplattform abstrahiert werden und bei denen die Verwaltung der Rechenplattform-Ressourcen weitgehend von menschlichen IT-Administratoren gesteuert und gestaltet wird, abstrahiert die Architektur des SDCS 200 nicht nur die übergeordneten, geschäftslogischen Dienste, Subsysteme und andere Softwarekomponenten der Anwendungsschicht 212 von der Hardware- und Software-Rechenplattform 208, sondern ermöglicht es den übergeordneten SD-Diensten, Subsystemen und anderen Softwarekomponenten 212, die Nutzung der Hardware- und Software-Ressourcen des Knotens und der Cluster der Rechenplattform 208 dynamisch, automatisch und reaktionsschnell zu steuern und zu verändern, z. B., über die APIs 228 und die SD-Unterstützungsdienste 215, 218, 220, 222, 225, und ohne dass ein menschliches Eingreifen oder eine Anweisung erforderlich ist. Insbesondere und vorteilhafterweise reagiert die Verwaltung der Ressourcen der Rechenplattform 208 dynamisch auf Änderungen der Konfigurationen und des Bedarfs dieser übergeordneten SD-Dienste, Subsysteme und anderen Softwarekomponenten der Anwendungsschicht 212, und zwar insbesondere im Hinblick auf die besonderen Anforderungen, Vorgaben und Grenzen der industriellen Prozesssteuerungssysteme.

[0044] Im SDCS 200 werden die industrielle Prozesssteuerung und andere zugehörige Geschäftslogik von den übergeordneten SD-Diensten, Subsystemen und anderen Softwarekomponenten 235, 238, 240, 242, 248 in der Anwendungsschicht 212 des SDCS 200 ausgeführt. Der Einfachheit halber werden diese übergeordneten SD-Dienste, Subsysteme und anderen Softwarekomponenten 235-248 in dieser Beschreibung kategorisch als Software-definierte „Anwendungsschichtsoftwarekomponenten“ des SDCS 200 bezeichnet. Zusammen bilden die Sätze der SD-Anwendungsschichtkomponenten 235, 238, 240, 242 (und optional zumindest einige der Drittanbieterdienste 248) ein logisches Prozesssteuerungssystem 245 (hier auch austauschbar als „virtuelles Prozesssteuerungssystem“ 245 bezeichnet) zur Steuerung eines oder mehrerer industrieller oder physischer Prozesse, die z.B. in der industriellen Prozessanlage 10 ablaufen. Wie in **Fig. 2** dargestellt, beinhalten die SD-Anwendungssoftwarekomponenten 212 eine Reihe von Prozesssteuerungsdiensten 235 und eine Reihe von Prozesssteuerungssubsystemen 238 und können optional eine Reihe von anderen SDCS-Geschäftslogikdiensten 240 beinhalten. In **Fig. 2** ist der E/A-Serverdienst 242 aus Gründen der Klarheit der Diskussion (und nicht zur Einschränkung) separat dargestellt; der E/A-Serverdienst 242 kann jedoch in einem Teilsystem 238 des SDCS 200 beinhalten sein oder in der Menge anderer SDCS-Geschäftslogikdienste 240 beinhalten sein. In der Tat kann in anderen Ausführungsformen des SDCS 200 (nicht gezeigt) zumindest ein entsprechender Bereich oder die Gesamtheit des E/A-Serverdienstes 242 im HCI-Adapter 230, im SD HCI-Betriebssystem 210 und/oder sogar im Netzwerkschalter 202a implementiert sein. Zusätzlich können in einigen Implementierungen des SDCS 200 eine Reihe von Geschäftslogikdiensten 248 von Drittanbietern in der SDCS-Anwendungsschicht 212 ausgeführt werden und können als Teil des logischen Prozesssteuerungssystems 245 arbeiten oder auch nicht. Die Dienste 248 von Drittanbietern können beispielsweise von einem Software Development Kit (nicht gezeigt) des SDCS 200 generiert werden, mit dem der Nutzer die Dienste 248 von Drittanbietern auf der SD Anwendungsschicht 212 entwickeln, generieren, installieren und verwalten kann. Der E/A-Serverdienst 242 und die Dienste von Drittanbietern 248 werden an anderer Stelle in dieser Beschreibung ausführlicher beschrieben.

[0045] In einer Ausführungsform können zumindest einige der SD-Anwendungssoftwarekomponenten 235-248 als Microdienste eingesetzt werden, die über einen Microdienst-Bus (nicht dargestellt) kommunikativ verbunden sind, so dass die Microdienste 235-248 Daten an andere Microdienste 235-248 übertragen und von diesen empfangen können. Die Microdienste 235-248 und die Übermittlung von Daten zwischen ihnen können vom E/A-Serverdienst 242 und/oder vom SD HCI-Betriebssystem 210 und seinen SD-Supportdiensten 215-225 unterstützt und/oder verwaltet werden. Die SD-Anwendungssoftwarekomponenten 235-248 können auf jeder geeigneten Hardware-Plattform 208 ausgeführt werden, auf der das SD-HCI-Betriebssystem 210 laufen kann, z. B. auf Server-Hardware, eingebetteter Hardware und dergleichen. Dementsprechend können die Microdienste 235-248 geschäftslogische Komponenten des SDCS 200 sein, die von der Rechenplattform 208 abstrahiert sind.

[0046] Innerhalb der Architektur des SDCS 200 können die Anwendungssoftwarekomponenten 235-248 in Containern, virtuellen Maschinenumgebungen mit Thick-Provisioning, virtuellen Maschinenumgebungen mit Thin-Provisioning und/oder anderen geeigneten Arten von gekapselten Ausführungsumgebungen als Instantiated Software Components (ISCs) ausgeführt werden. Eine ISC kann beispielsweise ein Container sein, der mit einer Instanz einer bestimmten Anwendungsschichtsoftwarekomponente 235-248 konfiguriert ist, um einen konfigurierten Container oder ein Containerbild für die bestimmte Anwendungsschichtsoftwarekomponente 235-248 zu bilden, und das Containerbild der bestimmten Anwendungsschichtsoftwarekompo-

nente 235-248 kann für die Ausführung auf einem bestimmten Knoten 208 als eine bestimmte ISC instanziiert werden. In einem anderen Beispiel kann eine ISC eine bestimmte Anwendungsschichtsoftwarekomponente 235-248 sein, die als Instanz einer virtuellen Maschine (z.B. einer virtuellen Prozess- oder Anwendungsmaschine) implementiert ist, um ein virtuelles Maschinenbild für die bestimmte Anwendungsschichtsoftwarekomponente 235-248 zu bilden, und das virtuelle Maschinenbild der bestimmten Anwendungsschichtsoftwarekomponente 235-248 kann zur Ausführung auf einem bestimmten Knoten 208 als eine bestimmte ISC instanziiert werden. Unabhängig davon, ob sie auf Containern oder virtuellen Maschinen basieren, isolieren die gekapselten Ausführungsumgebungen der SD-Anwendungssoftwarekomponenten 235-248 die instanziierten und ausgeführten Softwarekomponenten 235-248 von anderen Diensten und Anwendungen, die auf demselben Knoten 208 ausgeführt werden. Zur Vereinfachung der Diskussion (und nicht zur Einschränkung) werden die Ausführungsumgebungen der SD Anwendungsschichtsoftwarekomponenten 235-248 hier als „Container“ bezeichnet, obwohl ein Fachmann verstehen wird, dass die hier beschriebenen Prinzipien und Techniken in Bezug auf Container leicht auf virtuelle Maschinen angewendet werden können, falls gewünscht.

[0047] Mit dem SDCS 200 kann jede Instanz eines Anwendungsschichtdienstes 235, 240, 248 in einem entsprechenden Container ausgeführt werden, jedes Subsystem 238 kann in einem entsprechenden Container bereitgestellt oder ausgeführt werden, der E/A-Serverdienst 242 kann in einem entsprechenden Container ausgeführt werden, usw., wodurch entsprechend konfigurierte Container oder Containerabbilder gebildet werden. Beispielsweise kann ein Steuerungsdienst 235 mit einem oder mehreren Prozess-Steuerungsmodul-Diensten 235, Parametern und Werten der industriellen Prozessanlage 10, wie z.B. Kennzeichnungen von Eingängen und Ausgängen, Referenzwerten und dergleichen, konfiguriert werden, wodurch ein konfigurierter oder programmierter Steuerungsdienst entsteht. Ein Container kann mit einer Instanz des konfigurierten Steuerungsdienstes konfiguriert werden, wodurch ein Containerbild des konfigurierten Steuerungsdienstes entsteht. Anders ausgedrückt, der konfigurierte Container beinhaltet eine Instanz des konfigurierten Steuerungsdienstes, wobei die Instanz des konfigurierten Steuerungsdienstes ausführbar ist, um den spezifischen, konfigurierten Satz von Prozesssteuerungslogik unter Verwendung der konfigurierten Steuerungsmodul-Container, Tags, Referenzwerte usw. auszuführen. Mehrere Instanzen eines konfigurierten Steuerungsdienstes (oder anderer konfigurierter Dienste) können von der SDCS 200 instanziiert und ausgeführt werden, wie an anderer Stelle in dieser Beschreibung beschrieben wird.

[0048] Containerbilder (oder Instanzen von konfigurierten Steuerungsdiensten innerhalb von Containern) können zugewiesen, angeheftet oder dynamisch zugewiesen werden, z.B. über den SD Rechendienst 215, um auf entsprechenden SD Knoten und/oder Datenzentrums-Clustern 208 ausgeführt zu werden. Der SD Rechendienst 215 kann die Containerbilder und ihre jeweiligen Zuweisungen zu den Rechenknoten 208 bei Bedarf dynamisch ändern, aktualisieren, pflegen und/oder anderweitig verwalten, z.B. zum Lastausgleich zwischen den Rechenknoten 208, zur planmäßigen Wartung der Rechenknoten 208 und/oder ihrer physischen Komponenten, als Reaktion auf erkannte Leistungsprobleme, zur Unterstützung der Erweiterung oder Verkleinerung des logischen Prozesssteuerungssystems 245, zur Unterstützung der Erweiterung oder Verkleinerung der Rechenplattform 208 usw. In einigen Implementierungen können Container, in denen die Anwendungssoftwarekomponenten 235-248 ausgeführt werden (z.B. konfigurierte Container oder Containerbilder), einem E/A-Gerät außerhalb des (z.B. getrennt vom) SDCS 200 zugewiesen oder angeheftet werden (oder auf andere Weise ausgeführt werden), wie z.B. einem Gerät, das zum E/A-Schnittstellensystem 202 gehört. In diesen Implementierungen ermittelt das SDCS 200 solche konfigurierten Container, die auf anderen Geräten/Systemen ausgeführt werden (die hier als „Mikrocontainer“ bezeichnet werden), und bezieht die ermittelten Mikrocontainer in die Netzwerkplanung und andere Aspekte ein, die dem logischen Prozesssteuerungssystem 245 entsprechen.

[0049] Innerhalb des SDCS 200 können einige konfigurierte Container den jeweiligen SD-Rechenknoten 208 zugewiesen oder zugeordnet werden und vom SD-Rechen-Dienst 215 auf der Grundlage von sich dynamisch ändernden Konfigurationen, Leistungen und Bedürfnissen des logischen Prozesssteuerungssystems 245 dynamisch anderen SD-Rechenknoten 208 neu zugewiesen werden. In manchen Situationen können Container zugewiesen (und wieder zugewiesen) werden, um von bestimmten Prozessoren oder bestimmten Prozessorkernen des SD Rechenknotens 208 ausgeführt zu werden. Einige konfigurierte Container können jedoch an den jeweiligen SD Rechenknoten 208 angeheftet sein (z.B. durch den SD Rechendienst 215, durch eine Konfiguration, durch einen Nutzer usw.) und werden nicht dynamisch durch den SD Rechendienst 215 aufgrund von dynamisch auftretenden Bedingungen neu zugewiesen. Das heißt, ein angehefteter konfigurierter Container kann auf dem SDC-Rechenknoten 208 ausgeführt werden, an den der konfigurierte Container angeheftet ist, bis der konfigurierte Container von dem Rechenknoten 208 gelöst wird, z.B. unabhängig von dynamischen Bedingungen des logischen Prozesssteuerungssystems 245 (außer vielleicht dem Ausfall des Rechenknotens

208, an den der konfigurierte Container angeheftet ist). Anders ausgedrückt: Die Software-definierte Netzwerkschicht 210 kann die Nutzung durch den angehefteten konfigurierten Container auf die Hardware- und/oder Software-Ressourcen beschränken, an die er angeheftet ist, und wenn der konfigurierte Container gelöst wird, hebt die SD Netzwerkschicht 210 die Beschränkung auf. Container können zusätzlich oder alternativ an andere physische oder logische Komponenten des SDCS 200 angeheftet werden, falls gewünscht. Beispielsweise kann ein Container an einen anderen Container, an einen bestimmten Datencluster, an eine bestimmte Verarbeitungsressource (z.B. einen bestimmten physischen Prozessor oder einen bestimmten physischen Prozessorkern eines SD Rechenknotens 208), an ein physisches Rack oder einen Bereich eines physischen Racks, das von einer bestimmten Energieversorgung bedient wird (wobei das physische Rack physisch die Hardware eines oder mehrerer Knoten beherbergt), usw. angeheftet werden.

[0050] Darüber hinaus können konfigurierte Container in anderen konfigurierten Containern verschachtelt werden, was bei der Konfiguration und Organisation des logischen Prozesssteuerungssystems 245 besonders nützlich ist. Wenn beispielsweise ein bestimmtes Prozesssteuerungssubsystem 238 einen bestimmten Satz von Steuerungsdiensten 235 und/oder anderen SDCS-Diensten 240 bereitstellt, kann ein konfigurierter Container jedes bereitgestellten Dienstes 235, 240 des bestimmten Satzes in den konfigurierten Container des bestimmten Prozesssteuerungssystems 238 verschachtelt werden. Die Zuweisung/Zuordnung von konfigurierten Containern zu Rechenknoten 208, das Anheften und die Verschachtelung von konfigurierten Containern wird an anderer Stelle in dieser Beschreibung ausführlicher beschrieben.

[0051] Der Klarheit und Einfachheit halber wird der Begriff „Container“ hier verwendet, um sich allgemein auf eine instanziierte Softwarekomponente (ISC) zu beziehen, die ein konfigurierter Container oder ein Containerbild ist, z.B. ein Container, der so konfiguriert wurde, dass er eine Instanz eines entsprechenden SDCS-Steuerungsdienstes, eines SDCS-Subsystems oder eines anderen vom SDCS 200 bereitgestellten Dienstes beinhaltet. Dementsprechend kann im Rahmen dieser Beschreibung ein „Container“ instanziiert und zur Ausführung an einen Rechenknoten 208 zugewiesen werden, ein „Container“ kann an einen bestimmten Rechenknoten oder an andere Container angeheftet werden, und ein „Container“ kann in einem anderen „Container“ verschachtelt werden.

[0052] In jedem Fall können Container in ähnlicher Weise wie bei den Rechenressourcen der Rechenplattform 208 dynamisch zugewiesen und/oder zugeordnet, angeheftet und/oder verschachtelt werden, z.B. über den SD Speicherdienst 218, zu verschiedenen SDC Speicherknoten 208, um dadurch verschiedene Speicheranforderungen des logischen Prozesssteuerungssystems 245 zu unterstützen. Der SD Speicherdienst 218 kann zum Beispiel die logischen Speicherressourcen, die von den Containern des logischen Prozesssteuerungssystems 245 genutzt werden, über verschiedene physische Hardware-Speicherressourcen eines oder mehrerer Knoten 208 verwalten und managen. Zum Beispiel können der konfigurierte Container und der für seine Operationen benötigte Speicher (z.B. Random Access Speicher oder ähnliches) auf einem bestimmten SD Speicherknoten 208 oder einem bestimmten Speichergerät oder Speicherplatz eines SD Speicherknotens 208 gespeichert sein. Beispiele für Arten von physischen Hardware-Speicherressourcen 208 sind unter anderem (aber nicht ausschließlich) Pools von Volume-Dateisystemen auf mehreren Festplatten (und/oder Flash-Laufwerken), NRAM, MRAM, FRAM, PRAM und/oder andere Arten von NVRAM, NVMe-Speicher, um nur einige zu nennen. Darüber hinaus können einige Container, falls gewünscht, an den jeweiligen SD Speicherknoten 208 und/oder an bestimmte Speichergeräte oder Speicherbereiche des SD Speicherknotens 208 angeheftet werden. Der SD Speicherdienst 218 kann die physischen Hardwarespeicher oder Speicher 208 ändern, aktualisieren oder anderweitig verwalten, um die logischen Speicherressourcen des SDCS 200 zu unterstützen, wenn und soweit dies erforderlich ist, z.B. aufgrund von Festplatten- oder anderen Fehlern, für geplante Wartungsarbeiten, aufgrund der Hinzufügung/Erweiterung von verfügbaren physischen Speichern in der Rechenplattform 208, usw.

[0053] In ähnlicher Weise kann der SD-Netzwerkdienst 220 das logische oder virtuelle Netzwerk, das vom logischen Prozesssteuerungssystem 245 genutzt wird, verwalten und managen, das vom SD-Netzwerkdienst 220 über den Knoten 208 implementiert werden kann. Der SD-Netzwerkdienst 220 kann beispielsweise die Netzwerk- und Hardwareressourcen der Rechenplattform 208 verwalten und managen, um die logischen Netzwerkfunktionen des logischen oder virtuellen Prozesssteuerungssystems 245 zu unterstützen, wie z.B. virtuelle Schnittstellen, virtuelle Switches, virtuelle private Netzwerke, virtuelle Firewall-Regeln und ähnliches, sowie um die erforderliche Vernetzung zwischen verschiedenen Containern oder Containerbilder des logischen Prozesssteuerungssystems 245 zu unterstützen. Da das logische Prozesssteuerungssystem 245 die industrielle Prozessanlage 10 bedient, sind das Timing und die Synchronisierung der logischen und physischen Komponenten des SDCS 200 und die Vernetzung dazwischen von entscheidender Bedeutung, da verpasste und/oder verloren gegangene Nachrichten

oder Kommunikationen dazu führen können, dass der industrielle oder physische Prozess unkontrolliert wird, was wiederum zu katastrophalen Folgen wie Überlauf, Gasaustritt, Explosionen, Verlust von Geräten und in manchen Situationen auch zum Verlust von Menschenleben führen kann. Glücklicherweise reagiert der SD-Netzwerkdienst 220 auf das kritische Prozess-E/A-Timing und die Synchronisierung des SDCS 200, so dass die Kommunikation (und insbesondere die Kommunikation zu/von den Steuerungsdiensten 235) zuverlässig, zeitnah und deterministisch erfolgen kann. Beispielsweise kann der SD-Netzwerkdienst 220 die Zeitsynchronisation des Datenzentrums-Clusters 208 auf 1 Millisekunde genau unterstützen, um die erforderliche Synchronisation zwischen den ProzessSteuerungsdiensten 235, den Prozess-Steuerungssubsystemen 238, dem E/A-Server 242 und anderen SDCS-Diensten 240, 248 der SDCS-Anwendungsschicht 212 sicherzustellen.

[0054] Neben dem SD Rechendienst 215, dem SD Speicherdienst 218 und dem SD Netzwerkdienst 220 kann das SD HCI-Betriebssystem 210 weitere OS-Unterstützungsdienste 225 bereitstellen, auf die über die APIs 228, 232 zugegriffen werden kann und die von der Anwendungsschicht 212 zur Unterstützung des logischen Prozesssteuerungssystems 245 genutzt oder aufgerufen werden. Zu den anderen SD HCI OS-Diensten 225 können beispielsweise ein Dienst zur Verwaltung des Lebenszyklus, ein Suchdienst, ein Sicherheitsdienst, ein Verschlüsselungsdienst, ein Dienst zur Verwaltung von Zertifikaten, ein Schlüsselverwaltungsdienst, ein Autentifizierungsdienst, ein Zeitsynchronisierungsdienst, ein Dienst zum Auffinden von Standorten und/oder ein Konsolenunterstützungsdienst gehören (alle in **Fig. 2** nicht dargestellt), um nur einige zu nennen. Eine detailliertere Diskussion dieser anderen Prozesssteuerungssystem-bezogenen OS-Unterstützungsdienste 225 findet sich an anderer Stelle in dieser Beschreibung. In einigen Ausführungsformen des SDCS 200 können einer oder mehrere der Unterstützungsdienste in der Anwendungsschicht 212 ausgeführt werden, z.B. als andere SDCS-Dienste 240, anstatt in der Software-definierten Netzwerkschicht 210 als OS-Unterstützungsdienste 225 ausgeführt zu werden.

[0055] In der Anwendungsschicht 212 des SDCS 200 stellt die Menge der SD-Prozess-Steuerungsdienste 235 die Prozesssteuerungs-Geschäftslogik des logischen Prozesssteuerungssystems 245 bereit. Jeder unterschiedliche Steuerungsdienst 235 kann mit den gewünschten Parametern, Werten usw. und optional anderen Steuerungsdiensten 235 konfiguriert werden; jede Instanz eines konfigurierten Steuerungsdienstes 235 kann in einem entsprechenden Container ausgeführt werden; und jeder Container kann zur Ausführung einem entsprechenden Knoten oder Cluster zugewiesen (oder angeheftet) werden. So kann jeder konfigurierte Steuerungsdienst 235 eine logische oder Software-definierte Steuerungseinheit sein, die funktionell ähnlich konfiguriert werden kann wie ein herkömmliches, hardwareimplementiertes Prozesssteuerungsgerät, Prozesssteuerungsmodul, Prozesssteuerungsfunktionsblock usw. Im Gegensatz zu traditionellen, hardwareimplementierten Prozesssteuerungsgeräten, traditionellen Steuerungsmodulen und traditionellen Steuerungsfunktionsblöcken kann das SDCS 200 jedoch vorteilhafterweise mehrere Instanzen eines gleich konfigurierten Steuerungsdienstes 235 für verschiedene Zwecke wie Leistung, Fehlertoleranz, Wiederherstellung und ähnliches einfach replizieren. Beispielsweise kann ein Steuerungsdienst (der in einem eigenen Container ausgeführt wird) so konfiguriert werden, dass er einen Steuerungsmodul-Dienst (der in einem eigenen Container ausgeführt wird) ausführt, und der Steuerungsmodul-Dienst kann so konfiguriert werden, dass er eine Reihe von Steuerungsfunktionsblock-Diensten ausführt (von denen jeder in einem eigenen Container ausgeführt wird und jeder mit entsprechenden Parametern, Werten usw. konfiguriert werden kann). So kann der Satz von Containern, der dem Satz von konfigurierten Steuerungsfunktionsblockdiensten entspricht, in den Steuerungsmoduldienstcontainer verschachtelt werden, und der Steuerungsmoduldienstcontainer kann in den Steuerungsdienstscontainer verschachtelt werden. Der Satz von Containern, der dem Satz von konfigurierten Funktionsblockdiensten entspricht, kann zur Ausführung auf verschiedenen Kernen eines physischen Schichtprozessors 208 zugewiesen werden, z.B. zum Zwecke des Lastausgleichs. Wenn sich die Auslastung ändert, können ein oder mehrere Funktionsblockdienstcontainer verschoben werden, um auf anderen Prozessorkernen, anderen Prozessoren oder sogar anderen Knoten ausgeführt zu werden, um die Auslastung wieder auszugleichen; der verschobene Funktionsblockdienstcontainer wäre jedoch weiterhin unter dem Steuerungsmoduldienstcontainer verschachtelt und würde entsprechend ausgeführt.

[0056] Zusätzlich zu den Software-definierten Steuerungsdiensten 235 kann die SDCS-Anwendungsschicht 212 auch andere Arten von SDCS-Anwendungsschichtdiensten 240 beinhalten, wie z.B. Bedieneranzeigen und Schnittstellen, Diagnose, Analysen, Sicherheitsroutinen, Berichte, Historisierung von Daten, Konfiguration von Diensten, Konfiguration von Containern, Kommunikation von Informationen mit externen oder anderen Systemen, usw. Im Allgemeinen kann jedes Modul oder jede prozesssteuerungssystembezogene Funktionalität oder Geschäftslogik, die in einem herkömmlichen Prozesssteuerungssystem konfiguriert und in ein bestimmtes physisches Gerät des herkömmlichen

Prozesssteuerungssystems heruntergeladen und/oder dort instanziiert werden kann, um während der Laufzeit einer industriellen Prozessanlage ausgeführt zu werden, im SDCS 200 als ein entsprechender Dienst 235, 240 logisch implementiert werden, der in einem entsprechenden Container ausgeführt wird. Darüber hinaus kann jeder der containerisierten SD-Steuerungsdienste 235 eine kommunikative Verbindung, z.B. über die SD-Netzwerkschicht 210, mit einem oder mehreren Geräten in der Feldumgebung 12 der industriellen Prozessanlage (z.B., Prozesssteuerungsfeldgeräte 60, 62, 70, 80, 90; Nutzer-Schnittstelle-Geräte und/oder andere Feldumgebungsgeräte) und/oder mit einem oder mehreren Nutzer-Schnittstellen/Nutzer-Schnittstelle-Geräten 20a-20e kommunizieren, um E/A-Daten und/oder andere Datentypen dazwischen zu übertragen, wenn dies von der Geschäftslogik des containerisierten SD-Steuerungsdienstes 235 und/oder vom Empfängergerät (oder der auf dem Empfängergerät ausgeführten Anwendung oder dem Dienst) verlangt wird. In manchen Situationen können verschiedene containerisierte SD Steuerungsdienste 235 mit anderen containerisierten SD Steuerungsdiensten 235 und/oder mit anderen SDCS-Diensten 240 kommunizieren (z.B. über die SD Netzwerkschicht 210, den E/A Server Dienst 242, den Microdienst-Bus usw.), um Daten zwischen ihnen zu übertragen, wenn ihre jeweilige Geschäftslogik dies erfordert.

[0057] Die SD-Subsysteme 238 in der Anwendungsschicht 212 des SDCS 200 stellen die virtuellen oder logischen Prozesssteuerungs-Subsysteme des logischen Prozesssteuerungssystems 245 bereit. Jedes unterschiedliche SD-Subsystem 238 kann von einem entsprechenden Container bereitgestellt oder in diesem ausgeführt werden. In einigen Fällen (in **Fig. 2** nicht dargestellt) kann ein Subsystem 238 einen oder mehrere Anwendungsschichtdienste bereitstellen oder beinhalten, und als solche können die Container der von dem Subsystem bereitgestellten Dienste 235, 238 in dem Subsystem-Container verschachtelt sein. Ein Historiker-Subsystem 238 kann beispielsweise einen Lesedienst, einen Schreibdienst und einen Suchdienst beinhalten, deren jeweilige Container in den Historiker-Subsystem-Container verschachtelt sind. In einem anderen Beispiel kann ein Batch-Prozesssteuerungssubsystem 238 einen Einheitsprozedurdienst, einen Rezepturdienst und einen Dienst zur Erzeugung von Regulierungsprotokollen beinhalten, die im Container des Batch-Prozesssteuerungssystems verschachtelt sein können. Im Allgemeinen ermöglicht die Menge der SD-Subsysteme 238 eine einfache und kohärente Gruppierung und/oder Verwaltung der SDCS-Steuerungsdienste 235 und anderer SDCS-Dienste 240. In einer bevorzugten Ausführungsform beherbergt jeder Knoten 208 des SDCS 200 eine entsprechende Instanz jedes Subsystems des Satzes von SD-Subsystemen 238, so dass z.B. Subsystemdienste für andere Anwendungsschichtdienste 235, 240, 248, die momentan auf jedem Knoten 208 ausgeführt werden, unmittelbar und leicht verfügbar sind. Dementsprechend können Änderungen an einem oder mehreren der Subsysteme 238 zwischen den entsprechenden Instanzen koordiniert werden, die an jedem Knoten 208 ausgeführt werden (z.B. unter der Leitung des SD HCI OS 210). Dadurch ist der Satz von SD-Subsystemen 238 nicht nur in hohem Maße und in unmittelbarer Nähe für jeden SD-Dienst 235, 240, 248 verfügbar, der auf demselben Knoten 208 ausgeführt wird, sondern im Falle des Ausfalls eines Knotens, des Ausfalls einer Knotenkomponente oder des Ausfalls einer bestimmten Subsysteminstanz an einem Knoten können die von dem Satz von SD-Subsystemen 238 bereitgestellten Funktionalitäten für das logische Prozesssteuerungssystem 245 problemlos aufrechterhalten werden. Beispiele für SD-Subsysteme 238 sind unter anderem: kontinuierliche Prozesssteuerung, ereignisgesteuerte Prozesssteuerung, Batch-Prozesssteuerung, zustandsbasierte Steuerung, Kontaktplansteuerung, Historiker, Edge-Connectivity, Prozessnutzer, Alarm, Lizenzierung, Ereignis, Versionskontrolle, Prozesskonfiguration und Prozess-E/A, um nur einige zu nennen.

[0058] Der Satz von SD-Subsystemen 238 kann zum Beispiel ein kontinuierliches Prozesssteuerungssubsystem beinhalten. Das Steuerungssubsystem für kontinuierliche Prozesse kann eine Reihe von Steuerungsdiensten 235 beinhalten, die für die Ausführung von Prozesssteuerungen zuständig sind, die auf die kontinuierliche Produktion und den Betrieb zugeschnitten sind. Zum Beispiel können die vom kontinuierlichen Prozess Steuerungssubsystem bereitgestellten Steuerungsdienste 235 eine modulare Steuerung (z.B. Steuerungsmodul-Dienste) ausführen, die eine periodische Ausführung mit E/A-Zuweisung ermöglicht. Die Geschäftslogik der (logischen und physischen) Einheiten des Steuerungssystems, die innerhalb des Steuerungssubsystems für kontinuierliche Prozesse verwaltet werden können, kann Steuerungen, E/A-Zuweisungen, Steuerungsmodule, Funktionsblöcke, Kontaktplanlogik und strukturelle, textbasierte Steuerungsalgorithmen beinhalten (um nur einige zu nennen). Kontinuierliche Steuerungsmodul-Dienste können periodisch geplant werden, mit oder ohne Modulverkettung. Kontinuierliche Steuerungsmodul-Dienste können zum Beispiel Ausführungsketten bilden, so dass eine vom Benutzer definierte Menge von kontinuierlichen Steuerungsmodul-Diensten nacheinander verkettet ausgeführt werden kann. Die Kette der kontinuierlichen Steuerungsmodul-Dienste kann zu einem zugewiesenen (periodischen) Ausführungsquantum in einer Best-Effort-Auswertung der in der Modul-Dienstkette beinhalteten Steuerungslogik ausgeführt werden. Unverkettete kontinuierliche Steuerungsmodul-Dienste können parallel zu verket-

teten kontinuierlichen Steuerungsmodul-Diensten während desselben periodischen Quantums ausgeführt werden.

[0059] In einem anderen Beispiel kann die Menge der SD-Subsysteme 238 ein zustandsbasiertes Prozesssteuerungssubsystem beinhalten. Das zustandsbasierte Prozesssteuerungssystem kann einen Satz zustandsbasierter Steuerungsdienste 235 beinhalten, die für die Verfolgung, Zuweisung und Ableitung des Zustands des Prozesssteuerungssystems 245 als Ganzes verantwortlich sind. Im Allgemeinen können zustandsbasierte Operationen des Prozesssteuerungssystems Operationen beinhalten, die dazu dienen, den Zustand des Prozesses (oder eines Bereichs davon) in einer Reihe von Prozesseinheiten innerhalb der Assetinfrastruktur automatisch oder halbautomatisch zu ändern. Jede Zustandsoperation kann z.B. in der Lage sein, einen aktuellen Zustand einer Prozesseinheit abzuleiten, den aktuellen Zustand zu bestimmen, Unterschiede zwischen dem aktuellen Prozesszustand und aufgezeichneten Normalisierungen für einen bekannten Prozesszustand zu analysieren und den Prozess zu steuern, um einen Prozesszustand zu erreichen.

[0060] Zum Beispiel kann das zustandsbasierte Prozesssteuerungssubsystem automatisch Zwischenprozess-E/A- oder Steuerungsänderungen ableiten, um mindestens einen Bereich des Prozesssteuerungssystems 245 von einem Zustand in einen anderen zu bringen. Die Zustände des SDCS 200 können gespeichert und wiederhergestellt werden, wobei die automatisch abgeleiteten Übergänge zwischen den Zuständen die Randbedingungen der Prozesssicherheit und der Prozessrentabilität berücksichtigen. Zur Veranschaulichung: In einem Beispielszenario kann, um den Zustand der Prozesseinheit A sicher in den bekannten Zustand B zu bringen, eine Reihe von Prozessanweisungen generiert werden (z.B. durch einen oder mehrere Anwendungsschichtdienste 235, die im zustandsbasierten Prozesssteuerungssystem beinhaltet sind), wobei die generierten Prozessanweisungen die Prozesssicherheitsbeschränkung einhalten, dass ein Brenner für eine Kesseleinheit weniger als 200 Grad Celsius haben muss. Da die Rentabilität aufrechterhalten werden kann, indem die Menge des Brennstoffverbrauchs pro Zeitspanne minimiert wird, um die Zustandsänderung zu beeinflussen, und indem die monetären Kosten, die mit der Meldung einer Umweltbelastung verbunden sind, minimiert werden, können die automatisch abgeleiteten Prozessanweisungen auch Rentabilitätsbeschränkungen einhalten, die die Änderung der Brennerleistung auf 1 Grad Celsius pro Sekunde begrenzen, um eine Umweltbelastung aufgrund eines plötzlichen Abfackelns zu verhindern und/oder einen fetten Betriebszustand des Brenners selbst zu vermeiden.

[0061] Zusätzlich kann das zustandsbasierte Prozesssteuerungs-Subsystem Anwendungsschichtdienste 235 bereitstellen, die unbekannte Zustände innerhalb der Prozessanlage erkennen und die unbekannten Zustände auflösen. Im Allgemeinen kann ein unbekannter Zustand einer Prozessanlage auftreten, wenn Prozessanlage E/A und Prozess-Tags sich in einem Zustand befinden, der um mehr als einen vordefinierten Betrag von einem bekannten Zustand abweicht. Zusätzlich oder alternativ können unbekannte Zustände der Prozessanlage auftreten, wenn die Prozess-E/A oder Prozessgeräte einen unlesbaren oder unbestimmten Status oder Wert haben, z.B. wenn ein Sensor den Status außerhalb des Bereiches hat oder der Sensor überhaupt nicht kommuniziert. Die von den zustandsbasierten Prozesssteuerungssubsystemen bereitgestellten Anwendungsschichtdienste können den letzten bekannten Prozesszustand verschiedener Bereiche und/oder Komponenten des Prozesssteuerungssystems 245 aufzeichnen und die letzten bekannten Zustände einem Nutzer zum Vergleich mit unbekannten Zuständen präsentieren. Das zustandsbasierte Prozesssteuerungssubsystem kann aber auch Anwendungsschichtdienste 235 beinhalten, die den Zustand einer Prozesseinheit schätzen, wenn ein darin beinhaltetes Prozessgerät nicht kommuniziert, aber noch betriebsbereit ist, d.h. wenn alle anderen Steuer- und E/A-Kennzeichenwerte außer denen, die mit dem nicht kommunizierenden Prozessgerät verbunden sind, mit einem bekannten Zustand übereinstimmen. Ein Beispiel für diese Situation ist ein Feldventil, das nicht mehr kommuniziert, dessen Ventilstellung sich jedoch gegenüber dem letzten bekannten Zustand der Prozesseinheit nicht verändert hat. Ein Anwendungsschichtdienst 235, der in das zustandsbasierte Prozesssteuerungs-Subsystem integriert ist, kann feststellen, dass die Position des Feldventils auf den zuvor gemeldeten, bekannten Zustand geschätzt werden kann, da alle anderen Prozess-E/A- und Sensor-Tags noch einen gültigen Prozesswert für einen bestimmten Zustand melden. Ein Zustandsvisualisierungstool kann Abweichungen zwischen den geschätzten Zuständen und den tatsächlichen Prozesswerten anzeigen, um einen Nutzer zu alarmieren, so dass z.B. Wartungsaufgaben eingeleitet werden sollten, um das System in einen bekannten, aufgezeichneten und nachweisbaren (z.B. nicht geschätzten) Zustand zu bringen.

[0062] Darüber hinaus kann das zustandsbasierte Prozesssteuerungssubsystem Anwendungsschichtdienste 235 bereitstellen, die einem Nutzer automatisch bei der Erstellung und Speicherung einer Zustandsdefinition helfen. Im Allgemeinen können Prozesszustände vom Nutzer definiert werden, indem er sich auf Zustandsübergangsdiagramme bezieht. Um den Nutzer bei der Erstellung von Zustandsdefinitionen zu unterstützen, können die

vom zustandsbasierten Prozesssteuerungssubsystem bereitgestellten Anwendungsschichtdienste 235 automatisch eine Zustandsdefinition erstellen, indem sie die aktuellen Werte eines laufenden Prozesses oder digitalen Zwillingssystems nehmen und diese Werte in Zustandsbereiche für einen bestimmten benannten Zustand verarbeiten, z.B. wie vom Nutzer definiert. Wenn der Anlageprozess beispielsweise heruntergefahren ist, kann ein Anwendungsschichtdienst 235, der vom zustandsbasierten Prozesssteuerungssubsystem bereitgestellt wird, eine Zustandsdefinition mit der Bezeichnung Shutdown State erstellen, indem er Zustandsbereiche auf der Grundlage der aktuell gelesenen Prozess-E/A- und Geräte-Tag-Werte erstellt. Auftretende Abweichungen (unabhängig davon, ob sie autonom erzeugt oder absichtlich eingefügt wurden) können aufgezeichnet werden und Zustandsbereiche können erstellt werden, um diese Abweichungen als Teil der Zustandsdefinition zu erfassen. Wenn beispielsweise während eines Zeitraums der Datenerfassung eine Pegelabweichung aufgrund von Vibrationen oder Temperatur von 10% auftritt, kann der automatische Zustandsdefinitionserstellungs-Anwendungsschichtdienst 235, der vom zustandsbasierten Prozesssteuerungs-Subsystem bereitgestellt wird, einen Bereich von +/- 10% für diesen Prozesswert erzeugen, um ihn als verifizierten Bereich der gegebenen Prozesszustandsdefinitionen zu definieren. Prozesszustandsdefinitionen können automatisch aus einem laufenden Prozess abgeleitet werden, indem aktuelle Prozesswerte verwendet werden, oder sie können auf der Grundlage bestimmter Zeitabschnitte für einen bestimmten Zustand abgeleitet werden, wie von einem umfassenden Prozesshistoriker angegeben.

[0063] In einem anderen Beispiel kann ein ereignisbasiertes Prozesssteuerungs-Subsystem eine Reihe von Anwendungsschicht-Steuerungsdiensten 235 beinhalten, die auf der Grundlage des Auftretens eines oder mehrerer Ereignisse zur Ausführung gebracht werden können. Ein ereignisbasierter Steuerungsmodul-Dienst kann zum Beispiel ausgeführt werden, wenn eine E/A-Bedingung einen bestimmten Wert oder Status erreicht. Die Ausführungsketten der Steuerungsmodul-Dienste können auch ereignisbasiert ausgelöst werden. Darüber hinaus können verschiedene Steuerungsmodul-Dienste und/oder Steuerungsmodul-Dienstketten so konfiguriert werden, dass sie ausgeführt werden, wenn ein Ereignis-Timeout eintritt, z.B. wenn die Steuerungslogik hauptsächlich ereignisgesteuert ist und das auslösende Ereignis nicht innerhalb eines bestimmten Zeitraums eintritt. In diesen Situationen kann der periodische Scheduler die Dienste des Steuerungsmoduls und/oder die Dienstketten des Steuerungsmoduls in Ausführungsformen ausführen, nachdem die Ereigniszeitüberschreitung stattgefunden hat. Andere Ereignisse innerhalb des SDCS 200 können die Ausführung verschiedener Steuerungsmodul-Dienste auslösen, wobei zu den anderen Ereignissen Diagnoseereignisse oder -bedingungen, Prozessdownloadänderungen oder andere SDCS-Ereignisse gehören können.

[0064] In einem weiteren Beispiel kann ein Steuerungssubsystem für Batch-Prozesse eine Reihe von Anwendungsschicht-Steuerungsdiensten 235 beinhalten, die die Batch-Steuerung und die Verfolgung von regulatorischen Elementen (z.B. für die behördliche Rückverfolgbarkeit) durchführen. Die vom Steuerungssubsystem für Batch-Prozesse bereitgestellten Anwendungsschicht-Steuerungsdienste 235 können z.B. das Einheitsverfahren, das Rezept, die Phase, die Phasenübergänge usw. beinhalten. Darüber hinaus können die Anwendungsschicht Steuerungsdienste 235, die vom Batch-Prozess Steuerungssubsystem bereitgestellt werden, regulatorische Aufzeichnungen verwalten, die sich auf die Batch-Prozesssteuerung beziehen und generiert werden.

[0065] Der Satz von SDCS-Subsystemen 238 kann ein Historiker-Subsystem beinhalten, das einen Satz von Anwendungsschichtdiensten 240 bereitstellt, um Zeitreihendaten für Prozess-E/A und Ereignisse innerhalb des Software-definierten Steuerungssystems 200 aufzuzeichnen. Beispielsweise können verschiedene Anwendungsschichtdienste 240, die vom Historiker-Subsystem bereitgestellt werden, Prozess-E/A- und/oder Ereignisdaten zu Aufzeichnungszwecken abonnieren. Andere Anwendungsschichtdienste 235, die vom Historiker-Subsystem bereitgestellt werden, können Quell-Zeitstempel-Dienste, Zeitkompressionsdienste (die z.B. einen konstanten Wert einmal aufzeichnen und eine Reihe von Malen entsprechend aktualisieren), traditionelle Zeitserien-Datenbankfunktionen und ähnliches beinhalten. Die aufgezeichneten historischen Daten können dupliziert und allen Knoten 208 innerhalb des SDCS 200 zur Verfügung gestellt werden. Darüber hinaus können historische Daten in Ausführungsformen nach Quell-Subsystem (z.B. dem Dienst oder Subsystem, das die historischen Daten erzeugt hat), Produktions-Asset, Produktions-Tag, SDCS-Datenpfad und/oder nach jeder anderen gewünschten Kategorie kategorisiert werden.

[0066] Zusätzlich oder alternativ kann der Satz von SDCS-Subsystemen 238 ein Edge-Connectivity-Subsystem beinhalten, das über einen entsprechenden Satz von Anwendungsschichtdiensten 240 einen Satz von Edge-Protokollen bereitstellen kann, die es ermöglichen, Prozesssteuerungsdaten an verschiedene Drittkomponenten außerhalb des Prozesssteuerungssystems zu senden und von diesen zu empfangen. Beispiele für solche Edge-Protokolle sind OPC-UA und MQTT, um nur einige zu nennen. Das Edge-Connectivity-Subsystem kann einen oder

mehrere Anwendungsschichtdienste 240 beinhalten, die eine Cloud-Konnektivität zum SDCS 200 bereitstellen, wobei Cloud-basierte Anwendungen verschiedene Funktionen wie die Überwachung der industriellen Prozessanlage für den Assetsstatus und den Asset-Zustand sowie andere Arten von Funktionalitäten unterstützen können. Zumindest einige der Anwendungsschichtdienste 240, die vom Edge-Connectivity-Subsystem bereitgestellt werden, können eine logische Darstellung des SDCS 200 und der entsprechenden Prozess-E/A-Daten als ein Datenmodell generieren, das für das verwendete Edge-Protokoll spezifisch ist. Solche Datenmodelle ermöglichen den gesicherten Zugriff Dritter auf ausgewählte Prozessdaten, wenn dies gewünscht wird.

[0067] In einigen Ausführungsformen beinhaltet der Satz von SDCS-Subsystemen 238 ein Diagnose-Subsystem, das einen Satz von Anwendungsschichtdiensten 240 zum Sammeln und Bereitstellen von Diagnosedaten von verschiedenen anderen SD-Anwendungsschichtdiensten 235, 240, 248, von verschiedenen anderen SD-Subsystemen 238, von Knoten 208 und von SD-Netzwerkschichtkomponenten 210 des SDCS 200 bereitstellen kann.

[0068] Der Satz von SDCS-Subsystemen 238 kann ein Prozess-E/A-Subsystem beinhalten, das einen Satz von Anwendungsschichtdiensten 240 zur Verwaltung von E/A-Verbindungen und Konfigurationen für Prozess-E/A innerhalb des Prozesssteuerungssystems 245 bereitstellt. Wie bereits erwähnt, kann das Prozess-E/A-Subsystem den E/A-Serverdienst 242 in Ausführungsformen bereitstellen.

[0069] Der Satz von SDCS-Subsystemen 238 kann ein Prozess-Nutzer-Subsystem beinhalten, das einen Satz von Anwendungsschichtdiensten 240 bereitstellt, um die Anmeldedaten der Nutzer zu verifizieren und/oder zu validieren, wenn diese sich beim SDCS 200 anmelden. Zusätzlich können die Dienste 240 des Subsystems Prozess-Nutzer anderen Diensten 235, 240, 248 Informationen über den Nutzer zur Verfügung stellen, z.B. zur Autorisierung. Die Daten der Nutzer können innerhalb des Datenzentrums-Clusters 208 repliziert werden, falls gewünscht.

[0070] Der Satz von SDCS-Subsystemen 238 kann auch ein Alarm-Subsystem beinhalten, das einen Satz von Anwendungsschichtdiensten 240 zur Verwaltung der Definitionen, Status und Zustände von Alarmen innerhalb des SDCS 200 bereitstellt. Alarme können zum Beispiel Prozessalarme, Hardwarealarme, Wartungsalarme, Gerätealarme, Netzwerkschichtalarme, E/A-Alarme, Hardware-Asset-Alarme, Software-Asset-Alarme, Diagnosealarme und ähnliches sein.

[0071] In einigen Implementierungen kann der Satz von SDCS-Subsystemen 238 ein Lizenzierungs-Subsystem beinhalten, das einen Satz von Anwendungsschichtdiensten 240 bereitstellt, um zu verifizieren oder sicherzustellen, dass ein Nutzer über Berechtigungen entsprechend der Lizenzstufe des SDCS 200 verfügt. Die Lizenzstufen können allen SDCS-Diensten 235, 240 und Subsystemen 238 zur Verfügung gestellt werden und können die Form von unbefristeten Lizenzen, Zeitabonnementlizenzen, verbrauchsbasierten Lizenzen, Fernlizenzen (z.B. Lizenzdaten aus der Cloud oder von einem dedizierten Lizenzserver) usw. annehmen. Die vom Lizenzierungssubsystem bereitgestellten Anwendungsschichtdienste 240, die Lizenzen durchsetzen, sind besonders wichtig, denn wenn Lizenzen für das SDCS 200 ablaufen oder ungültig werden, läuft auf dem SDCS 200 möglicherweise ein kritischer oder gesundheitsgefährdender Prozess ab. In solchen Situationen können die Dienste zur Durchsetzung von Lizenzen verhindern, dass nicht lizenzierte Aktivitäten stattfinden, und gleichzeitig sicherstellen, dass die Durchsetzung von Lizenzen nicht zu einer unsicheren Umgebung für den Nutzer führt. Wenn das SDCS 200 beispielsweise nicht mehr lizenziert ist, können in einer Ausführungsform alle dem Nutzer zugewandten Anwendungen, Bedienergrafiken und Arbeitsplätze mit einem Wasserzeichen oder einem halbtransparenten Bannertext überlagert werden, der anzeigt, dass das System nicht mehr lizenziert ist, und alle Dienste mit Ausnahme der von Steuersubsystemen bereitgestellten Dienste können jegliche Änderungen oder Modifikationen daran ablehnen. Auf diese Weise können einige lizenzierte Funktionen eingeschränkt oder deaktiviert werden, während gleichzeitig sichergestellt wird, dass die Prozessausführung nicht unkontrolliert oder gefährlich wird.

[0072] Um die Lizenzierung zu verwalten, kann das Lizenzierungssubsystem in einer Ausführungsform einen Anwendungsschichtdienst 240 beinhalten, der nur eine einzige primäre Administratorkonsolensitzung oder Nutzersitzung vorsieht, die den Betrieb der Anlage im Hinblick auf lizenzbasierte Einschränkungen kontrollieren darf; alle anderen Konsolen- und/oder Nutzersitzungen können daran gehindert werden, von Nutzern initiierte Änderungen vorzunehmen. Als solches kann das Lizenzierungssubsystem einen Anwendungsschichtdienst 240 bereitstellen, der einen Mechanismus zur Verfügung stellt, um zu bestimmen, dass nur eine Sitzung mit Administratorrechten (z.B. zu einem Zeitpunkt) in der Lage ist, Steuerungsoperationen in einem nicht lizenzierten Zustand auszuführen. Wenn z.B. eine aktive Administrator-Konsole oder -Sitzung ausfällt oder nicht mehr reagiert, kann das Lizenzierungssubsystem einer nachfolgenden aktiven Administrator-Sitzung erlauben, die Anlageoperationen zu steuern. Alle anderen Konsolensitzungen und Nutzersitzungen können daran gehindert werden, Änderungen am

Prozesssteuerungssystem vorzunehmen, bis die Lizenzierung wiederhergestellt ist.

[0073] In bestimmten Ausführungsformen kann das Subsystem für die Lizenzierung außerdem einen Anwendungsschichtdienst 240 bereitstellen, der so konfiguriert ist, dass er den Lizenzierungsstatus und/oder Aktivitäten aus der Ferne an ein Herstellersystem meldet, z.B. zur Durchsetzung und/oder für Rechtsbehelfe. In Konfigurationen, in denen der Hersteller keine Fernmeldung zur Verfügung stellt, kann das Subsystem für die Lizenzierung über einen oder mehrere Anwendungsschichtdienste 240 ein Protokoll aller lizenzbezogenen Ereignisse zum späteren Abruf führen.

[0074] Der Satz von SDCS-Subsystemen 238 kann ein verteiltes Ereignis-Subsystem beinhalten, das einen Satz von Anwendungsschichtdiensten 240 bereitstellt, um generierte Ereignisse (oder Benachrichtigungen darüber) über alle Knoten 208 des SDCS 200 zu verteilen, zusammen mit entsprechenden Zeitstempeln, die die jeweiligen Zeiten des Auftretens an den jeweiligen Ereignisquellen angeben. Auf diese Weise kann eine konsistente Aufzeichnung über alle Knoten 208 hinweg gewährleistet werden.

[0075] Zusätzlich kann jeder Knoten 208 des SDCS 200 eine Instanz eines Konfigurationssubsystems 238 beinhalten, wobei das Konfigurationssubsystem 238 in einer Konfigurationsdatenbasis, die vom Konfigurationssubsystem 238 bereitgestellt wird, die Konfigurationen der Steuerungsdienste (z.B. aller Steuerungsdienste 235) speichert, die vom SDCS 200 ausgeführt werden. Wenn also Steuerstrategien geändert und gespeichert werden (z.B. als jeweils aktualisierte Steuerungsdienste 235), kann das Konfigurationssubsystem über die jeweiligen Anwendungsschichtdienste 240 die zugehörigen Konfigurationen innerhalb der Konfigurationsdatenbasis entsprechend aktualisieren. Da in jedem Knoten 208 eine entsprechende Instanz der Konfigurationsdatenbasis gespeichert ist, bietet das SDCS 200 Fehlertoleranz für die Konfigurationsdatenbasis in allen Knoten des SDCS. So können Schreibvorgänge in die Datenbank (z.B. durch einen Schreibdienst für die Konfigurationsdatenbasis, der vom Konfigurationssubsystem bereitgestellt wird) über alle fehlertoleranten Instanzen des SDCS hinweg atomar erfolgen. Das bedeutet, dass eine Datenbankschreibtransaktion erst dann abgeschlossen ist, wenn alle fehlertoleranten Instanzen des Konfigurationssubsystems an allen Knoten 208 die Schreiboperation empfangen und verarbeitet haben. Atomare Schreibvorgänge können sich auf das Element oder die bestimmte Konfiguration beziehen, auf die zugegriffen wird. Wenn also auf eine Entität in der Datenbank geschrieben wird, können auch andere Entitäten in der Datenbank (z.B. zur gleichen oder überlappenden Zeit) in einer Multi-Thread-Methode beschrieben werden, da der Umfang des Synchronisierungssperrmechanismus auf jedes Element oder Objekt (Eintrag), auf das geschrieben wird, beschränkt sein kann. Darüber hinaus können Sperr- und Entsperrvorgänge in allen Instanzen der Konfigurationsdatenbasis atomar sein, so dass eine Objektsperre erst dann als erfolgreich angesehen wird, wenn alle Kopien dieses Objekts in allen Instanzen der Konfigurationsdatenbasis gesperrt sind. Außerdem kann das Konfigurationssubsystem einen oder mehrere Anwendungsschichtdienste 240 bereitstellen, um die Versionskontrolle der Konfigurationsdatenbasis zu verwalten. Die Versions-Steuerungsdienste können beispielsweise Änderungen an der Konfigurationsdatenbasis, den Zeitpunkt der Änderungen und die jeweiligen Parteien, die die Änderungen eingecheckt haben, verfolgen.

[0076] Das Lesen der Konfigurationsdatenbasis (z.B. durch einen Konfigurationsdatenbasis-Lesedienst, der vom Konfigurationssubsystem bereitgestellt wird) kann von einer einzigen lokalen Instanz der Konfigurationsdatenbasis erfolgen. In manchen Situationen kann eine Datenbankleseanforderung jedoch auf mehrere Knoten 208 verteilt werden, z.B. so dass eine große Leseanforderung segmentiert und die Ergebnisse parallel von den mehreren Knoten 208 bereitgestellt werden können.

[0077] Wie bereits erwähnt, kann der E/A-Serverdienst 242 des SDCS 200 in das Subsystem Prozess E/A oder in ein anderes Subsystem 238 eingebunden sein. Alternativ kann der E/A-Serverdienst 242 auch ein SDCS-Dienst 240 sein, der sich in einem eigenen, eigenständigen Subsystem befindet oder mit keinem Subsystem verbunden ist. In jedem Fall arbeitet der E/A-Serverdienst 242 im Allgemeinen als ein Dienst, der für die Übertragung von E/A-Daten (und in einigen Szenarien auch von anderen Datentypen) zwischen den Endpunkten des logischen Prozesssteuerungssystems 245 zuständig ist, z.B., von einem Feldgerät zu einem instanziierten Containerbild eines Anwendungsschichtdienstes 235, 240, 248 (wie z.B. einer Steuerung, einer Bedienerschnittstelle, einer Diagnose, einer Analyse, einem Historiker oder einem Dienst eines Drittanbieters); von einem instanziierten Containerbild eines Anwendungsschichtdienstes 235, 240, 248 zu einem Feldgerät, von einem instanziierten Containerbild eines Steuerungsdienstes 235 zu einem anderen instanziierten Containerbild eines anderen Typs eines SDCS-Dienstes 240 (z.B. einer Bedienerschnittstelle, einer Diagnose, einer Analyse, einem Historiker, einem Dienst eines Drittanbieters etc.) Beispielsweise kann der E/A-Serverdienst 242 die jeweiligen Endpunkte kommunikativ koppeln und Daten zwischen ihnen übertragen, indem er ein beliebiges geeignetes Paradigma für die Datenlieferung oder Datenübertragung verwendet, einschließlich Anfrage/Antwort, Publish/Subscribe usw.

[0078] Auf den E/A-Serverdienst 242 kann von anderen Anwendungssoftwarekomponenten 235, 238, 240, 248 zum Zwecke der Datenübertragung oder Datenlieferung zugegriffen werden, und der E/A-Serverdienst 242 kann die APIs 228 nutzen, um dadurch die E/A-Daten und/oder andere Arten der Datenübertragung zu veranlassen, z.B. über die SD HCI OS Support Dienste 215-225. In manchen Situationen kann der E/A-Serverdienst 242 die Übertragung von Daten über den Microdienst-Bus veranlassen. Der E/A-Serverdienst 242 dient als logisches oder API-Gateway, das die Weiterleitung von Prozess-E/A und/oder anderen Datentypen zwischen den Containern des SDCS 200 sowie die Weiterleitung von Prozess-E/A zwischen den Containern des SDCS 200 und den in der Feldumgebung 12 der industriellen Prozessanlage 10 eingesetzten Geräten bewirkt. Vorteilhafterweise kann der E/A-Serverdienst 242 automatisch die Fehlertoleranz und die Dienstgüte des Prozess-Steuerungsdienstes und der Subsystemcontainer verwalten, um die industriellen Prozessausgaben zu steuern, wie hier an anderer Stelle noch ausführlicher beschrieben wird.

[0079] Darüber hinaus können in der Anwendungsschicht 212 des SDCS 200 zumindest einige physische Prozesssteuerungseinrichtungen oder -komponenten (z.B. Steuerungen, Sicherheitslogik-Löser oder -Geräte, Datenspeichergeräte, Edge Gateways usw.) herkömmlicher Prozesssteuerungssysteme logisch im logischen Prozesssteuerungssystem 245 als ein entsprechender Dienst 235, 240 oder Subsystem 238 implementiert sein, der in einem entsprechenden Container ausgeführt wird. Solche logischen oder virtuellen Instanzen von Prozesssteuerungseinrichtungen oder -komponenten können auf Wunsch in ähnlicher Weise wie ihre physischen Gegenstücke konfiguriert werden, indem die logischen Geräte mit Steuerungsroutinen, anderen Anwendungsschichtsoftwarekomponenten 212, Parametern, Referenzwerten, Listen und/oder anderen Daten konfiguriert werden. Beispielsweise kann ein bestimmter logischer Edge-Gateway-Dienst mit Whitelists und mit einer Verbindung zu einem bestimmten logischen Datendiodendienst konfiguriert werden, ein Steuerungsdienst kann mit mehreren Steuerungsmodulen konfiguriert werden, usw. Konfigurierte logische oder virtuelle ProzessSteuerungseinrichtungen oder Komponenten (z.B. Container-Instanzen von ProzessSteuerungseinrichtungen oder Komponenten) können innerhalb des logischen Prozesssteuerungssystems 245 beispielsweise über ein entsprechendes Geräte-Tag oder eine Identifikation identifiziert werden, und entsprechende Signale, die von konfigurierten logischen oder virtuellen Instanzen von ProzessSteuerungseinrichtungen empfangen und erzeugt werden, können innerhalb des logischen Prozesssteuerungssystems 245 über entsprechende Geräte-Signal-Tags oder Identifikatoren identifiziert werden.

[0080] Darüber hinaus sieht das SDCS 200 Container in der SD-Anwendungsschicht 212 vor, die zur Darstellung und/oder logischen Organisation von physischen und/oder logischen Bereichen, Regionen und Komponenten der industriellen Prozessanlage 10 verwendet werden können. Beispielsweise können Einheiten, Bereiche und dergleichen durch entsprechende Container dargestellt werden, und Container, die den physischen und/oder logischen Komponenten jeder Einheit, jedes Bereichs usw. entsprechen, können in ihren jeweiligen Organisationscontainern verschachtelt und/oder an diese angeheftet werden. Zum Beispiel kann ein Container für den Bereich der fraktionierten Destillation der industriellen Prozessanlage 10 einen Container für die Depropanisierungseinheit und einen Container für die Debutanisierungseinheit beinhalten; d.h. der Container für die Depropanisierungseinheit und der Container für die Debutanisierungseinheit können in den Container für den Bereich der fraktionierten Destillation eingebettet oder an diesen angeheftet sein. Innerhalb des Containers der Depropanisierungseinheit kann ein Steuerungscontainer mit einem Steuerungsroutinen-Container konfiguriert sein, der so konfiguriert ist, dass er auf Durchflussmessungen von einem physischen Messfeldgerät arbeitet, das an einem Ausgangsanschluss des physischen Depropanisierers innerhalb der Feldumgebung 12 der Prozessanlage 10 angeordnet ist. Auf der Grundlage der empfangenen Durchflussmessungen kann die Steuerungsroutine, die in dem konfigurierten Steuerungsroutinencontainer ausgeführt wird, einen Steuerungsausgang erzeugen, den der Steuerungscontainer einem Aktor eines Ventils zur Verfügung stellt, das den Ausgangsanschluss des Depropanisierers bedient, wobei der physische Aktor und das physische Ventil ebenfalls in der Feldumgebung 12 der Anlage 10 angeordnet sind. Innerhalb des SDCS 200 kann der konfigurierte Steuerungsroutinen-Container in den Steuerungscontainer verschachtelt oder an diesen angeheftet werden, und der Steuerungscontainer kann in den Container der Depropanisierungseinheit verschachtelt oder an diesen angeheftet werden. Der Steuerungs-Routinedienst-Container kann mit dem Signal-Tag der vom Feldgerät empfangenen Durchflussmessung und mit dem Signal-Tag des Steuerungsausgangssignals, das an den Aktor geliefert wird, konfiguriert werden und, falls gewünscht, kann der Steuerungsdienst-Container zusätzlich mit den Geräte-Tags oder Identifikationen des physischen Messfeldgeräts und des physischen Aktors konfiguriert werden. Im Hinblick auf die Konfiguration der Steuerungsdienste 235 kann beispielsweise ein Container der Nutzer-Schnittstelle mit einem Container des Prozesssteuerungskonfigurationsdienstes kommunizieren oder diesen ausführen, über den ein Nutzer den Steuerungsdienst und den Steuerungs-Routinedienst so konfigurieren kann, dass sie die gewünschten Tags,

Kennungen, Werte und Steuerungsroutine(n) beinhalten.

[0081] In der SD Anwendungsschicht 212 beinhaltet das SDCS 200 auch Software-definierte Speichereinheiten oder -komponenten 213, die eine abstrahierte Datenspeicherung (und den Zugriff darauf) für die Dienste und Subsysteme 235-248 der SD Anwendungsschicht 212 bereitstellen. So können beispielsweise Historikerdatenbanken, Konfigurationsdatenbanken und andere Arten von Prozesssteuerungssystem-Datenbanken und Datenspeichereinheiten sowie temporäre Speicher, die von verschiedenen Prozesssteuerungs-Anwendungsdiensten 235-248 während der Ausführung genutzt werden, von den SD definierten Speichereinheiten 213 bereitgestellt werden. Die SD-Speicherdatenbanken, -bereiche, -geräte usw. können virtualisierte oder logische Speichereinheiten oder -komponenten sein, die verschiedenen Speicherressourcen des Knotens der Rechenplattform 208 durch das SD-HCI-Betriebssystem 210 zugewiesen oder zugeordnet werden können (und neu zugewiesen und neu zugeordnet werden können). Zum Beispiel kann eine einzige SD definierte logische Datenbank über die Hardware Speicher Ressourcen mehrerer Knoten 208 implementiert werden. Darüber hinaus kann der SD Speicherdienst 218 des SD HCI-Betriebssystems 210 SD-Speicherentitäten 213 in der SDCS Anwendungsschicht 212 auf der Grundlage der Leistungs-, Ressourcen- und Konfigurationsanforderungen der SD-Speicherentitäten oder -komponenten 213 und optional anderer Komponenten der SD-Anwendungsschicht 212 zuweisen/neu zuweisen und neu zuweisen/neu zuordnen.

[0082] Kehren wir nun zur Software-definierten Netzwerkschicht 210 des SDCS 200 zurück, so ist in **Fig. 2** ein bestimmter SD HCI OS Dienst, nämlich der SD Orchestratordienst 222, der Einfachheit halber getrennt von den Darstellungen der anderen SD HCI OS Dienste 215-220, 225 dargestellt. Im Allgemeinen instanziiert der SD Orchestratordienst 222 Containerbilder (z.B. von Anwendungsschicht-Steuerungsdienste 235, Subsystemen 238, Diensten von Drittanbietern 248 und anderen SDCS-Diensten 240) in laufende oder ausführende Container-Prozesse auf den jeweiligen physischen Hardware- und/oder Software-Rechen-Ressourcen 208 und weist verschiedene SD-Datenspeichereinheiten zu, die sich auf den jeweiligen Hardware- und/oder Software-Speicherressourcen 208 befinden. Beispielsweise kann der SD Orchestrator 222 verschiedene Containerbilder instanziieren und zuweisen, um sie auf verschiedenen spezifischen Hardware- und/oder Software-Rechenressourcen 208 auszuführen und/oder zu nutzen, die Ressourcen eines einzelnen Knotens oder von zwei oder mehr Knoten sein können. Darüber hinaus kann der SD Orchestrator 222 verschiedene SD-Datenspeichereinheiten oder -komponenten 213 zuweisen, die sich auf physischen Schicht-Speicherressourcen 208 eines einzelnen Knotens, mehrerer Knoten usw. befinden, z.B. zur Vereinfachung und Beschleunigung des Zugriffs durch residente Container, zu Redundanzzwecken, zum Ausgleich der Speichernutzung auf der physischen Plattform usw. Dabei richtet der SD Orchestratordienst 222 nicht nur die laufenden Containerprozesse ein, sondern verwaltet auch die Fehlertoleranz, den Lastausgleich, die Dienstgüte (QoS) und/oder andere Leistungsaspekte der laufenden Containerprozesse des SDCS 200, z. B. über QoS-Konfigurationsdienste 252, Fehlertoleranzdienste 255, Lastausgleichsdienste 258 und optional andere leistungsbezogene Dienste 260, die vom SD HCI OS 210 bereitgestellt werden. So kann der SD Orchestratordienst 222 von den anderen SD HCI OS-Diensten 215, 218, 220, 225 aufgerufen oder angesprochen werden, und der SD Orchestratordienst 222 kann seinerseits einen oder mehrere der leistungsbezogenen Dienste 252-260 aufrufen oder darauf zugreifen. Im Allgemeinen weist der SD Orchestratordienst 222 den Containern und SD-Datenspeichereinheiten des logischen Prozesssteuerungssystems 245 Ressourcen zu, so dass die Container in der Lage sind, effizient und sicher zu arbeiten, z.B. um den industriellen Prozess zu steuern, zumindest auf einem Best-Effort-Leistungsniveau.

[0083] Zu diesem Zweck können die leistungsbezogenen Dienste 252-260 des SD HCI OS 210 Leistungsparameter, Ressourcennutzung und/oder Kriterien während der Laufzeit überwachen, alle damit zusammenhängenden Bedingungen erkennen, die auftreten und/oder für die ein Auftreten vorhergesagt wird, und alle Änderungen in den Zuweisungen von SD Anwendungssoftwarekomponenten (z. B. Containern) 212 zu Hardware- und/oder Softwareressourcen der Rechenplattform 208 bereitstellen und/oder umsetzen. Dementsprechend passt der SD Orchestratordienst 222 während der Laufzeit der industriellen Prozessanlage 10 beim Auftreten und Erkennen verschiedener erwarteter und/oder unerwarteter Hardware- und/oder Softwarebedingungen die Zuweisung von Hardware- und/oder Software-Ressourcen verschiedener Knoten 208 zu instanziierten Containerbilder an, um ein Ziel- oder Best-Effort-Niveau an Leistung und Betriebstreue aufrechtzuerhalten (oder zu versuchen, dies zu erreichen). Zu den erkannten Bedingungen, die den SD Orchestrator 222 veranlassen können, Zuweisungen und/oder Zuordnungen zwischen Containern 212 und Knoten Ressourcen 208 zu ändern, gehören beispielsweise Hardwarefehler oder -ausfälle, Softwarefehler oder -ausfälle, Überlastung eines bestimmten Knotens, erhöhte oder verringerte Bandbreite verschiedener Netzwerkkomponenten, Hinzufügen oder Entfernen von Knoten und/oder Clustern von Knoten, Hardware- und/oder Software-Upgrades, Anheften und/o-

der Lösen von Containern, Diagnose-, Wartungs- und andere Routinen, die dazu führen können, dass Hardware- und/oder Software-Ressourcen vorübergehend nicht für die Laufzeitnutzung zur Verfügung stehen, usw. Mögliche Reaktions- und/oder Abhilfemaßnahmen, die der SD Orchestratordienst ergreifen kann, beinhalten beispielsweise die Neuzuweisung von Containern zur Ausführung unter Verwendung anderer Software- und/oder Hardware-Ressourcen (in manchen Fällen auf anderen Knoten), die Aktivierung und/oder Deaktivierung von Software- und/oder Hardware-Ressourcen, die Änderung der Prioritäten für den Zugriff verschiedener Container auf verschiedene Software- und/oder Hardware-Ressourcen usw. Eine detailliertere Beschreibung des SD Orchestratordienstes 222 findet sich an anderer Stelle in dieser Beschreibung.

[0084] Dementsprechend und allgemein gesprochen können die Dienste, Subsysteme und anderen Softwarekomponenten der SDCS-Anwendungsschicht 212 (z.B. 235, 238, 240) den Verarbeitungs-, Containerisierungs-, Netzwerk- und Speicherbedarf des logischen Prozesssteuerungssystems 245 sowohl auf der Ebene einzelner Container als auch auf aggregierter Ebene (z.B. auf der Ebene von Subsystemen, Einheiten, Bereichen und/oder des Prozesssteuerungssystems 245 als Ganzes) bestimmen, definieren oder festlegen. Über die APIs 228 (und in einigen Konfigurationen auch über die HCI-Adapterschicht 230 und die APIs 232) verwalten und managen das SD HCI OS 210, seine Unterstützungsdienste 215, 218, 220, 222, 225 und sein SD Orchestratordienst 222 die Hardware- und Software-Ressourcen des Knotens 208, um diese Anforderungen zu unterstützen. In einigen Ausführungsformen kann der SD Orchestrator 222 beispielsweise veranlassen, dass verschiedene Instanzen eines bestimmten Steuerungscontainers 235 oder eines bestimmten anderen SDCS-Dienstcontainers 240 auf verschiedenen Knoten 208 ausgeführt werden, z.B. für Fehlertoleranz, Dienstgüte und/oder andere Leistungskriterien des SDCS 200. Da sich die Anforderungen des logischen Prozesssteuerungssystems 245 im Laufe der Zeit dynamisch ändern, können die SD HCI OS Support Dienste 215, 218, 220, 222, 225 und/oder der SD Orchestrator 222 die Nutzung der Hardware- und Softwareressourcen des Knotens 208 modifizieren, ändern und anpassen, z.B. in einer reaktiven und/oder vorausschauenden Weise. Wenn beispielsweise das logische Prozesssteuerungssystem 245 zusätzliche Instanzen von Steuerungsdiensten 235 erstellt, die in zusätzlichen Containern ausgeführt werden, können die SD HCI OS Support Dienste 215-225 (über das APIS 228 und optional den HCI-Adapter 230 und die APIs 232) den neu erstellten Containern die Ausführung auf entsprechenden Knoten zuweisen, die vorhandenen Container auf die Knoten verteilen, bestimmte Hardware-Speicherressourcen zuweisen, um den logischen Speicherressourcenbedarf der zusätzlichen Container zu unterstützen, die von den Knoten 208 verwendeten Routing-Tabellen anpassen, um den logischen Routing-Bedarf der neu erstellten Container zu unterstützen, usw. Ein weiteres Beispiel: Wenn ein bestimmter Cluster C2 außer Betrieb genommen werden muss (z.B. erwartet zu Wartungszwecken oder unerwartet aufgrund eines Blitzeinschlags), können die SD HCI OS Support Dienste 215-225 Container, die momentan zur Ausführung auf dem Cluster C2 zugewiesen sind, entsprechend den aktuellen Anforderungen des logischen Prozesssteuerungssystems 245 und der Verfügbarkeit von Hardware- und/oder Softwareressourcen der anderen Cluster vorausschauend anderen Clustern zuweisen, und die SD HCI Support Dienste 215-225 können die von den Clustern 208 verwendeten Routing-Tabellen entsprechend anpassen, so dass die Kontinuität der Ausführung der Container aufrechterhalten wird, selbst wenn der Cluster C2 außer Betrieb genommen wird. Die SDCS-Netzwerkschicht 210 bestimmt, initiiert und führt automatisch, dynamisch und reaktionsschnell Änderungen an der Zuweisung von Hardware- und Softwareressourcen des Knotens der Rechenplattform 208 zu verschiedenen SD-Anwendungssoftwarekomponenten 212 auf der Grundlage erkannter Bedingungen durch, wie z. B. Verbesserung der Leistung einzelner logischer und/oder physischer Komponenten oder Gruppen davon, Verschlechterung der Leistung einzelner logischer und/oder physischer Komponenten oder Gruppen davon, Auftreten von Fehlern, Ausfälle logischer und/oder physischer Komponenten, Konfigurationsänderungen (z. B. aufgrund von Nutzerbefehlen oder aufgrund automatischer Neukonfiguration durch Dienste des SDCS 200) usw. Folglich muss ein Nutzer oder Systemadministrator mit dem SDCS 200 die Neuverteilung der Hardware- und Softwareressourcen des Knotens 208 zur Unterstützung des SDCS 200 oder von Änderungen daran nicht vorschreiben oder steuern. In den meisten Fällen wird der Nutzer oder Systemadministrator nichts von der Umverteilung der Hardware- und/oder Software-Ressourcen des Knotens 208 wissen, die automatisch von der SDCS 200 als Reaktion auf sich ändernde Bedingungen und Komponenten der SDCS 200 durchgeführt wird.

[0085] Während **Fig. 2** die Rechenplattform 208 zeigt, die das SDCS 200 unterstützt, kann die Rechenplattform 208 in einigen Konfigurationen mehrere SDCSs unterstützen. Die mehreren SDCS können sich Sätze von Hardware- und/oder Software-Ressourcen der Rechenplattform 208 teilen, oder die Hardware- und/oder Software-Ressourcen der Rechenplattform 208 können unter den mehreren SDCS aufgeteilt werden. In bestimmten Ausführungsformen, in denen die Hardware- und/oder Software-Ressourcen von mehreren SDCS gemeinsam genutzt werden, kann das SDC HCI-Betriebssystem

210 die gemeinsam genutzten Ressourcen unter den Anwendungsschichtdiensten der mehreren SDCS verwalten.

[0086] Darüber hinaus kann das SDCS 200 in einigen Implementierungen digitale Zwillinge verschiedener SD Anwendungsdienste 235, 240, 248, der gesamten SD Anwendungsschicht 212, verschiedener SD Unterstützungsdienste 215-225, 252-260 und/oder der gesamten SD Netzwerkschicht 210 implementieren. Das heißt, ein digitaler Zwilling der Zielkomponenten/Schichten kann zusammen mit den aktiven Zielkomponenten/Schichten auf der Rechenplattform 208 ausgeführt werden und dabei Laufzeitdaten aus der Feldumgebung der industriellen Prozessanlage empfangen und entsprechend mit der gleichen Logik, den gleichen Zuständen, dem gleichen Timing usw. arbeiten wie die aktiven Zielkomponenten/Schichten. Die vom digitalen Zwilling erzeugten E/A- und anderen Datentypen werden jedoch daran gehindert, an die Feldumgebung geliefert zu werden. Auf diese Weise kann bei einem Ausfall der aktiven Ziele/Komponenten der digitale Zwilling der abgelegten Ziele/Komponenten einfach aktiviert werden, um den Laufbetrieb der industriellen Prozessanlage nahtlos aufrechtzuerhalten.

[0087] Darüber hinaus kann das SDCS 200 in einigen Implementierungen Simulationen von oder Änderungen an verschiedenen SD Anwendungsdiensten 235, 240, 248, an der gesamten SD Anwendungsschicht 212, an verschiedenen SD Unterstützungsdiensten 215-225, 252-260 und/oder an der gesamten SD Netzwerkschicht 210 durchführen. Das heißt, eine Simulation der Zielkomponenten/-Schichten kann zusammen mit den aktiven SDCS-Komponenten/Schichten auf der Rechenplattform 208 ausgeführt werden und dabei Laufzeitdaten aus der Feldumgebung der industriellen Prozessanlage empfangen und entsprechend arbeiten, z.B. mit derselben Logik, denselben Zuständen, demselben Timing usw. wie die aktiven Zielkomponenten/-Schichten oder mit der simulierten Testlogik, den Zuständen, dem Timing usw. Die von der Simulation erzeugten E/A- und anderen Datentypen werden jedoch nicht an die Feldumgebung weitergeleitet, und die Simulationen können angehalten, beschleunigt, verlangsamt, mit Testeingaben versorgt und anderweitig verwaltet werden, um das Verhalten zu beobachten und Änderungen an den simulierten Komponenten/Schichten vorzunehmen. Dementsprechend kann nach der Freigabe eines simulierten Bereichs des SDCS 200 der simulierte Bereich einfach für die Verwendung während der Laufzeit der industriellen Prozessanlage aktiviert werden, ohne dass dafür eine Pause eingelegt oder ein Teil des SDCS 200 außer Betrieb genommen werden muss.

[0088] Es sei noch darauf hingewiesen, dass, obwohl die physische Schicht 208, die mit dem SDCS 200 verbunden ist, oben beschrieben wurde, dass sie durch die Verwendung eines physischen Datenzentrums-Clusters C1-Cx implementiert wird, in einigen Ausführungsformen zumindest ein Bereich der physischen Schicht 208 als virtualisierte physische Schicht 208 implementiert werden kann. Zum Beispiel kann der Datenzentrums-Cluster C 1 -Cx (oder eine Teilmenge davon) als virtuelle Maschinen implementiert werden, die z.B. in einem Cloud-Computing-System ausgeführt werden. Als solches kann die HCI-Adapterschicht 230 die SD-Anwendungsschicht, die SD-Speicherschicht und die SD-Netzwerkschicht 210 mit der virtualisierten physischen Schicht 208 verbinden.

[0089] Wie aus der obigen Beschreibung ersichtlich sein sollte und von Fachleuten geschätzt wird, können industrielle Prozesssteuerungssysteme wie die hier beschriebenen äußerst komplexe Systeme sein und sind es oft auch. Man kann Hunderte, Tausende oder sogar Zehntausende von diskreten, aber miteinander verbundenen Feldgeräten haben, die koordiniert arbeiten müssen, um den Prozess zu steuern. Die Komplexität, die durch die schiere Anzahl der Geräte entsteht, wird durch die Komplexität der Inbetriebnahme und Wartung des Systems multipliziert. Dazu gehören die Erstellung und Wartung von drahtgebundenen und drahtlosen Netzwerken, die alle Geräte miteinander verbinden, die Erstellung und Wartung der Steuerungsmodule, die die Feldgeräte auf der Grundlage von Messungen der Feldgeräte steuern, die Sicherstellung, dass genügend Ressourcen (Netzwerkbandbreite, Verarbeitungsleistung usw.) zur Verfügung stehen, um zu gewährleisten, dass die Designtoleranzen (Netzwerk-Latenz, synchronisierte Nachrichtenübermittlung usw.) des Systems kontinuierlich eingehalten werden, und dergleichen.

[0090] Die Implementierung von Containern in das beschriebene Software-definierte Steuerungssystem eignet sich in vielfältiger Weise für die effiziente Verwaltung und den Betrieb einer industriellen Prozesssteuerungsumgebung. Wie weiter unten beschrieben wird, erleichtert die Containerisierung eine intuitivere Organisation der Steuerressourcen, die die physische oder logische Organisation der Geräte in der Prozessanlage und die physische oder logische Organisation der Prozesse und Rechenressourcen, die die Geräte in der Prozessanlage steuern, nachahmen können. Die Implementierung von Containern bietet außerdem unzählige Möglichkeiten zur Aufrechterhaltung von Dienstgüteparametern sowie zur Schaffung und Aufrechterhaltung von Fehlerredundanz.

[0091] **Fig. 3** ist ein Blockdiagramm, das die Prinzipien der Fehlertoleranz und des Lastausgleichs veranschaulicht. In **Fig. 3** stellen zwei Rechenknoten 300 und 302 Rechen-, Speicher- und Netzwerkres-

sourcen für das SDCS bereit. Selbstverständlich kann jeder der beiden Rechenknoten 300 und 302 einen Rechenknoten oder mehrere Rechenknoten (nicht dargestellt) beinhalten, und jeder der Rechenknoten kann wiederum einen oder mehrere Prozessoren (nicht dargestellt) beinhalten, von denen jeder einen oder mehrere Prozessorkerne (nicht dargestellt) haben kann. Der Orchestrator 222 verwaltet die Instanziierung von verschiedenen Containern und die ihnen zugewiesenen Ressourcen entsprechend den Anforderungen des spezifischen Systems (z.B. entsprechend den Anforderungen bestimmter Container oder Prozesssteuerungsanlagen), in Ausführungsformen und/oder entsprechend den allgemeinen Anforderungen für Lastausgleich und Fehlertoleranz (z.B. wenn keine spezifischen Anforderungen für die Prozesssteuerungsanlage festgelegt wurden).

[0092] Im Detail ist der Container Orchestratordienst (d.h. der Orchestrator 222) für die Instanziierung von Containerbilder in laufende Container-Prozesse auf verfügbaren Rechenressourcen verantwortlich. Der Orchestrator 222 ist dafür verantwortlich, dass jeder der Container ordnungsgemäß eingerichtet wird und kümmert sich außerdem um die Fehlertoleranz und den Lastausgleich bei Containern. Fehlertoleranz wird durch einen horizontalen Skalierungsansatz geschaffen, bei dem mehrere Kopien eines Containers für einen Mechanismus mit mehreren Eingängen und einem Ausgang instanziiert werden. In einigen Ausführungsformen wählt der Orchestrator 222 einen „aktiven“ Container aus den mehrfachen, redundanten Kopien eines Containers aus. Wie hier verwendet, bezieht sich der Begriff „aktiv“ auf einen von mehreren redundanten Containern, der so ausgewählt ist, dass die Ausgänge des ausgewählten Containers die Eingänge eines anderen Containers steuern, ein Feldgerät steuern oder ähnliches. Wenn zum Beispiel mehrere redundante Kopien eines Containers des verteilten Alarmsubsystems instanziiert sind, kann der Orchestrator 222 auswählen, welcher der redundanten Container der aktive Container ist. Ein weiteres Beispiel: Wenn mehrere redundante Kopien eines E/A-Server-Containers instanziiert sind, kann der Orchestrator 222 auswählen, welcher E/A-Server-Container der aktive Container ist. In diesem Fall kann jeder der redundanten E/A-Server-Container Prozessdaten von den Feldgeräten in der Prozessanlage und Ausgänge von einem oder mehreren Steuerungscontainern empfangen, aber nur die Ausgänge des aktiven E/A-Server-Containers werden über die physische E/A-Schicht an die Feldgeräte in der Prozessanlage übertragen, und jeder der Steuerungscontainer empfängt Prozessdaten nur von dem aktiven E/A-Server-Container.

[0093] Die Kommunikation zwischen den fehlertoleranten Kopien der Dienstcontainer ist möglich (und in einigen Fällen notwendig), um Zustandsinformationen zu übertragen und zu etablieren. Der Orchestrator 222 ist dafür verantwortlich, eine Liste der spezifischen Dienst-Container in einem fehlertoleranten Einsatz zu führen, wobei die Reihenfolge der Liste den nächsten verfügbaren Container angibt, der die Aufgabe übernimmt (der aktive Container steht ganz oben auf der Liste). Diese Liste wird ständig aktualisiert, wenn sich die Bedingungen im Rechenzentrum ändern. Bei der aktiven Benachrichtigung, dass ein aktiver Dienst-Container außer Betrieb geht, kann der Orchestrator 222 eine schnelle Entscheidung über die nächste verfügbare fehlertolerante Kopie treffen, die die Aufgabe übernimmt. Wenn ein aktiver Container ungeplant außer Betrieb geht (z.B. aufgrund eines Energieausfalls), kann der Container-Orchestrator über eine Zeitverzögerung verfügen, um zu erkennen, wann ein solcher „harter“ Ausfall stattgefunden hat, und den nächsten verfügbaren Dienst-Container aktivieren. Wenn mehrere aktive Zustände festgestellt werden, erhält der Empfänger der Dienstausgaben für einen kurzen Zeitraum die mehreren Ausgänge. Der empfangende Dienst informiert den Orchestrator 222 über die doppelten Ausgänge, woraufhin der Orchestrator 222 den alten aktiven Container rekonfiguriert (oder zerstört und neu erstellt, falls die Rekonfiguration fehlschlägt) und ihn als nicht aktiven Container instanziiert. Während dieser Zeit wird der empfangende Container auf die letzte bekannte gute Informationsquelle zurückgreifen, bis die doppelte Informationsquelle beseitigt ist.

[0094] Während in einigen Instanzen der Orchestrator 222 für die Auswahl aktiver Container verantwortlich ist, können unter bestimmten Umständen, wie z.B. im Fall eines E/A-Server-Containers, die Container selbst einen aktiven Container auswählen, und zwar auf der Grundlage verschiedener Parameter, wie unten in Bezug auf E/A-Server-Container beschrieben.

[0095] Wie hier verwendet, bezieht sich der Begriff „Lastausgleich“ auf die Verwendung von Rechen-, Speicher- und/oder Kommunikationsressourcen für Prozesse (z.B. Container), die auf einem System laufen, so dass die Prozessorkerne, Prozessoren, Rechenknoten und/oder Server die gewünschten Dienstqualitätsmessungen erfüllen. Lastausgleich bedeutet also, dass die Nutzung von Rechen-, Speicher- und/oder Kommunikationsressourcen in einigen Instanzen ausgeglichen wird und in einigen Instanzen sichergestellt wird, dass minimale QoS-Parameter erfüllt werden (d.h., dass die maximale Netzwerklatenz für bestimmte Signale einen programmierten Wert nicht überschreitet, dass die maximale Verarbeitungslatenz für bestimmte Prozesse einen programmierten Wert nicht überschreitet, dass die Gesamtlatenz für einen bestimmten Wert einen programmierten Wert nicht überschreitet,

dass genügend Speicherressourcen für bestimmte Prozesse vorhanden sind, usw.).

[0096] Lastausgleichsparameter, wie z.B. maximale Netzwerklatenz, maximale Rechenlatenz und ähnliches, können als Parameter eines oder mehrerer Container in Ausführungsformen und/oder als Parameter bestimmter Dienste, die in den Containern ausgeführt werden, und/oder als Parameter bestimmter Werte, die von den in den Containern ausgeführten Diensten empfangen oder gesendet werden, programmiert werden. Die Parameter für den Lastausgleich können auch auf Systemebene festgelegt werden, entweder als globale Parameter oder als Standardparameter, die durch Parameter ersetzt werden können, die in bestimmten Containern oder Diensten festgelegt werden. Die QoS-Konfigurationsdienste 252 des Orchestrators 222 können eine Schnittstelle bereitstellen, um die Konfiguration von QoS-Parametern auf globaler, Standard-, Container- und/oder Dienstebene zu erleichtern. Die QoS-Konfigurationsdienste 252 können auch die in den verschiedenen Containern und/oder Diensten programmierten QoS-Parameter lesen, um sicherzustellen, dass die Parameter vom Orchestrator 222 implementiert und gepflegt werden.

[0097] Die Fehlertoleranzdienste 255, die innerhalb des Orchestrator 222 arbeiten, halten die Fehlertoleranz innerhalb des SDCS in Ausführungsformen aufrecht. Wie hier verwendet, bezieht sich der Begriff „Fehlertoleranz“ auf die Erstellung redundanter Prozesse und/oder Dienste (z.B. durch die Erstellung mehrerer Container), unabhängig davon, ob diese auf verschiedenen Prozessorkernen, verschiedenen Prozessoren oder verschiedenen Rechenknoten/-Servern instanziiert werden, und schließt Ausführungsformen ein, bei denen der Orchestrator 222 (d.h. über die Fehlertoleranzdienste 255) sicherstellt, dass ein oder mehrere redundante Container auf Rechenressourcen instanziiert werden, die von separaten Energieversorgungen gespeist werden, um sicherzustellen, dass der Ausfall einer Energiequelle nicht alle Betriebskopien eines bestimmten Containers beeinträchtigt. In bestimmten Ausführungsformen kann der Orchestrator 222 selbst als redundante Komponente instanziiert werden, um sicherzustellen, dass die Fehlertoleranz auch dann bestehen bleibt, wenn eine aktive Instanz des Orchestrators 222 durch einen Prozessorausfall, einen Energieausfall usw. abnormal beendet wird.

[0098] In **Fig. 3** sind mehrere logische Funktionen dargestellt, die auf den beiden Servern 300 und 302 implementiert sind. Die logischen Funktionen beinhalten eine erste Steuerung 304 (d.h. eine Steuerung, die einen ersten Satz von Geräten eines ersten Bereichs einer zugehörigen Prozessanlage steuert), eine zweite Steuerung 306 (d.h. eine Steuerung, die einen zweiten Satz von Geräten eines zweiten Bereichs der zugehörigen Prozessanlage steuert), einen E/A-Server 308 und einen Historiker 310. Jede der logischen Funktionen 304-310 wird durch einen zugehörigen Dienst implementiert, der in einem oder mehreren entsprechenden Containern ausgeführt wird. Der Einfachheit halber werden diese Dienste, die innerhalb von Containern ausgeführt werden, hier einfach als „Container“ bezeichnet. Es sollte jedoch klar sein, dass jeder „Container“ in **Fig. 3** einen zugehörigen Dienst ausführt, der so konfiguriert ist, dass er in Bezug auf andere Container, Dienste und/oder Prozesssteuerungs-Feldgeräte arbeitet. Zum Beispiel wird in jedem Steuerungscontainer ein Steuerungsdienst ausgeführt, die so programmiert ist, dass sie den zugehörigen Satz von Geräten steuert. In einigen Ausführungsformen kann der Steuerungsdienst mit einem oder mehreren Steuerungsmodul-Diensten programmiert sein, und jeder Steuerungsmodul-Dienst kann mit einem oder mehreren Steuerungsfunktionsblock-Diensten programmiert sein, wobei jeder der Steuerungsmodul-Dienste und jeder der Steuerungsfunktionsblock-Dienste in einem jeweiligen Container ausgeführt werden kann.

[0099] **Fig. 3** zeigt, dass die logische Steuerung 304 drei Steuerungscontainer 304A, 304B und 304C beinhaltet. Jeder der Steuerungscontainer 304A-304C ist auf einer anderen Rechenressource (d.h. Prozessorkern, Prozessor, Rechenknoten oder Server) instanziiert als mindestens einer der anderen Steuerungscontainer 304A-304C. Das heißt, der Steuerungscontainer 304A ist auf einem anderen Server (Server 300) instanziiert als die anderen Steuerungscontainer 304B und 304C (instanziiert auf dem Server 302); Steuerungscontainer 304B ist auf einem anderen Server (302) instanziiert als der Steuerungscontainer 304A (instanziiert auf dem Server 300) und auf einem anderen Prozessor oder Prozessor-Kern als der Steuerungscontainer 304C; und der Steuerungscontainer 304C ist auf einem anderen Server (302) instanziiert als der Steuerungscontainer 304A (instanziiert auf dem Server 300) und auf einem anderen Prozessor oder Prozessorkern als der Steuerungscontainer 304B. **Fig. 3** zeigt auch drei Steuerungscontainer 306A, 306B und 306C, die auf ähnliche Weise auf den Servern 300 und 302 instanziiert sind, zwei E/A-Servercontainer 308A und 308B, die auf den Servern 300 bzw. 302 instanziiert sind, und zwei Historikercontainer 310A und 310B, die auf den Servern 300 bzw. 302 instanziiert sind.

[0100] In Bezug auf die logische Steuerung 304 sollte es offensichtlich sein, dass nur einer der Steuerungscontainer 304A-304C zu einem gegebenen Zeitpunkt aktiv sein kann (d.h. Steuerungsausgänge für die gesteuerten Geräte bereitstellt), indem die Steuerungscontainer 304A-304C auf unterschiedlicher Computerhardware instanziiert

werden, so dass ein Fehler in einem der Steuerungscontainer 304A-304C nicht zu einem Steuerungsverlust der von der logischen Steuerung 304 gesteuerten Geräte führt. Tritt der Fehler an der aktiven der Steuerungen 304A-304C auf, würde eine der beiden verbleibenden Steuerungen zur aktiven Steuerung werden. Da alle drei Steuerungscontainer 304A-304C denselben Steuerungsalgorithmus implementieren und alle von der aktiven Steuerung empfangenen Daten empfangen, sind die von jedem der Steuerungscontainer 304A-304C gelieferten Ausgänge identisch und eine neue aktive Steuerung kann aus den Steuerungen 304A-304C ausgewählt werden, wenn die aktive Steuerung einen Fehler aufweist. Wenn der Fehler an der aktiven Steuerung durch einen Ausfall der Energieversorgung auf dem Server verursacht wird, auf dem der Steuerungscontainer instanziiert ist, kann außerdem mindestens eine andere Instanz des Steuerungscontainers verfügbar sein, um als aktiver Steuerungscontainer zu fungieren, wenn mindestens einer der Steuerungscontainer 304A-304C auf einer Rechenressource instanziiert ist, die eine andere Energieversorgung verwendet.

[0101] In bestimmten Ausführungsformen kann der Orchestrator 222 die QoS-Metriken der verschiedenen instanziierten Container überwachen. Zu den QoS-Metriken können beispielsweise Prozessorauslastung, Output-Latenz, Netzwerk-Latenz und Netzwerkbandbreite gehören. Wenn die QoS-Metriken darauf hindeuten, dass einer der Container oder der in dem Container ausgeführte Dienst instabil wird, oder wenn die QoS-Metriken darauf hindeuten, dass einer der Container nicht innerhalb der für den Container oder den Dienst spezifizierten Anforderungen arbeitet, kann der Orchestrator 222 eine weitere Instanz des Containers instanziieren und die instabile Container-Instanz beenden und dabei das gleiche Maß an Redundanz aufrechterhalten, während er einen schlecht arbeitenden Container durch einen gut arbeitenden Container ersetzt. Der neu instanziierte Container kann in Ausführungsformen auf einer anderen Hardware (anderer Prozessor, anderer Server usw.) instanziiert werden als der Container mit schlechter Leistung, je nachdem, ob die QoS-Metriken darauf hindeuten, dass der Container aufgrund der Hardware, auf der er instanziiert wurde, eine schlechte Leistung aufweist. Wenn die QoS-Metriken darauf hinweisen, dass eine Hardware-Ressource nicht ausgelastet ist, während eine andere Hardware-Ressource stark ausgelastet ist, kann der Lastausgleichsdienst 258 den Orchestrator 222 veranlassen, einen oder mehrere Container von der stark ausgelasteten Ressource auf die nicht ausgelastete Ressource zu verschieben (d.h. einen neuen Container auf der nicht ausgelasteten Ressource zu erstellen und den Container auf der stark ausgelasteten Ressource zu beenden).

[0102] Wie in **Fig. 3** dargestellt, hat der Orchestrator 222 die vier logischen Funktionen 304-310 auf den beiden Servern 300 und 302 instanziiert. Wie bereits beschrieben, befindet sich eine Instanz des Containers 304A der Steuerung #1 auf dem ersten Server 300, während sich zwei Instanzen der Container 304B und 304C der Steuerung #1 auf dem zweiten Server 302 befinden. Gleichzeitig hat der Orchestrator 222 die Belastung der beiden Server „ausgeglichen“, indem er zwei von drei Containern der Steuerung #2 (306A und 306B) auf dem ersten Server 300 instanziiert hat und nur einen der Container der Steuerung #2 (306C) auf dem zweiten Server 302. Zwei Container 308A und 308B führen den E/A Serverdienst auf dem ersten Server 300 bzw. dem zweiten Server 302 aus. In ähnlicher Weise führen zwei Container 310A und 310B den Historikerdienst auf dem ersten Server 300 bzw. dem zweiten Server 302 aus.

[0103] **Fig. 4A** veranschaulicht das Konzept des Lastausgleichs. In **Fig. 4A** sind fünf Container 312, 314, 316, 318, 320 auf drei Rechenknoten 322, 324, 326 instanziiert. Jeder der in **Fig. 4A** dargestellten Container 312, 314, 316, 318, 320 führt einen anderen Dienst aus. Obwohl in **Fig. 4A** keine redundanten Container dargestellt sind, kann eine solche Redundanz in jeder beschriebenen Ausführungsform vorhanden sein, auch wenn sie nicht dargestellt ist, um die Abbildung(en) für das beschriebene Konzept zu vereinfachen. **Fig. 4A** zeigt einen Steuerungscontainer 312 und einen kontinuierlichen Steuerungssubsystem-Container 314, die auf dem ersten Rechenknoten 322 instanziiert sind, einen verteilten Alarm-Subsystem-Container 316 und einen E/A-Server-Container 318, die auf dem zweiten Rechenknoten 324 instanziiert sind, und einen Safety Instrumented System (SIS) Steuerungscontainer 320, der auf dem dritten Rechenknoten 326 instanziiert ist.

[0104] **Fig. 4A** zeigt, dass der Container des verteilten Alarmsubsystems 316 vom zweiten Rechenknoten 324 zum ersten Rechenknoten 322 „verschoben“ werden kann, wenn der zweite Rechenknoten 324 stark belastet wird (z.B. für den Fall, dass der E/A-Server-Container 318 einen erheblichen Teil der Ressourcen des zweiten Rechenknotens 324 verbraucht), so dass die QoS-Metriken für den E/A-Server-Container 318 nicht aufrechterhalten werden, so dass die QoS-Metriken für den Container des verteilten Alarmsubsystems 316 nicht aufrechterhalten werden, oder so dass eine Mindestmenge an verfügbaren Ressourcen auf dem zweiten Rechenknoten 324 nicht aufrechterhalten wird, zum Beispiel. In einem solchen Fall kann der Orchestrator 222 eine zweite Instanz 316' des Containers 316 auf einem anderen Rechenknoten instanziieren (z.B. auf dem ersten Rechenknoten 322, wie in **Fig. 4A** dargestellt), der über ausreichende Ressourcen verfügt. Sobald das neu instanziierte verteilte Alarmsubsys-

tem 316' stabil ist, kann der Orchestrator 222 den Container 316' zum aktiven Container machen und den Container des verteilten Alarmsubsystems 316, der auf dem zweiten Rechenknoten 324 instanziiert wurde, beenden, wodurch Ressourcen auf dem zweiten Rechenknoten 324 frei werden.

[0105] Es sollte auch beachtet werden, dass nicht aktive Instanzen von redundanten Containern zwar nicht die Ausgänge des Dienstes steuern (z.B. können nicht aktive Steuerungscontainer den Prozess nicht steuern), redundante Container aber dennoch Daten an Bereiche des Systems liefern können, vorausgesetzt, die von jedem der redundanten Container empfangenen Daten sind gleichwertig. Während beispielsweise ein aktiver Steuerungscontainer den Prozess steuert, indem er Steuersignale an die in der Prozessanlage betriebenen Prozesssteuerungs-Feldgeräte liefert, können einer oder mehrere der redundanten Steuerungscontainer Daten an andere Dienste innerhalb des SDCS liefern, z.B. an einen Historikerdienst. Auf diese Weise kann die Leistungsbelastung des Systems auf mehrere der redundanten Container verteilt werden, insbesondere wenn diese redundanten Container auf mehrere Hardware-Ressourcen verteilt sind.

[0106] Das SDCS 100 kann auch so konfiguriert werden, dass es „Prioritäts“-Container (hier auch als „Hochprioritäts“-Container bezeichnet) beinhaltet. Prioritätscontainer sind Container, die Dienste mit hoher Priorität ausführen. Man kann vom Konfigurationstechniker bei der Konfiguration des SDCS oder standardmäßig für bestimmte Dienste bestimmt werden. Beispielsweise können Containerdienste, die als sicherheitsrelevant eingestuft sind (wie SIS-Steuerungen), allgemein als Prioritätscontainer ausgewiesen werden. Im Hinblick auf den Lastausgleich können prioritären Containern Rechenressourcen (z.B. Prozessor-Ressourcen, Netzwerkbandbreite, Speicher, Speicherplatz usw.) garantiert werden.

[0107] Daher kann der Orchestrator 222 einen Lastausgleich durchführen, um die garantierten Ressourcen für prioritäre Container aufrechtzuerhalten. In **Fig. 4A** ist der SIS-Steuerungscontainer 320 als Instanz auf dem dritten Rechenknoten 326 dargestellt (der dicke Containerrand zeigt in der Abbildung an, dass der Container ein Prioritätscontainer ist). In bestimmten Ausführungsformen kann ein Prioritätscontainer standardmäßig auf einem ansonsten unbelasteten Rechenknoten (wie in **Fig. 4A** dargestellt), auf einem ansonsten unbelasteten Prozessorkern usw. arbeiten, um sicherzustellen, dass garantierte Ressourcen verfügbar sind. Es ist jedoch nicht erforderlich, dass sich die Prioritätscontainer auf Servern, Prozessoren oder anderen Hardwarekomponenten befinden, auf denen nicht auch andere Container (mit oder ohne Priorität) instanziiert sind, solange die garantierten Ressourcen dem/den Prioritätscontainer(n) bereitgestellt werden.

[0108] Die garantierten Ressourcen können nach Containertyp (z.B. hierarchische Container, Steuerungscontainer, E/A-Server-Container), nach Diensttyp (z.B. E/A-Server, Steuerung, Subsystem, SIS-Steuerung) oder nach einzelnen Containern (z.B. Steuerung #1, die einen bestimmten Bereich der Prozessanlage steuert) festgelegt werden. Unabhängig von der Ebene, auf der Prioritätscontainer spezifiziert werden, kann die Spezifikation eines Prioritätscontainers die Angabe der Arten und Mengen der für einen solchen Container reservierten Ressourcen beinhalten. Beispielsweise kann einem Prioritätscontainer eine bestimmte Prozessorleistung, eine Mindestmenge an Systemspeicher, eine Mindestmenge an Netzwerkbandbreite, eine Mindestmenge an Speicher und/oder eine maximale Übertragungslatenz garantiert werden.

[0109] **Fig. 4B** veranschaulicht die Konzepte von Prioritätscontainern und veranschaulicht auch eine zusätzliche Fähigkeit der Lastausgleichsdienste 258 des Orchestrator 222. Insbesondere veranschaulicht **Fig. 4B**, dass der Orchestrator 222 in Ausführungsformen einen oder mehrere Rechenknoten, Prozessoren und/oder Prozessorkerne zum Cluster hinzufügen und/oder aus ihm entfernen kann. **Fig. 4B** zeigt einen ersten Rechenknoten 328, auf dem sich jeweils ein Steuerungscontainer 330, ein kontinuierlicher Steuerungssubsystem-Container 332 und ein verteilter Alarmsubsystem-Container 334 befinden. Auf einem zweiten Rechenknoten 336 sind ein Prioritäts-SIS-Container 338 und ein E/A-Server-Container 340 instanziiert. In dem in **Fig. 4B** dargestellten System benötigt der E/A-Server-Container 340 Ressourcen des zweiten Rechenknotens 336, die in die dem Prioritätscontainer 338 garantierten Ressourcen eingreifen, so dass der Lastausgleichsdienst 258 des Orchestrators 222 Ressourcen für den Prioritätscontainer 338 freigibt. In dem dargestellten Beispiel gibt der Orchestrator 222 die Ressourcen frei, indem er einen neuen Rechenknoten (d.h. einen dritten Rechenknoten) 342 zum Cluster hinzufügt und einen doppelten Container 340' des E/A-Server-Containers 340 auf dem neuen Rechenknoten 342 instanziiert. Sobald der neu instanziierte E/A-Server-Container 340' stabil ist, kann der Orchestrator 222 den Container 340' zum aktiven E/A-Server-Container machen und den E/A-Server-Container 340, der auf dem zweiten Rechenknoten 336 instanziiert wurde, beenden, wodurch die Ressourcen auf dem zweiten Rechenknoten 336 frei werden, um die garantierten Ressourcen für den Prioritätscontainer 338 zu erfüllen.

[0110] Ein Beispiel für die Implementierung von Fehlertoleranz ist in **Fig. 5A** dargestellt. In **Fig. 5A** sind auf dem ersten und zweiten Rechenknoten 344

und 346 jeweils ein Steuerungscontainer 350A, 350B, ein kontinuierliches Steuerungssubsystem Container 352A, 352B, ein verteiltes-Alarmsubsystem Container 354A, 354B und ein E/A Server Container 356A, 356B instanziiert. Ein dritter Server 348 steht im Leerlauf. **Fig. 5A** zeigt, dass der Steuerungscontainer 350A instabil wird oder plötzlich ausfällt (gekennzeichnet durch den differenzierten Umriss). Der Orchestrator 222, der erkennt, dass der Container 350A instabil ist oder beendet wurde, stellt sicher, dass der verbleibende Steuerungscontainer 350B der aktive Steuerungscontainer ist, und instanziiert eine weitere redundante Kopie des Steuerungscontainers 350C auf dem dritten Rechenknoten 348, um die Redundanz aufrecht zu erhalten.

[0111] Ein ähnlicher Prozess findet statt, wenn z.B. ein ganzer Rechenknoten funktionsunfähig wird (z.B. durch einen Energieausfall). **Fig. 5B** illustriert einen solchen Fall. In **Fig. 5B** sind auf dem ersten und zweiten Rechenknoten 358 und 360 jeweils ein Steuerungscontainer 364A, 364B, ein kontinuierliches Steuerungssubsystem Container 366A, 366B, ein verteiltes-Alarmsubsystem Container 368A, 368B und ein E/A Server Container 370A, 370B instanziiert. Ein dritter Server 362 steht im Leerlauf. **Fig. 5B** zeigt, dass der erste Rechenknoten 358 nicht mehr verfügbar ist oder jedenfalls alle Container 364A, 366A, 368A, 370A plötzlich ausfallen (gekennzeichnet durch die differenzierten Umrisse). Der Orchestrator 222, der erkennt, dass der erste Rechenknoten 358 nicht mehr verfügbar ist, stellt sicher, dass die Container 364B, 366B, 368B, 370B die aktiven Container sind, und sorgt für die Aufrechterhaltung der Redundanz, indem er weitere redundante Kopien der Container 364C, 366C, 368C, 370C auf dem dritten Rechenknoten 362 instanziiert.

[0112] In bestimmten Ausführungsformen unterhält der Orchestrator 222 eine Liste, eine Tabelle, eine Datenbank oder eine andere Datenstruktur, in der alle instanziierten Dienste und Container, die im Rechenzentrum 208 (oder in jedem Fall in dem Bereich des Rechenzentrums 208, der in den Zuständigkeitsbereich des Orchestrators 222 fällt) instanziiert wurden, verzeichnet sind, oder greift darauf zu. Die Informationen in der Datenstruktur können zum Beispiel von einem Dienst (z.B. den leistungsbezogenen Diensten 260), der im Orchestrator 222 ausgeführt wird, von einem Dienst (z.B. den Software-definierten Diensten und Funktionen 225, die im HCI-Betriebssystem 210 ausgeführt werden), von den Software-definierten Rechendiensten 215, von den Software-definierten Speicherdiensten 218 und/oder von den Software-definierten Netzwerkdiensten 220 gefüllt werden. **Fig. 6** zeigt in einer Tabelle 372 die Art der Informationen, die der Orchestrator 222 in der Datenstruktur verwaltet oder auf die er zugreift. Im Allgemeinen beinhaltet die Datenstruktur eine Liste aller im Rechenzentrum instanziierten Container und Dienste (Spalte 373), die Angabe, ob es sich um einen aktiven Container oder Dienst handelt (Spalte 374), sowie verschiedene Informationen und Metriken 376 zu den einzelnen Containern oder Diensten. Beispielhaft können die Informationen und Metriken 376 eines oder mehrere der folgenden Elemente beinhalten: eine Angabe 377 darüber, welche einer Vielzahl von Energieversorgungen Energie an die Ressourcen liefert, auf denen jeder Container oder Dienst instanziiert ist; eine Angabe 378 darüber, auf welchem einer Vielzahl von Knoten der Container oder Dienst instanziiert ist; eine Angabe 379 über das Laden des Knotens; eine Angabe 380 darüber, auf welchem einer Vielzahl von Prozessoren der Container oder Dienst instanziiert ist; eine Angabe 381 über das Laden des Prozessors; eine Angabe 382 darüber, auf welchem einer Vielzahl von Prozessorkernen der Container oder Dienst instanziiert ist, und eine Angabe 383 über das Laden des Prozessorkerns.

[0113] Der Orchestrator 222 kann auch eine Datenstruktur pflegen oder darauf zugreifen, die Informationen auf einer höheren Ebene als der Container- und Dienstebene verfolgt. Beispielsweise kann der Orchestrator 222 auf Statistiken über die Menge an Rechenressourcen, Speicherressourcen und/oder Netzwerkressourcen, die auf und/oder für jeden Cluster, Knoten, Server, Prozessor und/oder Prozessorkern verfügbar sind, Statistiken über die Stabilität verschiedener Energieversorgungen (z.B. Spannungsstabilität, Status unterbrechungsfreier Energieversorgungen usw.), Statistiken über die Latenz verschiedener physischer Netzwerkverbindungen usw. zugreifen oder diese pflegen. Der Orchestrator 222 kann die Informationen in der Datenstruktur 372 und/oder die Datenstruktur, die Informationen auf höherer Ebene nachverfolgt, verwenden, um zu jedem beliebigen Zeitpunkt zu bestimmen, welcher von jedem Satz redundanter Container aktiv ist (z.B. Spalte 374 in Tabelle 372) und welcher von jedem Satz redundanter Container der nächstbeste oder nächstverfügbare Container ist (Spalte 375 in Tabelle 372). Auf diese Weise kann der Orchestrator 222 sofort einen neuen Container aktiv machen, wenn der zuvor aktive Container instabil wird, eine verminderte Leistung aufweist oder beendet wird.

[0114] Damit der Orchestrator 222 zu Zwecken des Lastausgleichs, der Fehlertoleranz oder der Fehlerbehebung neue Container instanziieren kann, stützt sich der Orchestrator 222 (und die instanziierten Dienste) zum Teil auf den Software-definierten Speicherdienst 218. **Fig. 7** ist ein Blockdiagramm, das den Software-definierten Speicherdienst 218 sowie einige der anderen Komponenten des HCI-Betriebssystems 210 und der SDCS-Anwendungsschicht 212 im Kontext zeigt. Wie oben beschrieben, kommunizieren die Anwendungen (d.h. Microdienste),

die in den Containern der SDCS-Anwendungsschicht 212 ausgeführt werden, über einen Microdienst-Bus 384, der Teil des Software-definierten Netzwerks 220 des HCI-Betriebssystems 210 ist. Der Microdienst-Bus 384 erleichtert nicht nur die Kommunikation zwischen und unter den instanziierten Containern, sondern auch die Kommunikation zwischen den Containern und dem Orchestrator 222, zwischen den Containern und dem Software-definierten Speicher 218 sowie zwischen dem Orchestrator 222 und dem Software-definierten Speicher 218.

[0115] Der Software-definierte Speicher 218 beinhaltet eine Vielzahl von Speicherressourcen, darunter drei Konfigurationsdatendienste, die allgemein als kalter Prozesskonfigurationsdatendienst 386 („kalter PCDS“), warmer Prozesskonfigurationsdatendienst 388 („warmer PCDS“) und heißer Prozesskonfigurationsdatendienst 390 („heißer PCDS“) bezeichnet werden. Der kalte PCDS 386 speichert z.B. Daten, die sich auf die Startkonfiguration des Software-definierten Steuerungssystems 100 beziehen. Die im kalten PCDS 386 gespeicherten Daten können beispielsweise Redundanz- und Fehlertoleranzanforderungen für das SDCS 100, die zu instanziierenden Anwendungsdienste 235, die zu instanziierenden Subsysteme 238, die zu instanziierenden anderen SDCS-Dienste und/oder Anwendungen 240 und die zu instanziierenden Drittanwendungen 248 beinhalten. Zusätzlich kann der kalter PCDS 386 die Startkonfigurationen für jeden der Containerdienste speichern. Während beispielsweise jede Instanz eines Steuerungscontainers ein Steuerungsdienst implementiert, benötigt der Steuerungsdienst Konfigurationsinformationen, um den Steuerungsdienst mit den Steuerungsmodul-Diensten oder Regelkreis-Diensten und anderen Informationen zu programmieren, die für die Steuerung erforderlich sind, um die Steuerung der Prozessanlage oder des Bereichs der Prozessanlage, den die Steuerung steuern soll, zu implementieren. Die Daten im kalten PCDS 386 werden daher in der Regel vom Nutzer (z.B. einem Konfigurationsingenieur) oder dem Hersteller so gestaltet, dass jeder Dienst eine Reihe von dienstspezifischen Betriebsanweisungen erhält. Jeder SDCS-Dienst (Container) würde den kalten PCDS 386 nach den gespeicherten Konfigurationsdaten abfragen. In bestimmten Ausführungsformen werden die im kalten PCDS 386 gespeicherten Daten auf für den Dienst bestimmten Software-definierten Disk Volumes gespeichert.

[0116] Der warme PCDS 388 speichert Daten, die benötigt werden, wenn ein Containerdienst gestartet wird und den Betriebszustand entweder von einer früheren Instanziierung des Dienstes oder bei der Wiederherstellung nach einem Dienstausfall wiederherstellen muss. Die im warmen PCDS 388 gespeicherten Daten können daher Zustandsinformationen über den Zustand jedes instanziierten Dienstes, Zustandsinformationen über den Zustand jedes aktiven instanziierten Dienstes und dergleichen beinhalten. Beispielsweise können solche Zustandsinformationen Integrationsakkumulatorwerte beinhalten, wenn die Konfiguration eine laufende mathematische Integration über die Zeit durchführt, die sich schnell ändern und daher für die Speicherung im kalten PCDS 386 ungeeignet wären. Der warme PCDS 376 ist für die Speicherung von sich schnell ändernden Parametern im Falle von Warmstart-Anwendungen zuständig. Daher verwendet der warme PCDS 388 in Ausführungsformen einen Write-Back-Cache auf einem gemappten Volume, um schnell wechselnde Parameter zu erfassen.

[0117] In manchen Situationen kann es jedoch erforderlich sein, dass ein instanziierter Container Informationen über den genauen Betriebszustand eines Dienstes hat. Dies kann z.B. der Fall sein, wenn ein Container unerwartet ausfällt, ohne dass ein redundanter Container zur Ausfallsicherung zur Verfügung steht. In solchen Fällen, in denen der exakte Betriebszustand eines Dienstes benötigt wird, können die Daten im heißen PCDS 390 gespeichert werden, der den exakten Betriebszustand eines SDCS-Dienstes (d.h. eines Containers) erfasst, so dass der heiße PCDS 390 an die Stelle der traditionellen RAM-Einrichtungen treten kann, die für Microdienste verfügbar sind. Die im heißen PCDS 390 gespeicherten Daten werden in der Regel in sehr schnellen, nichtflüchtigen Speicher-Volumes gespeichert, z.B. in MRAM oder NVMe-Laufwerkstechnologie. Ein neu instanziierter Ersatzcontainer kann mit Konfiguration unter Verwendung von kalten, warmen und heißen Prozessdaten aktualisiert werden, um Prozessoperationen von einem beendeten Vorgängercontainer zu übernehmen.

[0118] In einer großen industriellen Prozessanlage ist es üblich, parallele Prozessabläufe zu verwenden. Das heißt, die für die Herstellung eines Produkts erforderlichen Assets können um ein Vielfaches vervielfacht werden, um entweder ein identisches Produkt oder Variationen des Produkts herzustellen. Prozessanlagen sind daher häufig in verschiedene physische Hierarchien und Bereiche unterteilt. So kann beispielsweise eine bestimmte Gruppe von Geräten eine Einheit bilden, die innerhalb eines physischen Bereichs der Prozessanlage mehrfach dupliziert werden kann, so dass verschiedene Produktströme durch die jeweiligen Einheiten fließen können, während ähnliche Gruppen von Geräten innerhalb eines bestimmten Bereichs der Prozessanlage beibehalten werden. In ähnlicher Weise existieren logische Hierarchien, manchmal in Kombination mit den physischen Hierarchien, um Assets zu unterscheiden. Im Bereich der Chargenkontrolle wird eine „Prozesszelle“ beispielsweise als eine logische Gruppierung von Geräten definiert, die die Geräte

für die Produktion einer oder mehrerer Chargen beinhaltet. Die Prozesszelle kann eine oder mehrere Einheiten beinhalten, von denen jede ein oder mehrere Ausrüstungsmodule beinhaltet, aus denen die Einheit besteht. Jedes der Ausrüstungsmodule kann aus einem oder mehreren Steuerungsmodulen (z.B. Feldgeräten) bestehen.

[0119] Innerhalb der Prozessanlage 10 und insbesondere innerhalb des SDCS 100 kann eine Vielzahl von Verfahren in Bezug auf den Orchestrator 222 implementiert werden. Ein Verfahren kann die Konfiguration eines ersten Containers beinhalten, der einen Dienst beinhaltet, der innerhalb des ersten Containers ausgeführt wird, und die Zuweisung des konfigurierten ersten Containers zur Ausführung auf einer verfügbaren Hardware-Ressource aus einer Vielzahl von Hardware-Ressourcen. Dabei kann der erste Container so konfiguriert werden, dass er die in der Prozessanlage 10 arbeitenden Prozesssteuerungsfeldgeräte 60, 70, 80, 90 steuert. Der erste Container kann so konfiguriert sein, dass er einen Steuerungsdienst ausführt, der Daten von den Feldgeräten empfängt und aus den empfangenen Daten einen oder mehrere Steuerungsausgänge bestimmt, und dass er den einen oder die mehreren Steuerungsausgänge an die Vielzahl von Feldgeräten sendet. Der erste Container kann alternativ so konfiguriert sein, dass er einen E/A-Serverdienst ausführt. In noch anderen Ausführungsformen kann der erste Container so konfiguriert sein, dass er einen Historiker Dienst, einen Distributed Alarm Subsystem Dienst oder einen Diagnose Subsystem Dienst ausführt.

[0120] Die Zuweisung des ersten Containers zur Ausführung auf einer verfügbaren Hardwareressource kann die Zuweisung des ersten Containers zur Ausführung auf einer bestimmten Energieversorgung beinhalten. Alternativ kann die verfügbare Hardwareressource als ein bestimmtes Datencluster, eine bestimmte Gruppe von Datenclustern, ein bestimmtes Rack von Servern oder ein bestimmter Server angegeben werden. In anderen Ausführungsformen kann die verfügbare Hardwareressource als ein bestimmter Prozessor, ein bestimmter Prozessorkern, ein bestimmtes Speichergerät oder eine bestimmte Speicherressource angegeben werden.

[0121] Darüber hinaus kann das Verfahren in einigen Ausführungsformen das dynamische Hinzufügen oder Entfernen von Hardware-Ressourcen, wie physischen Servern, Datenclustern oder Knoten, beinhalten.

[0122] In bestimmten Ausführungsformen wird die verfügbare Hardware-Ressource, der der erste Container zugewiesen wird, anhand einer auf die verfügbare Hardware-Ressource bezogenen Metrik ausgewählt. Das Zuweisen des konfigurierten ersten Containers zur Ausführung auf einer verfügbaren Hardwareressource kann das Verschieben des konfigurierten ersten Containers von der Ausführung auf einer aktuellen Hardwareressource zur Ausführung auf der verfügbaren Hardwareressource gemäß einer Metrik in Bezug auf die aktuelle Hardwareressource, die verfügbare Hardwareressource oder einen Vergleich zwischen den Metriken der aktuellen und der verfügbaren Hardwareressource beinhalten. Diese Metrik kann in verschiedenen Ausführungsformen z.B. die Verarbeitungsbandbreite, die Netzwerkbandbreite, die Speicherressourcen oder die Kommunikationslatenz zwischen der Hardwareressource und einer anderen Komponente beinhalten.

[0123] Das Verfahren kann auch die Konfiguration von einem oder mehreren redundanten Containern beinhalten, um den Dienst in jedem der einen oder mehreren Container auszuführen und jedem der einen oder mehreren Container die Ausführung auf den jeweils verfügbaren Hardware-Ressourcen zuzuweisen. Der erste Container kann als aktiver Container zugewiesen werden, so dass die Ausgänge des aktiven Containers Treiberausgänge sind (d.h. den Feldgeräten zur Verfügung gestellt werden oder die Eingänge eines anderen Containers steuern).

[0124] Das Verfahren kann das Führen einer Liste von redundanten Containern (einschließlich des aktiven Containers) und das Aktualisieren der Liste der redundanten Container beinhalten, um anzuzeigen, welcher Container der aktive Container ist. In solchen Implementierungen kann die Zuweisung jedes der redundanten Container zur Ausführung auf den jeweils verfügbaren Hardwareressourcen die Auswahl der jeweils verfügbaren Hardwareressourcen beinhalten, so dass jeder der ein oder mehreren redundanten Container in mindestens einer Hinsicht Fehlertoleranz schafft, wie z.B. die Schaffung von Prozessor-Diversität, Server-Diversität und/oder Energieversorgungs-Diversität.

[0125] In noch weiteren Ausführungsformen kann das Verfahren den Empfang eines Hinweises beinhalten, dass der erste Container ein Prioritätscontainer ist, und infolgedessen die Aufrechterhaltung einer vorbestimmten Schwelle der Ressourcenverfügbarkeit auf der Hardwareressource beinhalten, um sicherzustellen, dass der Prioritätscontainer und/oder die verfügbare Hardwareressource bestimmte Leistungsanforderungen erfüllt oder übertrifft.

[0126] Fig. 8 ist ein Blockdiagramm, das die logische und physische hierarchische Anordnung einer beispielhaften Prozessanlage 400 zeigt. Die Prozessanlage 400 beinhaltet zwei Prozesszellen 402A und 402B, von denen jede drei Einheiten 404 bein-

haltet. Die Prozesszelle 402A beinhaltet die Einheiten A1, A2 und A3, während die Prozesszelle 402B die Einheiten B1, B2 und B3 beinhaltet. Jede der Einheiten beinhaltet ein oder mehrere Ausrüstungsmodule, die ihrerseits ein oder mehrere Steuerungsmodule beinhalten. Zum Beispiel beinhaltet die Einheit A1 in der Prozesszelle 402A zwei Ausrüstungsmodule 404A und 404B. Das Ausrüstungsmodul 404A beinhaltet die Steuerungsmodule 406A und 406B, während das Ausrüstungsmodul 404B die Steuerungsmodule 408A und 408B beinhaltet. Andere Einheiten in den Prozesszellen 402A und A02B beinhalten jeweils ein oder mehrere Ausrüstungsmodule (nicht gezeigt), die wiederum ein oder mehrere Steuerungsmodule (nicht gezeigt) beinhalten.

[0127] Gleichzeitig kann innerhalb der Prozessanlage 400 eine physische Hierarchie oder Organisation verwendet werden. Wenn z.B. die Prozesszellen 402A und 402B ähnliche Produkte verarbeiten, können die Einheiten A1 und B1, A2 und B2 sowie A3 und B3 jeweils identische Ausrüstungen beinhalten, die nach denselben oder unterschiedlichen Steuerschemata arbeiten. Infolgedessen kann der Betreiber der Prozessanlage ähnliche Einheiten in „Bereichen“ der Prozessanlage gruppieren. In der Prozessanlage 400 befinden sich zum Beispiel die Einheiten A1 und B1 in einem Bereich 1, die Einheiten A1 und B2 in einem Bereich 2 und die Einheiten A3 und B3 in einem Bereich 3.

[0128] Es ist zu verstehen, dass je nach Prozessanlage verschiedene logische und physische Hierarchien und Anordnungen möglich sind und dass das in **Fig. 8** dargestellte Beispiel einer Prozessanlage 400 nur ein mögliches Organisationsschema darstellt. Natürlich kann ein großer industrieller Prozess eine beliebige Anzahl von Bereichen, Prozesszellen, Einheiten, Ausrüstungsmodulen und Steuerungsmodulen haben, und infolgedessen kann eine logische Organisation dieser Module innerhalb des Steuerungsschemas besonders hilfreich sein.

[0129] Wie oben beschrieben, implementiert das SDCS 100 eine containerisierte Architektur, in der jeder Container eine isolierte Ausführungsumgebung darstellt, die innerhalb des Betriebssystems eines Rechenknotens ausgeführt wird, der den Container beherbergt (d.h. innerhalb des Betriebssystems des Rechenknotens, auf dem der Container instanziiert ist). Da jeder Container im unkonfigurierten Zustand im Wesentlichen eine „Sandkiste“ ist, in der Dienste und andere Elemente instanziiert werden können, können die Container im SDCS 100 logische und/oder physische Hierarchien innerhalb der Prozessanlage 10 darstellen. Insbesondere können Container innerhalb des SDCS 100 verschachtelt werden, um die logische und/oder physische Konfiguration der Prozessanlage genau darzustellen.

[0130] **Fig. 9** ist ein Blockdiagramm, das eine beispielhafte Implementierung von verschachtelten Containern in einem Prozesssteuerungssystem zeigt. Auf einem Rechenknoten 410 in einem Datencluster (z.B. in dem Datencluster 208) ist ein Container 412 instanziiert, der einen Prozessbereich „Prozessbereich 1“ repräsentiert. Prozessbereich 1 beinhaltet zwei Einheiten, Einheit 1 und Einheit 2. Dementsprechend sind in dem Container 412, der den Prozessbereich 1 repräsentiert, ein Container 414, der Einheit 1 repräsentiert, und ein Container 416, der Einheit 2 repräsentiert, instanziiert. Auf diese Weise kann die Hierarchie der Prozessanlage innerhalb der Organisation der Rechenelemente des SDCS 100 dargestellt werden. In dem in **Fig. 9** dargestellten Beispiel ist ein einziger kontinuierlicher Steuerungssubsystemdienst, der in einem Container 418 innerhalb des Containers 412 ausgeführt wird, sowohl für Einheit 1 als auch für Einheit 2 zuständig, und ein einziger Historikerdienst, der in einem Container 420 innerhalb des Containers 412 ausgeführt wird, historisiert Daten sowohl für Einheit 1 als auch für Einheit 2. Steuerungsdienste, E/A-Serverdienste, verteilte Alarmsubsystemdienste und Diagnosesubsystemdienste, die für jede Einheit spezifisch sind, werden jeweils in den Containern 422, 424, 426 und 428 ausgeführt, die im Container 414 verschachtelt sind, und in den Containern 430, 432, 434 und 436, die im Container 416 verschachtelt sind.

[0131] Auf diese Weise kann ein Assetbetreiber das SDCS 100 so konfigurieren, dass es das logische und/oder physische Design der zugehörigen Prozessanlage darstellt. Auf diese Weise können Container auch so konfiguriert werden, dass sie die Duplizierung von Containerstrukturen erleichtern, um die Kontrolle über getrennte, aber identische Bereiche der Prozessanlage zu implementieren und/oder um Redundanz zu schaffen und/oder um Lastausgleichsoperationen zu erleichtern. Ein Container kann beispielsweise so konfiguriert werden, dass er bei seiner Instanziierung spezifische Untercontainer beinhaltet, die bei der Instanziierung nur für den spezifischen Gerätebereich der Prozessanlage konfiguriert werden müssen, der gesteuert werden soll. Wiederum mit Bezug auf **Fig. 9** können die Container 414 und 416 verschiedene Instanzen desselben Containers sein, die bei der Instanziierung nur so konfiguriert werden müssen, dass die Container 422, 424, 426 und 428 innerhalb des Containers 414 mit den Geräten der Einheit 1 und die Container 430, 432, 434 und 436 innerhalb des Containers 416 mit den Geräten der Einheit 2 verbunden sind.

[0132] In **Fig. 10** können einzelne und/oder verschachtelte Container dupliziert werden, um die Fehlertoleranz zu erhöhen und/oder zwischen Rechenknoten oder anderen Ressourcen verschoben werden, um den Lastausgleich zu erleichtern. **Fig. 10** zeigt ein Beispiel, bei dem der Container

412 aus **Fig. 9** auf dem Rechenknoten 410 (Container 412) und auf einem zweiten Rechenknoten 440 (Container 412') instanziiert ist. Die Container 412 und 412' sind funktional identisch, aber da sie auf verschiedenen Rechenknoten instanziiert sind, kann einer der Container (z.B. der Container 412) als aktiver Container bezeichnet werden, während der andere der Container (z.B. der Container 412') als redundant bezeichnet wird (wie durch die gestrichelten Linien der Container angezeigt). Auf diese Weise kann der redundante Container (z.B. der Container 412') als aktiver Container bezeichnet werden, wenn der aktive Container nicht mehr funktioniert (wie weiter unten beschrieben) oder der Rechenknoten, auf dem der aktive Container instanziiert ist, einen Fehler aufweist (z.B. einen unerwarteten Serverfehler, einen Energieausfall usw.), und der zugehörige Bereich der Prozessanlage kann kontinuierlich und zuverlässig gesteuert werden.

[0133] Natürlich können die Container so konfiguriert werden, dass jede Instanziierung des Containers notwendigerweise alle darin verschachtelten Container einschließt (z.B. so, dass die Instanziierung eines Containers für Einheit 1 alle Container 422, 424, 426 und 428 einschließt), aber es ist auch möglich, jeden Container einzeln zu instanziieren. Eine solche Implementierung ist zum Beispiel in **Fig. 11** dargestellt, in der die beiden Rechenknoten 410 und 440 jeweils einen Bereich des dargestellten Prozesssteuerungssystems ausführen. In dem in **Fig. 11** dargestellten Beispiel ist der Container 412 auf dem Rechenknoten 410 instanziiert. In dem Container 412 sind der Container 418, der den Dienst kontinuierliches Steuerungssubsystem ausführt, und der Container 420, der den Dienst Historiker ausführt, instanziiert. Der Container 414, der zu Einheit 1 gehört, ist im Container 412 instanziiert, und die Container 422, 424, 426 und 428, die jeweils den Steuerungsdienst, den E/A-Serverdienst, den verteilten Alarmsubsystemdienst und den Diagnosesubsystemdienst ausführen, sind im Container 414 instanziiert. Gleichzeitig wird der Container 412' auf dem Rechenknoten 440 instanziiert. Im Container 412' ist ein Container 418' instanziiert, der eine redundante Instanz (gekennzeichnet durch die gestrichelten Linien) des kontinuierlichen Steuerungssubsystemdienstes ausführt, und ein Container 420', der eine redundante Instanz (gekennzeichnet durch die gestrichelte Linie) des Historikerdienstes ausführt. Der der Einheit 2 zugeordnete Container 416 ist im Container 412' instanziiert, und die Container 430, 432, 434 und 436, die jeweils den Steuerungsdienst, den E/A-Serverdienst, den verteilten Alarmsubsystemdienst und den Diagnosesubsystemdienst ausführen, sind im Container 416' instanziiert. Auf diese Weise kann ein Lastausgleich erreicht werden, indem auf dem Rechenknoten 440 Dienste, die sich auf die Einheit 2 beziehen, und auf dem Rechenknoten 410 Dienste, die sich auf die Einheit 1 beziehen, implementiert werden, während gleichzeitig eine Redundanz der Historiker- und kontinuierlichen Steuersubsystemdienste erreicht wird.

[0134] **Fig. 12** zeigt ein weiteres Beispiel für die Verschachtelung von Containern. In **Fig. 12** sind redundante Konfigurationen auf dem ersten und zweiten Rechenknoten 442 bzw. 444 instanziiert. In jeder der beiden redundanten Konfigurationen wird ein Container 446, 446' instanziiert, der demselben Prozessbereich 1 entspricht, und darin wird ein Container 448, 448' instanziiert, der einer gleichen Einheit 1 des Prozessbereichs 1 entspricht. Jeder der Container 448, 448' beinhaltet einen Satz von Containern, die Dienste für die Einheit 1 bereitstellen können, einschließlich eines Steuerungscontainers 450, 450', eines Historikercontainers 452, 452', eines Containers für ein kontinuierliches Steuerungssubsystem 454, 454', eines Containers für ein verteiltes-Alarmsubsystem 456, 456' und eines Diagnose-Subsystem-Containers 458, 458'. Redundante E/A-Server-Container 460, 460' sind auf dem ersten Rechenknoten 442 und dem zweiten Rechenknoten 444 instanziiert. Der von den E/A-Server-Containern 460, 460' implementierte E/A-Server kann E/A-Dienste für andere als die in **Fig. 12** dargestellten Prozessbereiche, Einheiten und Steuerungen ausführen und ist daher nicht in den Containern 446, 446' für Prozessbereich 1 oder den Containern 448, 448' für Einheit 1 dargestellt.

[0135] Während der E/A-Server, der durch die E/A-Server-Container 460, 460' implementiert ist, von anderen Containern als den in **Fig. 12** dargestellten verwendet werden kann, sind die Container 446, 446' für den Prozessbereich 1 in der Abbildung als an den E/A-Server 1 „angeheftet“ dargestellt. Auf diese Weise veranschaulicht **Fig. 12** ein weiteres Merkmal des SDCS 100, nämlich dass Elemente innerhalb des SDCS 100 aneinander angeheftet sein können, so dass angeheftete Elemente auf derselben Hardware arbeiten oder auf der Hardware arbeiten, an die sie angeheftet sind. In **Fig. 12** sind beispielsweise die Container 446, 446' für den Prozessbereich 1 an die jeweiligen E/A-Server-Container 460, 460' angeheftet, so dass der Container 446 auf demselben Server wie der E/A-Server-Container 460 und der Container 446' auf demselben Server wie der E/A-Server-Container 460' instanziiert wird. Wenn also der Prozessbereichcontainer 446 auf einen anderen Server verschoben wird, würde der E/A-Servercontainer 460 ebenfalls auf denselben Server wie der Prozessbereichcontainer 446 verschoben werden. Dasselbe gilt für den Container 446', der an den Container 460' angeheftet ist.

[0136] Container können an eine Vielzahl von Komponenten der Prozessanlage 10 angeheftet werden. Wie in **Fig. 12** beschrieben, können Container in Ausführungsformen an andere Container angeheftet

werden, so dass die Container, wenn sie von einem Teil der Prozessanlage zu einem anderen bewegt werden, als eine Einheit bewegt werden und auf demselben Teil der Anlage ausgeführt werden. Dies kann z.B. nützlich sein, um sicherzustellen, dass die Netzwerklatenz zwischen angehefteten Containern minimal bleibt. In bestimmten Ausführungsformen können Container an bestimmte Verarbeitungshardware angeheftet werden, z.B. an einen bestimmten Datencluster, einen bestimmten Rechenknoten eines Datenclusters, einen bestimmten Prozessor eines bestimmten Rechenknotens, ein bestimmtes Server-Rack, einen bestimmten Prozessorkern eines Prozessors, usw. In einigen Ausführungsformen kann ein Container auf einem intelligenten Feldgerät instanziiert werden und als solcher kann ein Container an ein bestimmtes Feldgerät angeheftet werden. Container können auch an bestimmte physische nicht-Computer-Ressourcen angeheftet werden. So kann ein Container beispielsweise an eine bestimmte physische E/A-Schnittstelle oder sogar an eine bestimmte Energieversorgung gebunden sein, die eine Vielzahl von Computerressourcen versorgt. Im letzteren Fall könnte jeder von zwei redundanten Containern zwischen Rechenressourcen, die von entsprechenden Energieversorgungen versorgt werden, verschoben werden, während die Fehlertoleranz in Bezug auf die Energieversorgungen erhalten bleibt.

[0137] **Fig. 13** und **Fig. 14** zeigen verschiedene Beispiele für das Anheften von Containern an Komponenten. In **Fig. 13** ist auf einem Rechenknoten 462 eine Vielzahl von Containern 464-474 instanziiert, darunter ein Steuerungscontainer 464, ein Historikercontainer 466, ein kontinuierlicher Steuerungssubsystem-Container 468, ein verteilter Alarm-Subsystem-Container 470, ein Diagnose-Subsystem-Container 472 und ein E/A-Server-Container 474. Wie in **Fig. 13** dargestellt, ist der E/A-Server-Container 474 an den Rechenknoten 462 angeheftet. Während also andere der auf dem Rechenknoten 462 instanziierten Container „verschoben“ werden können (d.h. vor Beendigung der auf dem Rechenknoten 462 instanziierten Instanz auf anderer Hardware instanziiert werden), verbleibt der E/A-Server-Container 464 so lange auf dem Rechenknoten 462, bis ein Umstand (z.B. Instabilität des Servers, abnormale Beendigung usw.) dazu zwingt, den E/A-Server-Container 464 zu verschieben. Gleichzeitig wird der kontinuierliche Steuerungssubsystem Container 468 an den Steuerungscontainer 464 angeheftet. Der Steuerungscontainer 464 und der kontinuierliche Steuersubsystem Container 468 werden als Paar instanziiert, um z.B. sicherzustellen, dass der Datenverkehr zwischen den Containern 464, 468 aufgrund ihrer Instanziierung auf denselben Hardware-Ressourcen eine minimale Latenz aufweist.

[0138] Wenn ein Container an eine bestimmte Hardware-Ressource angeheftet wird, kann diese Anheftung spezifisch für die Instanz des Containers sein - das heißt, eine Instanz eines Containers kann an eine erste Hardware-Ressource angeheftet werden, während eine zweite, redundante Instanz des Containers an eine zweite, separate Hardware-Ressource angeheftet werden kann. In einem solchen Fall kann das Anheften eines Containers an eine Hardware-Ressource die Redundanz und Fehlertoleranz erleichtern. Wenn jedoch ein Container an einen anderen Container gebunden ist, kann dieses Anheften in einigen Instanzen auf alle redundanten Instanzen des Containerpaars übertragen werden - d.h., ein Steuerungssubsystem-Paar kann gemeinsam instanziiert werden, unabhängig davon, auf welcher Hardware-Ressource jede Instanz des Paars instanziiert ist. Auf diese Weise kann das Anheften eines Containers an einen anderen implementiert werden, um z.B. Ziele im Zusammenhang mit der Netzwerk-Latenz und dem Bandbreitenmanagement zu erreichen.

[0139] **Fig. 14** zeigt ein Beispiel, bei dem zwei Energieversorgungen 476 und 478 Energie an die jeweiligen Rechenknoten liefern. Eine erste der Energieversorgungen 476 liefert Energie an drei Rechenknoten 479, 480, 481, während eine zweite der Energieversorgungen 478 Energie an drei andere Rechenknoten 482, 483, 484 liefert. Auf den Servern 479-481 und 482-484 ist jeweils derselbe Satz von Containern instanziiert, so dass eine Fehlertoleranz von 1:2 gegeben ist, d.h. wenn eine der Energieversorgungen 476, 478 ausfällt, bleiben die redundanten Container auf den anderen Energieversorgungen 476, 478 aktiv. Insgesamt sind auf den Servern 479-481 instanziiert: ein SIS-Steuerungscontainer 485, ein Steuerungscontainer 486, ein kontinuierlicher Steuerungssubsystem-Container 487, ein verteilter Alarm-Subsystem-Container 488, ein E/A-Server-Container 489, ein Historikercontainer 490 und ein Diagnose-Subsystem-Container 491. Ebenso sind auf den Servern 482-484 instanziiert: ein SIS-Steuerungscontainer 485', ein Steuerungscontainer 486', ein kontinuierlicher Steuerungssubsystem-Container 487', ein verteilter Alarm-Subsystem-Container 488', ein E/A-Server-Container 489', ein Historikercontainer 490' und ein Diagnose-Subsystem-Container 491'. Tatsächlich ist jeder der auf den Servern 479-481 instanziierten Container 485-491 an die erste Energieversorgung 476 angeheftet, wobei der SIS-Steuerungscontainer 485 speziell an den ersten Rechenknoten 479, der Historikercontainer an den dritten Server 481 und die übrigen Container 485-491 allgemein an die erste Energieversorgung 476 angeheftet sind. Gleichzeitig ist jeder der auf den Servern 482-484 instanziierten Container 485'-491' effektiv an die zweite Energieversorgung 478 angeheftet, wobei der SIS-Steuerungscontainer 485' speziell an den vierten Rechen-

knoten 482, der Historikercontainer an den sechsten Server 484 und die übrigen Container 485'-491' allgemein an die zweite Energieversorgung 478 angeheftet sind. Mit Ausnahme der SIS-Steuerungscontainer 485, 485' und der Historikercontainer 490, 490' können die Container 485-491 zwischen dem ersten, zweiten und dritten Server 479-481 und die Container 485'-491' zwischen dem vierten, fünften und sechsten Server 482-484 verschoben werden, um einen Lastausgleich zu erreichen und gleichzeitig die Fehlertoleranz zu erhalten.

[0140] Wie in den obigen Abschnitten erläutert, können die Verschachtelung und das Anheften von Containern natürlich in Verbindung miteinander oder separat verwendet werden. Dementsprechend kann ein Verfahren die Instanziierung von ersten und zweiten Containern in einem ersten Rechenknoten eines Daten-Clusters beinhalten, wobei jeder Container eine isolierte Ausführungsumgebung innerhalb eines Betriebssystems des ersten Rechenknotens darstellt. Der zweite Container kann innerhalb des ersten Containers instanziiert werden, während ein Dienst innerhalb des zweiten Containers instanziiert wird. Jeder der ersten und zweiten Container entspricht einer ersten bzw. zweiten Ebene einer hierarchischen Struktur der Prozessanlage, in Ausführungsformen. Gleichzeitig kann der erste Container auch einen oder mehrere Dienste beinhalten, die darin ausgeführt werden. Bei dem im ersten Container ausgeführten Dienst kann es sich in bestimmten Ausführungsformen um einen E/A-Dienst handeln.

[0141] Das Verfahren kann auch die Instanziierung eines dritten Containers auf dem ersten Rechenknoten beinhalten, der insbesondere innerhalb des ersten Containers instanziiert wird. In bestimmten Ausführungsformen kann der im zweiten Container ausgeführte Dienst ein Steuerungsdienst sein, der eine Steuerungsroutine ausführt, die so konfiguriert ist, dass sie eine Teilmenge der Prozesssteuerungsfeldgeräte in einem ersten Bereich der industriellen Prozessanlage steuert, während der im dritten Container ausgeführte Dienst ein Steuerungsdienst sein kann, der eine Steuerungsroutine ausführt, die so konfiguriert ist, dass sie eine andere Teilmenge der Prozesssteuerungsfeldgeräte in einem zweiten Bereich der industriellen Prozessanlage steuert. In einigen Ausführungsformen können die in den zweiten und dritten Containern ausgeführten Dienste entsprechende E/A-Serverdienste beinhalten, die für die Datenkommunikation zwischen den Prozesssteuerungsfeldgeräten und den jeweiligen Steuerungsdiensten konfiguriert sind. In bestimmten Ausführungsformen kann das Verfahren die Instanziierung redundanter verschachtelter Containerstrukturen auf einem oder mehreren verschiedenen Knoten des Datenclusters beinhalten.

[0142] In verschiedenen Ausführungsformen kann ein Verfahren die Instanziierung einer Vielzahl von Containern in einem Datencluster des industriellen Prozesssteuerungssystems 10 beinhalten, das ein SDCS 100 zur Steuerung einer Vielzahl von Prozesssteuerungs-Feldgeräten 60, 70, 80, 90 ausführt, die zur Steuerung eines physischen Prozesses in einer industriellen Prozessanlage arbeiten. Jeder der mehreren instanziierten Container kann eine isolierte Ausführungsumgebung sein, die innerhalb eines Betriebssystems eines der mehreren Rechenknoten, auf denen der Container instanziiert ist, ausgeführt wird. Die mehreren instanziierten Container können zusammenarbeiten, um die Ausführung einer Steuerstrategie in dem Software-definierten Steuerungssystem zu erleichtern. Das Verfahren kann auch das Anheften eines ersten Containers aus der Vielzahl von Containern an eine Komponente des Software-definierten Steuerungssystems beinhalten. Wie oben beschrieben, können in einigen Ausführungsformen ein oder mehrere der Vielzahl von Containern einer Ebene einer hierarchischen Struktur der Prozessanlage entsprechen.

[0143] In bestimmten Ausführungsformen kann das Verfahren auch das Ausführen eines Dienstes in mindestens einem der mehreren instanziierten Container beinhalten. Der Dienst kann z.B. einen E/A-Serverdienst, einen Steuerungsdienst, einen Historikerdienst, einen verteilten Alarmsubsystemdienst, einen Diagnosesubsystemdienst, einen Drittanbieterdienst oder einen Sicherheitsdienst beinhalten. Darüber hinaus kann das Anheften eines ersten Containers an eine Komponente des SDCS auch das Anheften des Containers an einen anderen Container beinhalten, der selbst innerhalb des ersten Containers instanziiert sein kann oder in dem der erste Container instanziiert sein kann.

[0144] Bei der Komponente, an die der Container angeheftet wird, kann es sich um eine Energieversorgung handeln, die einen oder mehrere Datencluster oder einen Bereich eines Datenclusters mit Energie versorgt, oder es kann sich um einen Datencluster, einen Rechenknoten des Datenclusters, ein Server-Rack innerhalb des Datenclusters, einen Server, einen bestimmten Prozessor oder einen bestimmten Prozessorkern innerhalb eines Prozessors handeln. Bei der Komponente kann es sich alternativ um einen E/A-Server-Container handeln, in dem ein E/A-Server-Dienst ausgeführt wird, um ein Prozesssteuerungs-Feldgerät oder um eine physische E/A-Schnittstelle. In bestimmten Ausführungsformen kann das Verfahren die Instanziierung redundanter Containerstrukturen beinhalten, die an verschiedene Knoten, Server, Energieversorgungen, Prozessoren oder Prozessorkerne angeheftet sind.

[0145] Fig. 15 ist ein Blockdiagramm eines E/A-Subsystems oder E/A-Netzwerks 500 mit container-

isierten Diensten zur Implementierung der Steuerung eines Bereichs eines Prozesses in einem Bereich 501 und eines Bereichs eines Prozesses in einem Bereich 502 der in **Fig. 1** dargestellten Anlage 10. Das E/A-Subsystem 500 kann Teil des E/A-Gateways 40 und der SDCS 100/200 sein, die in **Fig. 1** und **Fig. 2** dargestellt sind, und/oder mit diesen verbunden sein.

[0146] Was den Begriff „E/A-Netzwerk“ betrifft, so kann das Netzwerk, das aus einer oder mehreren Steuerungen oder Steuerungsdiensten (z.B. in Containern), den Feldgeräten, die kommunikativ mit der einen oder den mehreren Steuerungen oder Steuerungsdiensten verbunden sind, und den zwischengeschalteten Hardware- oder Softwareknoten (z.B. E/A-Serverdienste, E/A-Karten usw.), die die Kommunikation zwischen den Steuerungen oder Steuerungsdiensten und den Feldgeräten erleichtern, gebildet wird, allgemein als „E/A-Netzwerk“ oder „E/A-Subsystem“ bezeichnet werden.

[0147] Auf einer hohen Ebene beinhaltet das E/A-Subsystem 500: (i) einen E/A-Serverdienst (manchmal auch „E/A-Dienst“ oder einfach „Dienst“) 511a für den Bereich 501 und (ii) einen E/A-Dienst 511b für den Bereich 502. Es ist zu beachten, dass sich der Großteil der nachfolgenden Beschreibung auf die Konfiguration und den Betrieb des E/A-Dienstes 511a konzentriert. Es versteht sich jedoch von selbst, dass der E/A-Dienst 561a in ähnlicher Weise konfiguriert werden kann, um eine ähnliche Funktionalität in Bezug auf Einheiten zu bieten, die zur Implementierung der Steuerung der Prozessausrüstung im Bereich 502 verwendet werden.

[0148] Der E/A-Dienst 511a ist ein Softwaredienst, der auf einem beliebigen geeigneten Computer oder Knoten implementiert ist. Den Dienst 511a kann man sich als Plattform, Anwendung oder Suite oder Reihe von Anwendungen vorstellen, die E/A-Funktionen (z.B. über eine Verbindung oder ein Netzwerk) in Bezug auf das E/A-Subsystem 500 für verschiedene Routinen, Module, Dienste, Container, Geräte oder Knoten in der Anlage 10 bereitstellt. Zum Beispiel kann ein Feldgerät (oder eine mit einem Feldgerät gekoppelte E/A-Karte) mit dem E/A-Dienst 511a interagieren, indem es: (i) vom Dienst 511a Steuerungsausgänge wie Befehle zur Betätigung eines Feldgeräts empfängt und/oder (ii) an den E/A-Dienst 511a Feldgerätausgaben wie gemessene Prozessparameter oder vom Feldgerät erzeugte oder berechnete Indizes übermittelt. Außerdem kann ein Steuerungsdienst mit dem E/A-Dienst 511a interagieren, indem er: (i) dem E/A-Dienst 511a Steuerungsausgänge zur Verfügung stellt (z.B. Befehle übermittelt) und/oder (ii) vom E/A-Dienst 511a Steuerungseingängen empfängt (z.B. die Feldgerät-Ausgänge, die z.B. gemessene Prozessparameter darstellen). Die Kommunikation zwischen dem E/A-Dienst 511a und den von ihm bedienten Einheiten (z.B. Feldgeräte, Steuerungsserver) kann unter Verwendung jedes geeigneten Kommunikationsmodells erfolgen, wie z.B. eines Push-Modells, bei dem der E/A-Dienst 511a Herausgeber ist und Feldgeräte und/oder Steuerungsdienste Abonnenten sind; oder bei dem der E/A-Dienst 511a ein Abonnent ist und Feldgeräte und/oder Steuerungsdienste Herausgeber sind. Ebenso kann ein Pull-Modell verwendet werden, bei dem der E/A-Dienst 511a Anforderer ist und Feldgeräte und/oder Steuerungsdienste auf die Anfrage antworten; oder bei dem der E/A-Dienst 511a auf Anfragen der Feldgeräte und/oder Steuerungsdienste antwortet. Falls gewünscht, kann ein hybrides Modell verwendet werden, bei dem der E/A-Dienst 511a eine andere Kommunikationsrolle mit den Feldgeräten (z.B. Herausgeber, Teilnehmer, Anforderer, Beantworter, usw.) übernimmt als mit den Steuerungsdiensten.

[0149] In jedem Fall empfängt der E/A-Dienst 511 a während des Beispielbetriebs mehrere Sätze von Steuerungsausgänge von einer Vielzahl von containerisierten Steuerungsdiensten, die jeweils die gleiche Steuerungsroutine zur Steuerung des Bereichs 501 implementieren. In einem typischen Beispiel übergibt der Dienst 501 einen einzigen „aktiven“ Satz der Steuerungsausgänge (d.h. die Ausgänge von einem bestimmten der containerisierten Steuerungsdienste) an die entsprechenden Feldgeräte, um den Bereich 501 zu steuern. Außerdem werden die anderen „inaktiven“ Sätze von Steuerungsausgängen nicht an die entsprechenden Feldgeräte weitergeleitet. Der E/A-Serverdienst 561a ist in Bezug auf den Bereich 502 ähnlich konfiguriert und in der Lage, mehrere Sätze von Steuerungsausgängen zu verarbeiten, einschließlich eines „aktiven“ Satzes von Steuerungsausgängen und eines oder mehrerer „inaktiver“ Sätze.

[0150] Auf einer hohen Ebene agiert der E/A-Dienst 511a als Vermittler zwischen: (i) einem Satz von Feldgeräten 531 (z.B. einschließlich Pumpen, Ventilen und anderen Betätigungsgeräten), die eine physische Steuerungsaktion in der Anlage durchführen, einem Satz von Feldgeräten 532 (z.B., einschließlich sensorbasierter Feldgeräte), die als Transmitter arbeiten, um Prozessvariablen in der Anlage zu messen und zu übertragen, sowie möglicherweise eine Reihe von Feldgeräten 533, die eine Reihe von Mikrocontainern kapseln, die „kundenspezifische“ Algorithmen ausführen (wie ein Mikrocontainer für die Spektralverarbeitung, der für die Spektralverarbeitung in einem Spektrometergerät relevant ist, oder ein Bildverarbeitungsmikrodienst für ein Gerät mit angeschlossener Kamera) und die verarbeitete E/A-Daten für bestimmte Verwendungszwecke (die Steuer- oder Wartungszwecke sein können) erzeugen und übertragen, und (ii) einen oder mehrere containerisierte Steuerungsdienste 521a-c, die jeweils

Instanzen 525a-c der gleichen Steuerungsroutine #1 ausführen (z. B. g., denselben konfigurierten Steuerungs-Routinedienst #1), um denselben Satz von Feldgeräten 531 und 532 zu steuern und so den Bereich 501 zu steuern. Während die Feldgeräte 531 als aktivierende Feldgeräte dargestellt sind, die sich von den Feldgeräten 532 unterscheiden, die als Übermittler (z.B. von gemessenen Prozessparametern) fungieren, die sich von den Feldgeräten 533 unterscheiden, die benutzerdefinierte Algorithmen oder benutzerdefinierte Mikrocontainer beinhalten, um Prozessvariablendaten zu verarbeiten oder zu manipulieren, wird der Einfachheit halber verstanden, dass die beschriebenen Feldgeräte in der Lage sein können, ein Steuerelement oder alle Steuerelemente (z.B. ein Ventilstellglied), um eine Prozessvariable zu manipulieren, gemessene oder berechnete Feldgeräte- oder Prozessvariablen zu messen und zu übertragen und gesammelte Prozessdaten oder andere Messungen zu verarbeiten oder zu manipulieren und die verarbeiteten oder manipulierten Daten zu übertragen. Ein intelligenter Ventilpositionierer kann beispielsweise so konfiguriert sein, dass er einen Befehl zur Betätigung des Ventils empfängt und den gemessenen Durchfluss, die ermittelte Ventilstellung, Zustandsindizes zum Zustand des Ventils überträgt und gesammelte Bilddaten von einer Kamera auf dem Ventilstellglied verarbeitet, um ein defektes Ventil zu erkennen und diese verarbeiteten oder gesammelten Daten zu übertragen, usw.

[0151] In einigen Ausführungsformen ist der E/A-Dienst 511a nicht containerisiert. Falls gewünscht, ist der E/A-Dienst 511a jedoch in einem E/A-Server-Container (manchmal auch „E/A-Container“) 505a untergebracht. In verschiedenen Ausführungsformen beinhaltet das E/A-Subsystem 500 mehrere E/A-Container 505a-c. Jeder der E/A-Container 505a-c empfängt dieselben Eingaben (z.B. von den Steuerungsdiensten und Feldgeräten), erzeugt dieselben Ausgänge (z.B. an die Feldgeräte und Steuerungsdiensten) und implementiert dieselbe Logik (z.B. zur Auswertung, welcher containerisierte Steuerungsdienst aktiv sein sollte, zur Behandlung von Übergängen zwischen Steuerungsdiensten usw.). Wenn mehrere E/A-Server-Container 505a-c implementiert sind, kann dementsprechend ein einzelner der E/A-Server-Container 505a-c als „aktiv“ bezeichnet werden. Zum Beispiel wird in **Fig. 15** durch durchgezogene und gestrichelte Linien angezeigt, dass der E/A-Container 505a „aktiv“ ist und dass die E/A-Server-Container 505b und 505c „inaktiv“ sind. In einem solchen Beispiel leitet der E/A-Container 505a den Datenverkehr an Steuerungsdienste und Feldgeräte weiter, die Container 505b und 505c jedoch nicht. Man könnte sagen, dass in einer Ausführungsform alle Container (einschließlich der „inaktiven“ Container) dieselben E/A-Daten empfangen, aber nur „aktive“ Container E/A-Daten senden, die von Steuerungsdiensten und Feldgeräten empfangen und verarbeitet werden.

[0152] In einigen Fällen übertragen die inaktiven E/A-Container keinen Datenverkehr. In anderen Fällen überträgt jeder der E/A-Container 505a-c E/A-Verkehr (einschließlich der inaktiven E/A-Container), aber ein Switch fängt den Verkehr ab und leitet den Verkehr nur dann an sein Ziel weiter, wenn er vom „aktiven“ E/A-Server-Container übertragen wird. In einigen Fällen können „inaktive“ E/A-Server-Container Daten an andere Container übertragen, obwohl sie nicht aktiv als zwischengeschalteter E/A-Server zwischen Feldgeräten und Steuerungsdiensten fungieren. Beispielsweise kann ein „inaktiver“ E/A-Server-Container an Lastausgleichsoperationen teilnehmen, indem er E/A-Verkehr (z.B. Steuerungseingänge, Steuerungsausgänge usw.) an einen Historiker oder Historikercontainer, eine Nutzer-Workstation oder einen Workstation-Container, an andere Assets oder externe Netzwerke usw. weiterleitet. Dementsprechend kann der/die „inaktive(n)“ E/A-Server den „aktiven“ E/A-Container von der „Verschwendung“ von Verarbeitungsenergie oder Netzwerkkapazität für die Ausführung solcher Funktionen entlasten. Dies kann besonders vorteilhaft sein, wenn die E/A-Container 505a-c über mehr als einen physischen Computer verteilt sind. Jeder E/A-Container 505a-c kann auf einem oder mehreren physischen Servern implementiert werden, wie sie in **Fig. 16** und **Fig. 17** dargestellt sind.

[0153] Wie bereits erwähnt, führen die containerisierten Steuerungsdienste 521a-c jeweils eine Instanz 525a-c der gleichen Steuerungsroutine #1 in den Containern 515a-c aus, um den gleichen Satz von Feldgeräten 531 und 532 zu steuern und damit den Bereich 501 zu steuern. In einigen Ausführungsformen kann die Steuerungsroutine #1 z.B. als ein oder mehrere konfigurierte Steuerungs-Routinedienste und/oder ein oder mehrere konfigurierte Steuerungsfunktionsblockdienste implementiert sein. Die Container 515a-c können auf jedem geeigneten Computergerät, Knoten oder Computercluster implementiert werden. In einigen Fällen werden einer oder mehrere der Container auf Computergeräten in der Anlageumgebung in der Nähe der Feldgeräte implementiert, für deren Steuerung die entsprechenden Steuerungsdienste konfiguriert sind. In einigen Fällen können die Geräte, die die Container implementieren, in ein Rack eingebaut sein und einen ähnlichen Formfaktor oder ein ähnliches Gehäuse haben, wie es für eine physische Prozesssteuerung typisch ist. In anderen Fällen werden die Container der Steuerungsdienste von Servern oder Computern an einem anderen Ort in der Anlage, in einem Steuerungsraum, in einem Rechenzentrum, in einem Computer-Cluster, an einem entfernten Standort usw. implementiert. Einfach ausgedrückt: Solange die containerisierten Steuerungsdienste eine geeignete

Netzwerkverbindung mit den von ihnen gesteuerten Feldgeräten herstellen können (z.B. über einen E/A-Serverdienst wie den Dienst 511a), können die containerisierten Steuerungsdienste auf jeder geeigneten Hardware an jedem geeigneten Standort implementiert werden.

[0154] Wie bereits erwähnt, stellt jeder der containerisierten Steuerungsdienste 521a-c dieselbe konzeptionelle Steuerung dar, die dieselbe Steuerungsroutine #1 implementiert (jede ist so konfiguriert, dass sie auf und von denselben Tags, die mit denselben Feldgeräten verbunden sind, liest und auf sie schreibt). Zu jedem beliebigen Zeitpunkt können zwei der drei containerisierten Steuerungsdienste 521a-c als Duplikate oder als redundante Steuerungsdienste zum „aktiven“ containerisierten Steuerungsdienst betrachtet werden. Im Allgemeinen stellt jeder Steuerungsdienst eine Softwareplattform oder -infrastruktur dar, die derjenigen entspricht, die in Hardware-Steuerungen zu finden ist. Jeder Steuerungsdienst ist so konfiguriert, dass er Steuerungsroutinen erkennt und ausführt, die oft spezialisierte und erwartete Datenformate und -strukturen haben (z.B. wie von konfigurierten Steuerungsmodul-Diensten definiert, die wiederum mit Steuerungsfunktionsblock-Diensten konfiguriert wurden). Ein Steuerungsdienst kann als eine Schicht zwischen dem Container, der auf dem physischen Gerät läuft, und der Top-Level-Anwendung (z.B. den Steuerungsroutinen) betrachtet werden. Zu diesem Zweck kann ein „Steuerungsdienst“ analog zu einem Betriebssystem betrachtet werden, das in einem Container auf einem Computergerät implementiert ist, damit der Container und das Computergerät die Steuerungsroutinen richtig erkennen und ausführen können. In einigen Fällen kann ein Steuerungsdienst ein Emulator sein oder einen Emulator beinhalten, der ein bestimmtes Hardwaremodell einer physischen Prozesssteuerung emuliert.

[0155] Eine Steuerungsroutine oder ein Steuerungsmodul ist ein Satz von Anweisungen, die von einem Prozessor ausgeführt werden können, um eine oder mehrere Operationen auszuführen, um zumindest einen Teil eines Prozesses zu steuern oder zu kontrollieren. Im Allgemeinen kann eine Steuerungsroutine oder ein Steuerungsmodul als Software verstanden werden, die so konfiguriert ist, dass sie eine bestimmte Steuerungsstrategie implementiert. Sie kann innerhalb des SDCS 200 als konfigurierter Steuerungsmodul-Dienst implementiert werden, der in seinem Container ausgeführt wird. Eine Steuerungsroutine oder ein Steuerungsmodul kann einen oder mehrere miteinander verbundene Steuerungsfunktionsblöcke beinhalten, die mit verschiedenen Funktionen verbunden sind. Bei diesen Funktionsblöcken kann es sich um Objekte in einem objektorientierten Programmierprotokoll handeln, die Funktionen innerhalb eines Steuerungsschemas auf der Grundlage von Eingaben ausführen und Ausgänge an andere Funktionsblöcke innerhalb des Steuerungsschemas liefern können. In einer Ausführungsform kann ein Steuerungsfunktionsblock innerhalb des SDCS 200 als ein konfigurierter Steuerungsfunktionsblock-Dienst implementiert werden, der in seinem Container ausgeführt wird. Allgemeiner ausgedrückt, stellt eine Steuerungsroutine eine Logik dar, die auf der Grundlage eines oder mehrerer Steuerungseingänge (z.B. gemessene Prozessvariablen wie Temperatur, Druck, Durchfluss usw.) ausgeführt wird, um einen oder mehrere Steuerungsausgänge (z.B. Befehle zur Manipulation eines Feldgeräts wie eines Steuerventils) zu erzeugen. Die Steuerungsausgänge können dazu führen, dass die Manipulation eines Prozesseingangs, wie z.B. der oben erwähnten Ventilstellung (solche Prozesseingänge können auch als „Stellgrößen“ bezeichnet werden), einen Prozessausgang (der als „Steuergröße“ oder einfach als „Prozessgröße“ bezeichnet werden kann) verändert oder steuert. Die gesteuerte Variable kann jede geeignete Variable sein, die die Steuerungsroutine zu steuern versucht. Um beim vorherigen Beispiel zu bleiben, kann die Stellung des Steuerventils an einem Einlassventil manipuliert werden, um das Einlassventil zu öffnen und den Füllstand im Tank zu erhöhen (der Füllstand ist hier die gesteuerte Variable). In vielen Fällen wird die Steuergröße gemessen und als Steuerungseingang an die Steuerungsroutine zurückgegeben. Die Steuerungsroutine kann auch einen gewünschten Wert für die gesteuerte Variable (d.h. einen Sollwert) als Eingabe akzeptieren, der von einem Nutzer oder einer Steuerungsroutine (z.B. dieselbe Steuerungsroutine oder eine andere Steuerungsroutine) geliefert werden kann. In **Fig. 15** sind zwar nicht explizit Sollwerte als Eingaben für die Steuerungsroutineninstanzen 525a-c oder 575a-c dargestellt, aber jede beschriebene oder dargestellte Steuerungsroutineninstanz kann einen Sollwert erhalten.

[0156] Um bei **Fig. 15** zu bleiben: Während des typischen Betriebs empfängt der E/A-Dienst 511a eine Prozessausgabe (manchmal „Feldgerätausgabe“) oder eine Reihe von Prozessausgaben vom Feldgerät 532 über einen E/A-Kanal 542a oder eine Reihe von verarbeiteten Daten vom Feldgerät 533 über einen E/A-Kanal 542b. Bei der Prozessausgabe kann es sich um eine beliebige Prozessvariable handeln, die einen erkannten oder berechneten Wert beinhaltet (z.B. die Anzeige, dass die Variable LT004 für den Tankfüllstand einen Wert von 20% hat). Der E/A-Dienst 511a gibt die Prozessausgabe über die E/A-Kanäle 543a-c an jede Steuerungsroutineninstanz 525a-c als Steuerungseingang weiter. Das heißt, jeder der E/A-Kanäle 543a-c ist dieselben Variablen oder Variablengruppen mit denselben Werten oder Wertegruppen zugewiesen (z.B. die Angabe LT004 = 20%).

[0157] Die Steuerungs-Routinedienst Instanzen 525a-c empfangen die Steuerungseingängen und erzeugen auf der Grundlage der Werte der Steuerungseingängen (z.B. LT004 = 20%) und der Logik der Steuerungsroutine (z.B. Anzeige, dass der Tank auf ein höheres Niveau gefüllt werden soll) Steuerungsausgänge (z.B. einen Befehl, ein Einlassventil auf 75% zu öffnen). Die Steuerungsdienste 521a-c übermitteln die Steuerungsausgänge über die E/A-Kanäle 544a-c an den E/A-Dienst 511a. Anders ausgedrückt: Der E/A-Kanal 544a überträgt eine Reihe von Ausgänge der Steuerungsroutineninstanz 525a; der E/A-Kanal 544b überträgt eine Reihe von Steuerungsausgänge der Steuerungsroutineninstanz 525b; und der E/A-Kanal 544c überträgt eine Reihe von Steuerungsausgänge der Steuerungsroutineninstanz 525c. In einem typischen Beispiel sind die Steuerungseingänge typischerweise identisch und da die Instanzen 525a-c der Steuerungsroutine #1 identisch sind, sind auch die Sätze der Steuerungsausgänge oft identisch (z.B. kann jeder E/A-Kanal 544a-c einen Befehl zum Öffnen des Einlassventils auf 75% übertragen). Wenn jedoch eine Steuerungsroutine oder der Netzwerkverkehr auf irgendeine Weise beeinträchtigt wird, können sich die verschiedenen Sätze unterscheiden. Dementsprechend kann der E/A-Dienst 511a verschiedene Fehlerprüfungen an den empfangenen Sätzen vornehmen. In einigen Fällen kann der E/A-Dienst eine Konsensanalyse oder ein Best-of-n-Abstimmungsschema durchführen, um ein Set auszuwählen. Wenn sich zum Beispiel die ersten beiden vom Dienst 511 a empfangenen Sätze unterscheiden, kann der Dienst 511a einen der beiden Sätze zur Weiterleitung auswählen, je nachdem, welcher der beiden empfangenen Sätze mit einem dritten vom Dienst 511a empfangenen Satz übereinstimmt.

[0158] Genauer gesagt, analysiert der E/A-Dienst 511a die empfangenen Sätze von Steuerungsausgänge und/oder die mit jedem Satz von Steuerungsausgängen verbundenen Metadaten. Insbesondere kann eine QoS-Metrik für jeden Satz analysiert werden, und der Satz mit der besten QoS-Metrik kann entweder vom E/A-Dienst 511a oder von einem anderen Dienst (z.B. einem Orchestratordienst) als „aktiver“ Satz von Steuerungsausgängen bestimmt werden. Bei der QoS-Metrik kann es sich um eine beliebige Metrik zur Analyse der Qualität der von den containerisierten Steuerungsdiensten erbrachten Dienstleistung handeln, z.B. Latenz, Genauigkeit, Nachrichtenrate usw. Die Routine, der Dienst, der Container und der E/A-Kanal, die der „besten“ QoS-Metrik entsprechen, können (explizit oder implizit) als „aktiv“ bezeichnet werden. In einer Ausführungsform können eine einzelne Steuerungs-Routinedienst Instanz 525a-c, ein einzelner Steuerungsdienst 521a-c, ein einzelner Container 521a-c und ein einzelner E/A-Kanal 44a-c zu einem bestimmten Zeitpunkt als „aktiv“ gelten. Die übrigen Steuerungs-Routinedienst Instanzen 525a-c, Steuerungsdienste 521a-c, Container 521a-c und E/A-Kanäle 544a-c können als „inaktiv“ bezeichnet oder betrachtet werden. Der E/A-Dienst 511a leitet die Sätze der Steuerungsausgänge der „aktiven“ Container und Steuerungsdienste über den E/A-Kanal 540 an das Feldgerät 531 weiter. Die Sätze der Steuerungsausgänge aus den „inaktiven“ Containern werden nicht an die Feldgeräte weitergeleitet, obwohl sie zu anderen Zwecken (z.B. zur Optimierung der Nutzung von Computer- und/oder Netzwerkressourcen) an andere Container und/oder Dienste (z.B. an einen Datenhistoriker) weitergeleitet werden können.

[0159] Die gestrichelten Linien in **Fig. 15** zeigen an, welche Routinen, Dienste, Container und Kanäle inaktiv sind. Wie dargestellt, sind der Container 515c, der Steuerungsdienst 521c, der Routinedienst 525c und der E/A-Kanal 544c „aktiv“, d.h. die von der Routinedienst Instanz 525c erzeugten und an den E/A-Dienst 511a übergebenen Steuerungsausgänge werden vom E/A-Dienst 511a über den E/A-Kanal 540 an das/die Feldgerät(e) 531 weitergeleitet. Die Container 515a und b, die Steuerungsdienste 521a und b, die Routinedienste 525a und b und die E/A-Kanäle 544a und b sind dagegen „inaktiv“. Infolgedessen leitet der E/A-Serverdienst 511a die Steuerungsausgänge der Routinedienste 525a und b nicht an das/die Feldgerät(e) 531 weiter.

[0160] Wie bereits erwähnt, erleichtert der E/A-Serverdienst 561a die Steuerung des Bereichs 502 in ähnlicher Weise, wie dies für den E/A-Dienst 511a und den Bereich 501 beschrieben wurde. Der Dienst 561a fungiert beispielsweise als Vermittlungsknoten zwischen: (i) einer Reihe von Feldgeräten 581 und 582 und 583 und (ii) containerisierten Steuerungsdiensten 571a und 571b, auf denen die Instanzen 575a und 575b derselben Steuerungsroutine #2 laufen, um dieselbe Reihe von Feldgeräten 581 und 582 und 583 zu steuern und so den Bereich 502 der Anlage 10 zu steuern. Der E/A-Serverdienst 561a kann die containerisierten Steuerungsdienste auswerten, einen „aktiven“ Dienst auswählen und die Steuerungsausgänge des aktiven Dienstes verwenden, um den Satz von Feldgeräten zu steuern (und damit die Steuerung des Prozesses zu implementieren).

[0161] Es versteht sich von selbst, dass die in **Fig. 15** gezeigten Container auf physische Ressourcen in der Anlage 10 oder anderswo in beliebiger Weise verteilt sein können. Beispielsweise können die Container 515 und 505 für den Bereich 501 auf Computern in der Nähe oder innerhalb des Bereichs 501 implementiert werden, und die Container 555 und 565 für den Bereich 502 können auf Computern in der Nähe oder innerhalb des Bereichs 502 implementiert werden. Einige oder alle Container 505

und/oder 515 können jedoch auch auf Computern in der Nähe oder im Bereich 502 implementiert werden und/oder einige oder alle Container 555 und/oder 565 können auch in der Nähe oder im Bereich 501 implementiert werden, falls gewünscht. Man kann aber auch einen oder mehrere der vorgenannten Container auf Computern in anderen Bereichen der Anlage 10 oder an einem von der Anlage 10 entfernten Standort implementieren (was besonders nützlich sein kann, um einen nahtlosen Übergang im Falle von Energieausfällen oder anderen Störungen in der Anlage 10 zu gewährleisten). Darüber hinaus ist keiner der oben genannten Container notwendigerweise dauerhaft an den Computer-Cluster oder Knoten/Server gebunden, auf dem er gerade ausgeführt wird. Container können dynamisch (z.B. in oder nahezu in Echtzeit, während der Ausführung) instanziiert, gelöscht und auf verschiedenen Computern neu instanziiert werden, wenn dies gewünscht wird, um Rechen- und Netzwerklasten auszugleichen und Ineffizienzen bei der Berechnung oder im Netzwerk zu beseitigen (z.B. wenn eine bestimmte physische Ressource Computerisch oder durch Netzwerkverkehr übermäßig belastet wird). Außerdem kann die Gesamtzahl der Instanzen eines bestimmten Containers je nach Bedarf dynamisch reduziert oder erhöht werden. Wenn beispielsweise die physischen Ressourcen, die die Steuerungscontainer 565a und 565b implementieren, übermäßig belastet zu sein scheinen, kann ein dritter Steuerungscontainer für den Dienst Steuerung #2 auf einem neuen Computer oder einer neuen physischen Ressource instanziiert werden (und, falls gewünscht, kann der dritte Container aktiviert werden). Der E/A-Serverdienst 561a kann dann die drei Container für den Dienst Steuerung #2 weiter überwachen und kontinuierlich den jeweils leistungsstärksten Container aktivieren. Dieses „Jonglieren“ zwischen den Containern kann hilfreich sein, wenn die Rechen- und Netzwerkauslastung der physischen Ressourcen sehr unterschiedlich ist. Jeder Steuerungsdienst kann in einem eigenen Container untergebracht werden, wodurch eine relativ isolierte, konsistente und vorhersehbare Umgebung geschaffen wird, in der jeder Steuerungsdienst implementiert wird, unabhängig von der breiteren Softwareumgebung auf dem Knoten, der die Container implementiert. Ein Container kann zum Beispiel Software-Abhängigkeiten und Software-Bibliotheken beinhalten, die für einen bestimmten Steuerungsdienst benötigt werden. Ohne Container wäre es möglicherweise erforderlich, jeden einzelnen Knoten, auf dem der Steuerungsdienst ausgeführt wird, ordnungsgemäß zu konfigurieren, um eine konsistente Umgebung für den Steuerungsdienst zu gewährleisten. Und wenn ein bestimmter Knoten in der Lage sein muss, verschiedene Arten von Diensten zu implementieren (die unterschiedliche Umgebungsanforderungen haben können), kann die Gewährleistung einer ordnungsgemäßen Konfiguration des Knotens komplex werden. Im Gegensatz dazu ermöglichen die beschriebenen Steuerungsdienstcontainer die einfache Instanziierung jedes Steuerungsdienstes an jedem beliebigen Knoten und die einfache Verschiebung zwischen Knoten/Servern oder Rechenclustern.

[0162] Obwohl sich die obige Diskussion auf Steuerungsdienstcontainer bezieht, die an jedem beliebigen Knoten instanziiert und zwischen Knoten/Servern oder Rechenclustern verschoben werden können, lassen sich die Konzepte und Techniken auch auf andere Arten von Steuerungsdiensten 235 anwenden, wie z.B. Steuerungsmoduldienste und/oder Steuerungsfunktionsblockdienste. Beispielsweise können mehrere Instanzen eines konfigurierten Steuerungsfunktionsblockdienstes auf verschiedenen Prozessorkernen instanziiert und zwischen verschiedenen Prozessorkernen oder sogar verschiedenen Prozessoren verschoben werden, und der aktive E/A-Server kann eine der mehreren Instanzen des konfigurierten Steuerungsfunktionsblockdienstes auswählen und die Ausgabe der ausgewählten Instanz des konfigurierten Steuerungsfunktionsblockdienstes an jede einer Vielzahl von Instanzen eines konfigurierten Steuerungsmoduldienstes für den Betrieb darauf liefern. In ähnlicher Weise kann der aktive E/A-Server eine der mehreren Instanzen des konfigurierten Steuerungsmodul-Dienstes auswählen und die Ausgabe der ausgewählten Instanz des konfigurierten Steuerungsmodul-Dienstes an jede Instanz des konfigurierten Steuerungsdienstes weitergeben.

[0163] In jedem Fall kann jeder E/A-Kanal 540-544c und 570-574b so konfiguriert werden, dass er eine bestimmte Variable oder einen Satz von Variablen überträgt (siehe **Fig. 15**). Zum Beispiel kann das Feldgerät 531 ein Ventil sein, und der E/A-Kanal 540 kann so konfiguriert sein, dass er immer einen Ventilbefehl (z.B. eine gewünschte Ventilstellung) überträgt. In manchen Instanzen sind ein oder mehrere E/A-Kanäle so konfiguriert, dass sie eine bestimmte Primärvariable (z.B. eine gewünschte Ventilstellung) und eine oder mehrere Sekundärvariablen (z.B. einen Ventilzustandsindex, eine erkannte Ventilstellung, einen gemessenen Durchfluss, eine gemessene Belastung eines Aktuators usw.) übertragen. In jedem Fall könnte man beispielsweise den E/A-Kanal 540 als Steuerungsausgang 540 bezeichnen.

[0164] **Fig. 16** ist ein Blockdiagramm eines Computerclusters 601 mit mehreren Knoten oder physischen Ressourcen (z.B. Computern, Servern, Netzwerkgeräten usw.), auf denen einer oder mehrere der verschiedenen hier beschriebenen Container, Mikrocontainer, Dienste und/oder Routinen implementiert, dynamisch zugewiesen und die Last ausgeglichen werden kann, um die Nutzung und Leistung der Computerressourcen zu optimieren. Insbesondere

kann der Cluster 601 physische Server 602 und 604 beinhalten, die so konfiguriert sind, dass sie einen oder mehrere der in **Fig. 15** dargestellten Container 515, 505, 555 und/oder 565 implementieren.

[0165] Bei jedem der Server 602 und 604 kann es sich um ein beliebiges geeignetes Computergerät handeln, beispielsweise einen Prozessor, einen Speicher und eine Kommunikationsschnittstelle, und jeder Server kann an einem beliebigen geeigneten Ort innerhalb oder außerhalb der Anlage 10 angeordnet sein. **Fig. 17** zeigt zum Beispiel eine beispielhafte Ausführungsform 700 des Servers 602 (manchmal auch als System/Server/Gerät 700 bezeichnet). Wie dargestellt, beinhaltet der Server 700 einen Prozessor 702, einen Speicher 704 und eine Kommunikationsschnittstelle 706. Die Komponenten des Servers 700 können in jedem geeigneten Gehäuse untergebracht werden (nicht gezeigt).

[0166] Während die Abbildung einen einzelnen Prozessor 702 zeigt, kann der Server 700 in verschiedenen Ausführungsformen mehrere Prozessoren 702 beinhalten. In diesem Beispiel kann der Prozessor 702 den Container 505a, den E/A-Serverdienst 511a und/oder die E/A-Logik 711 (z.B. einschließlich der Logik zur Durchführung der hier beschriebenen E/A-Serveroperationen oder -funktionen) implementieren. Der Prozessor 702 kann auch andere Container 715 implementieren (z.B. einen der anderen Container, die in den **Fig. 1**, **Fig. 2**, **Fig. 15** oder **Fig. 16** gezeigt werden). Falls gewünscht, kann eine beliebige Anzahl von Containern 505 und/oder 715 instanziiert und auf dem Server 700 implementiert werden (z.B. während der Laufzeit bei Lastausgleichsoperationen).

[0167] Der Speicher 704 kann Software und/oder maschinenlesbare Anweisungen speichern, wie die Container 505 und 715, die vom Prozessor 702 ausgeführt werden können. Der Speicher 704 kann flüchtige und/oder nicht-flüchtige Speicher oder Festplatten mit nicht-übertragbaren computerlesbaren Medien („CRM“) zum Speichern von Software und/oder maschinenlesbaren Anweisungen beinhalten.

[0168] Der Server 700 beinhaltet eine oder mehrere Kommunikationsschnittstellen 706, die so konfiguriert sind, dass der Server 700 beispielsweise mit einem anderen Gerät, System, Hostsystem oder einer anderen Maschine kommunizieren kann. Die Kommunikationsschnittstelle 706 kann eine Netzwerkschnittstelle beinhalten, die die Kommunikation mit anderen Systemen über ein oder mehrere Netzwerke ermöglicht (z.B. die Kommunikation des Servers 700 mit dem Server 604). Die Kommunikationsschnittstelle 706 kann jede geeignete Art von drahtgebundener und/oder drahtloser Netzwerkschnittstelle(n) beinhalten, die so konfiguriert ist/sind, dass sie in Übereinstimmung mit einem oder mehreren geeigneten Protokoll(en) arbeiten. Zu den Beispielschnittstellen gehören eine TCP/IP-Schnittstelle, ein Wi-Fi™-Transceiver (gemäß den Standards der I19E 802.11-Familie), ein Ethernet-Transceiver, ein Mobilfunknetz-Funkgerät, ein Satellitennetz-Funkgerät, ein Koaxialkabelmodem, ein drahtloses HART-Funkgerät oder jede andere geeignete Schnittstelle, die ein beliebiges Kommunikationsprotokoll oder einen beliebigen Standard implementiert.

[0169] Zurück zu **Fig. 16**: Jeder der Knoten oder Server 602 oder 604 kann ähnliche Komponenten beinhalten wie der in **Fig. 17** gezeigte Server 700. Wie in **Fig. 16** dargestellt, sind die Container 505 und 515 auf die Server 602 und 604 verteilt. Es ist zu beachten, dass die Steuerungsdienste 521 konzeptionell als eine einzige „Steuerung“ bezeichnet werden können. Das heißt, wenn man von „Steuerung #1“ spricht, bezieht man sich auf die Gruppe von Containern 515, die die Steuerungsdienste 521 implementieren, die wiederum jeweils Instanzen 525 desselben Steuerungs-Routinedienstes #1 zur Steuerung desselben Gerätesatzes ausführen. Da ein Orchestrator und/oder der E/A-Serverdienst 511a die Anzahl der vorhandenen containerisierten Steuerungsdienste 521 dynamisch ändern kann, und da sie dynamisch ändern können, welcher containerisierte Steuerungsdienst 521 zu einem bestimmten Zeitpunkt aktiv ist, und da sie ändern können, welche physischen Server die containerisierten Steuerungsdienste 521 zu einem bestimmten Zeitpunkt implementieren, bezieht sich ein Verweis auf „Steuerung #1“ nicht notwendigerweise auf ein bestimmtes Gerät oder einen bestimmten Container. Besser gesagt, das bestimmte Gerät und der bestimmte Container, die „Container 1“ repräsentieren, können sich zu verschiedenen Zeiten unterscheiden, abhängig von verschiedenen Lastausgleichsoperationen und Entscheidungen, die vom E/A-Serverdienst 511a und von einem Orchestratordienst getroffen werden. In jedem Fall können die in **Fig. 16** gezeigten Container und Server in beliebiger Weise auf physische Ressourcen und Standorte in der Anlage 10 verteilt werden.

[0170] Die Feldgeräte 631 können mit einem oder mehreren der Container 505 und/oder 515 auf die gleiche Weise kommunizieren wie die in **Fig. 15** gezeigten Feldgeräte 531 und 532 und können auf ähnliche Weise konfiguriert werden. Wie in **Fig. 6** gezeigt, können die Feldgeräte 631 über physische E/A-Module oder -Karten 614 und einen Netzwerkschalter 612 mit dem Cluster 601 kommunizieren.

[0171] Bei den E/A-Modulen oder -Karten 614 kann es sich um jede geeignete E/A-Karte handeln (manchmal auch „E/A-Geräte“ oder „E/A-Module“ genannt). Die E/A-Karten 614 befinden sich typischerweise in der Asset-Umgebung und fungieren

als Vermittlungsknoten zwischen Steuerungsdiensten und einem oder mehreren Feldgeräten, die die Kommunikation dazwischen ermöglichen. Die Ein- und Ausgänge von Feldgeräten sind manchmal entweder für analoge oder diskrete Kommunikation konfiguriert. Um mit einem Feldgerät zu kommunizieren, benötigt eine Steuerung oder ein Steuerungsdienst oft eine E/A-Karte, die für den gleichen Typ von Ein- oder Ausgang konfiguriert ist, den das Feldgerät verwendet. Das heißt, für ein Feldgerät, das so konfiguriert ist, dass es analoge Steuersignale (z.B. ein 4-20 mA-Signal) empfängt, benötigt die/der entsprechende Steuerung oder Steuerungsdienst möglicherweise eine E/A-Karte mit analogem Ausgang (AO), um das entsprechende Steuersignal zu übertragen. Und für ein Feldgerät, das so konfiguriert ist, dass es Messungen oder andere Informationen über ein analoges Signal überträgt, benötigt die Steuerung oder der Steuerungsdienst möglicherweise eine analoge Eingangskarte (AI), um die übertragenen Informationen zu empfangen. In ähnlicher Weise kann für ein Feldgerät, das für den Empfang diskreter Steuersignale konfiguriert ist, die Steuerung oder der Steuerungsdienst eine diskrete Ausgabe (DO) E/A-Karte benötigen, um das entsprechende Steuersignal zu übertragen; und für ein Feldgerät, das für die Übertragung von Informationen über ein diskretes Signal konfiguriert ist, kann die Steuerung oder der Steuerungsdienst eine diskrete Eingabe (DI) E/A-Karte benötigen. Im Allgemeinen kann jede E/A-Karte an mehrere Feldgeräteingänge oder -ausgänge angeschlossen werden, wobei jede Kommunikationsverbindung zu einem bestimmten Eingang oder Ausgang als „Kanal“ bezeichnet wird. Zum Beispiel kann eine DO E/A-Karte mit 120 Kanälen mit 120 verschiedenen diskreten Feldgeräteingängen kommunikativ verbunden sein, so dass die Steuerung (über die DO E/A-Karte) diskrete Steuerungsausgangssignale an die 120 verschiedenen diskreten Feldgeräteingänge übertragen kann. In einigen Fällen ist/sind eine oder mehrere der E/A-Karten 614 rekonfigurierbar, so dass die Kommunikation mit einem Feldgerät möglich ist, das für eine beliebige Art von E/A konfiguriert ist (z.B. für AI, AO, DO, DI, etc.). Einige Feldgeräte sind nicht für die Kommunikation über E/A-Karten konfiguriert. Solche Geräte können dennoch an die im E/A-Subsystem 500 dargestellten Steuerungsdienste angeschlossen werden. Einige Feldgeräte kommunizieren beispielsweise über einen Ethernet-Anschluss und eine Verbindung mit Steuerungen oder Steuerungsdiensten. Einige Feldgeräte kommunizieren mit Steuerungen oder Steuerungsdiensten über ein beliebiges geeignetes drahtloses Protokoll.

[0172] In jedem Fall kommunizieren die E/A-Karten 614 mit den Feldgeräten 631 über ein bestimmtes Prozesssteuerungsprotokoll (z.B. HART) und können mit dem Cluster 601 über jedes andere geeignete Protokoll (z.B. TCP/IP) kommunizieren. Die E/A-Karten 614 leiten Nachrichten an den Netzwerkschalter 612 weiter und empfangen Nachrichten von ihm. Bei dem Netzwerkschalter 612 kann es sich um jeden geeigneten Netzwerkschalter handeln, der so konfiguriert ist, dass er Nachrichten zwischen dem Computercluster 601 und den Feldgeräten 631 weiterleitet oder weitergibt. In einigen Fällen können eine oder mehrere der E/A-Karten 614 Mikrocontainer implementieren, die E/A-Kartendienste implementieren. Wenn also ein bestimmtes E/A-Karten-Gerät ausfällt und durch ein neues E/A-Karten-Gerät ersetzt wird, kann es mit dem E/A-Karten-Microcontainer geladen und dadurch schnell auf die gleiche Weise konfiguriert werden wie das vorherige E/A-Karten-Gerät. In diesem System könnte ein physischer E/A-Server beispielsweise über eine aktive E/A-Karte und zusätzlich über eine inaktive E/A-Karte verfügen, die mit den entsprechenden Mikrocontainern bereitsteht, um im Falle eines Ausfalls der aktiven E/A-Karte schnell zu übernehmen. Die aktive E/A-Karte sendet empfangene Eingabedaten von angeschlossenen Geräten an die Backup-E/A-Karte, und zwar in ähnlicher Weise, wie die „aktiven“ und „inaktiven“ E/A-Server-Container zuvor funktionierten. Wichtig ist, dass in diesem Fall sowohl die ‚aktive‘ als auch die ‚inaktive‘ E/A-Karte (bei der es sich z.B. um eine typische oder bekannte Schienenbuskarte oder eine Emerson CHARM E/A-Karte handeln könnte) physisch mit dem logischen E/A-Server verbunden sein müssen, damit die ‚inaktive‘ Karte als ‚aktive‘ Karte fungieren und anfangen kann, E/A-Daten vom logischen E/A-Server zu empfangen. Ein Beispiel für einen Microcontainer wäre eine extrem leichtgewichtige Containerisierungstechnik, die als „Jail“ bezeichnet wird. Dabei handelt es sich um einen in der Branche bekannten Kunstbegriff, bei dem das Betriebssystem einen Microdienst in einer Sandkisten-Umgebung isoliert.

[0173] In einigen Fällen kann der Netzwerkschalter 612 containerisiert werden. Der Container kann die Logik beinhalten, auf die sich der Schalter 612 stützt. Diese Logik kann eine Routing-Tabelle mit Routen zu Adressen für Feldgeräte, E/A-Karten (oder E/A-Karten-Container) und/oder Steuerungsdienste beinhalten. Die Logik kann eine Weiterleitungstabelle beinhalten, die solche Adressen den Ports des Switches zuordnet (z.B. mit oder ohne Kenntnis des Weges zu der Adresse). Durch die Containerisierung der Logik des Switches kann der Netzwerkschalter 612 auf jeder gewünschten und geeigneten Hardware instanziiert werden, so dass die Switch-Hardware schnell für jede gewünschte Switch-/Routing-Operation konfiguriert und rekonfiguriert werden kann (z.B. für den Fall, dass das physische Gerät für den Netzwerkschalter 612 ersetzt wird).

[0174] In einer Ausführungsform kann jeder geeignete Container, Microcontainer oder E/A dem Computercluster 601 zugewiesen werden und je nach

Ressourcenverfügbarkeit entweder dem Server 602 oder dem Server 604 dynamisch zugewiesen und dort instanziiert werden. Diese dynamische Lastverteilung und Ressourcenzuweisung ermöglicht es dem Steuerungssystem, schnell auf sich ändernde Verarbeitungslasten, Ressourcenverfügbarkeit, Netzwerkbeschränkungen usw. zu reagieren, ohne die Funktionalität zu verlieren.

[0175] Es ist zu beachten, dass das E/A-Subsystem 500, obwohl nicht explizit dargestellt, physische E/A-Karten und/oder einen oder mehrere Netzwerkschalter (z.B. ähnlich denen in **Fig. 16**) beinhalten kann, die als Vermittler zwischen den Feldgeräten (531, 532, 581, 582) und den E/A-Serverdiensten 511a und/oder 561a dienen.

[0176] In einer Ausführungsform, wenn physische oder logische Assets mit dem System verbunden sind, wird der E/A-Serverdienst 505 diese Assets automatisch auflösen und in Betrieb nehmen, sobald sie vom Suchdienst ermittelt werden. Beispielsweise kann ein Feldgerät eine eindeutige Feldgerätekennung haben, und das Steuerungssystem kann so konfiguriert sein, dass es das Feldgerät mit einem oder mehreren variablen Tags verknüpft (z.B. Befehle repräsentierend, für die das Feldgerät konfiguriert ist, um sie zu empfangen und/oder Parameter repräsentierend, für die das Feldgerät konfiguriert ist, um sie zu übertragen), basierend auf der eindeutigen Feldgerätekennung. Mithilfe dieser eindeutigen Kennung kann das Feldgerät vom Steuerungssystem getrennt und wieder verbunden werden. Das Steuerungssystem kann die Kommunikation zwischen dem Feldgerät und den Steuerungsdiensten, die auf dem Feldgerät beruhen, automatisch weiterleiten, unabhängig davon, welche Hardware die Steuerungsdienste instanziiert und implementiert haben und wo sich diese Hardware geografisch befindet. Jeder Container kann ebenfalls eine eindeutige Kennung haben, die das Routing zwischen den entsprechenden Containern/Diensten ermöglicht, unabhängig davon, welche Hardware die Container instanziiert haben und wo sich diese Hardware geografisch befindet.

[0177] **Fig. 18** ist ein Flussdiagramm eines Verfahrens 800 zur Implementierung eines E/A-Serverdienstes, wie einer der in **Fig. 15-17** gezeigten. Das Verfahren 800 kann ganz oder teilweise von den SDCS 100/200 und/oder dem E/A-Gateway 40, die in den **Fig. 1** und **Fig. 2** dargestellt sind, und insbesondere von den E/A-Serverdiensten 511/61, die in den **Fig. 15-17** dargestellt sind, implementiert werden. Dementsprechend kann das Verfahren 800 als eine oder mehrere Anweisungen oder Routinen in einem Speicher gespeichert werden (z.B. in dem in **Fig. 17** gezeigten Speicher 704). Der Einfachheit halber bezieht sich die Beschreibung von **Fig. 18** auf den Dienst 511a von System 15 als Implementierung des Verfahrens 1800.

[0178] Das Verfahren 800 beginnt in einem Schritt 805, wenn eine Reihe von Feldgeräten oder Prozessausgaben 542a und 542b vom E/A-Serverdienst 511a empfangen werden. Zum Beispiel kann der E/A-Serverdienst 511a vom Feldgerät 532 einen gemessenen Durchfluss von 10 Gallonen pro Minute (gpm) für eine Variable FT002 empfangen.

[0179] In einem Schritt 810 erzeugt der E/A-Serverdienst 511a eine Vielzahl von Sätzen von Steuerungseingängen (z.B. über den E/A-Kanal 543), die jeweils dem empfangenen Satz von Prozessausgaben entsprechen, die über die E/A-Kanäle 542a und 542b empfangen wurden, so dass jeder Satz von Steuerungseingängen denselben Satz von Werten trägt wie jeder andere Satz in der Vielzahl von Sätzen von Steuerungseingängen. Um beim letzten Beispiel zu bleiben, kann jeder Satz von Steuerungseingängen denselben FT002-Parameter mit demselben Wert (z.B. 10 gpm) beinhalten. Zur Veranschaulichung: Der E/A-Serverdienst 511a kann einen ersten Satz von Steuerungseingängen aus dem Satz von Prozessausgängen erzeugen (z.B. kann der Kanal 543a der erste Steuerungseingang für den Steuerungsdienst 521a sein, den Parameter FT002 darstellen und den Wert 10 gpm haben). In ähnlicher Weise kann der E/A-Serverdienst 511a einen zweiten Satz von Steuerungseingängen aus dem Satz von Prozessausgängen generieren (z.B. kann der Kanal 543b einen zweiten Steuerungseingang für den Steuerungsdienst 521b darstellen, kann in ähnlicher Weise den Parameter FT002 darstellen und kann denselben Wert 10 gpm haben).

[0180] In einem Schritt 815 überträgt der E/A-Serverdienst 511a jeden Satz von Steuerungseingängen (z.B. die Sätze 543a-c) an einen anderen aus der Vielzahl der Steuerungsdienste 521a-c. Wie in **Fig. 15** dargestellt, implementiert jeder Steuerungsdienst 521a-c eine andere Instanz derselben Steuerungsroutine #1 (einschließlich der Instanzen 525a-c). Da die Steuerungsroutinen jeweils eine Instanz derselben Routine sind, sind sie alle so konfiguriert, dass sie denselben Satz von Steuerungsausgängen (z.B. denselben Satz von Befehlsvariablen) erzeugen, um denselben Bereich 501 der Prozessanlage 10 über die Feldgeräte 531 und 532 auf der Grundlage desselben Satzes von Werten für denselben Satz von Steuerungseingängen zu steuern. Es ist zu beachten, dass es eine beliebige Anzahl von containerisierten Steuerungsdiensten geben kann, und dass für jeden containerisierten Steuerungsdienst ein Satz von Steuerungseingängen (die jeweils den/-die gleichen Parameter und Werte haben) verwendet werden kann.

[0181] In einem Schritt 820 empfängt der E/A-Serverdienst 511a eine Vielzahl von Sätzen von Steuerungsausgängen über die E/A-Kanäle 544a-c, wobei jeder Satz von einem anderen der Vielzahl von Steuerungsdiensten 521a-c stammt.

[0182] In einem Schritt 825 analysiert der E/A-Serverdienst 511a die Vielzahl von Sätzen von Steuerungsausgänge, die über die E/A-Kanäle 544a-c empfangen wurden, und/oder die mit den Sätzen verbundenen Metadaten (z.B. Latenzinformationen). Insbesondere kann eine QoS-Metrik für jeden Satz analysiert werden und ein Satz mit der besten QoS-Metrik kann identifiziert werden. Bei der QoS-Metrik kann es sich um eine beliebige Metrik zur Analyse der Qualität der von den containerisierten Steuerungsdiensten erbrachten Dienste handeln, z.B. Latenz, Genauigkeit usw.

[0183] In einem Schritt 830 wählt der E/A-Serverdienst 511a auf der Grundlage der Analyse einen aktiven Satz von Steuerungsdiensten aus. In einer Ausführungsform aktiviert der E/A-Serverdienst 511a den aktiven Satz von Steuerungsausgängen auf der Grundlage der Analyse. Zum Beispiel kann der Dienst 511a den Satz 544c auf der Grundlage von QoS-Metriken aktivieren, die mit jedem Container 515a-c verbunden sind. Der Dienst 511a kann z.B. den Container oder den Steuerungsdienst mit der niedrigsten Latenz auswählen. In einer Ausführungsform aktiviert der Dienst einen bestimmten Container, Server oder Kanal, nachdem sich eine Art Konsens gebildet hat. Zum Beispiel kann er den ersten Container, Server oder Kanal aktivieren, für den ein zweiter Container die gleichen Werte für den Satz von Steuerungsdiensten 544a-c liefert. In einem Beispiel aktiviert der Dienst 511a einen Container/Steuerungsdienst/Kanal nach einem Best-of-n-Abstimmungsschema. In einer Ausführungsform führt ein anderer Dienst, z.B. ein Orchestratordienst, den Schritt 830 anstelle des Dienstes 511a aus.

[0184] In einigen Fällen kann der E/A-Serverdienst 511a den Status eines oder mehrerer der Steuerungsausgänge 544a-c bestätigen (z. B. vor oder nach der Auswahl eines aktiven Containers). So kann der Dienst 511a beispielsweise verifizieren, ob die Ausgänge kürzlich aktualisiert wurden und nicht veraltet sind. Dies kann zumindest teilweise durch den Abgleich mindestens eines Satzes 544a-c der Ausgänge mit einem anderen der Sätze 544a-c erfolgen.

[0185] In einem Schritt 835 überträgt der E/A-Serverdienst 511a den aktiven Satz von Steuerungsausgängen (z.B. einschließlich eines Befehls zum Öffnen oder Schließen eines Ventils) an die Feldgeräte 531, um einen Prozessausgang (z.B. eine vom Status des manipulierten Ventils abhängige Durchflussmenge) des industriellen Prozesses zu steuern und dadurch den bestimmten Bereich 501 des industriellen Prozesses zu steuern.

[0186] Der E/A-Serverdienst 511a kann Signale, die Steuerungseingänge oder Steuerungsausgänge beinhalten, auf jede geeignete Weise konditionieren, bevor er die Steuerungseingänge oder -ausgänge von einem Feldgerät an einen Steuerungsdienst (oder umgekehrt) weiterleitet. Der E/A-Serverdienst 511a kann analoge Aufbereitungstechniken und/oder digitale Signalaufbereitungstechniken implementieren. Beispiele für analoge Signalaufbereitungstechniken, die vom E/A-Serverdienst 511a implementiert werden können, sind Filterung, Verstärkung, Skalierung und Linearisierungstechniken. Beispiele für digitale Aufbereitungstechniken, die vom E/A-Serverdienst 511a implementiert werden können, sind die Konvertierung von Einheiten, die Aufzählung, die Kodierung und das Hinzufügen oder Bearbeiten eines Statuswertes zu einem Signal. Eine Charakterisierungs- oder Linearisierungsfunktion kann vom E/A-Serverdienst 511a entweder während der analogen oder digitalen Aufbereitung implementiert werden.

[0187] **Fig. 19** ist ein Flussdiagramm eines Verfahrens 900 zur Auswertung und zum Übergang zwischen containerisierten Steuerungsdiensten (oder entsprechenden E/A-Kanälen), wie z.B. einem der in **Fig. 15-17** gezeigten. Das Verfahren 900 kann ganz oder teilweise von den SDCS 100/200 und/oder dem E/A-Gateway 40, die in den **Fig. 1** und **Fig. 2** dargestellt sind, und insbesondere von den E/A-Serverdiensten 511/61, die in den **Fig. 15-17** dargestellt sind, implementiert werden. Dementsprechend kann das Verfahren 900 als eine oder mehrere Anweisungen oder Routinen in einem Speicher gespeichert werden (z.B. in dem in **Fig. 17** gezeigten Speicher 704). Der Einfachheit halber bezieht sich die Beschreibung von **Fig. 19** auf den Dienst 511a von System 15 als Implementierung des Verfahrens 1900.

[0188] In einem Schritt 905 empfängt der E/A-Serverdienst 511 a Prozesssteuerungsverkehr über eine Vielzahl von E/A-Kanälen 544a-c.

[0189] In einem Schritt 910 identifiziert der E/A-Serverdienst 511a einen ersten E/A-Kanal (z.B. 544c), der aktiv ist. Wie in **Fig. 5** dargestellt, sind der Dienst 521c und der E/A-Kanal 544c aktiv, während die Dienste 521a/b und die E/A-Kanäle 544a/b inaktiv sind. In einer Ausführungsform aktiviert der E/A-Serverdienst 511a den aktiven Dienst 544c.

[0190] In einem Schritt 915 verwendet der E/A-Serverdienst 511a den Prozesssteuerungsverkehr des aktiven E/A-Kanals 544c, um ein oder mehrere Feldgeräte zu steuern. Beispielsweise kann der Dienst 511a in Übereinstimmung mit der Beschreibung des

Verfahrens 800 den empfangenen Steuerverkehr (z.B. einschließlich Steuerungsausgänge oder -befehle) über einen E/A-Kanal 540 an das Feldgerät weiterleiten.

[0191] In einem Schritt 920 wertet der E/A-Serverdienst 511a eine QoS-Metrik für jeden E/A-Kanal 544a-c der Steuerungsdienste aus. Wie bereits erwähnt, kann es sich bei der QoS-Metrik um eine beliebige Metrik zur Analyse der Qualität der von den containerisierten Steuerungsdiensten erbrachten Dienstleistung handeln, wie z.B. Latenz, Genauigkeit, usw.

[0192] In einem Schritt 925 bestimmt der E/A-Serverdienst 511 a, ob die höchste oder beste QoS-Metrik einem inaktiven Kanal entspricht oder nicht. Wenn dies nicht der Fall ist (d.h. wenn sie dem momentan aktiven E/A-Kanal oder Steuerungscontainer entspricht), behält der E/A-Serverdienst 511a den momentan aktiven E/A-Kanal bei (Schritt 930) und kehrt zum Schritt 910 zurück. Wenn die höchste oder beste QoS-Metrik einem aktiven Kanal entspricht, kann der E/A-Serverdienst 511a alternativ in einem Schritt 935 den inaktiven Kanal mit der höchsten oder besten QoS als den aktiven E/A-Kanal bestimmen. Der E/A-Serverdienst 511a kehrt dann zum Schritt 910 zurück.

[0193] In einer Ausführungsform verfolgt jeder Steuerungsdienst, wo sich jede Steuerungsroutine im Prozess der Ausführung der Steuerungsroutine befindet. Die Steuerungsroutine kann z.B. in Phasen oder Stufen unterteilt sein, so dass die Steuerungsroutinen für einen Übergang zwischen den Steuerungsdiensten synchronisiert werden können. In einer Ausführungsform werden die Steuerungsdienste im Gleichschritt oder relativen Gleichschritt ausgeführt. Beispielsweise kann jeder Steuerungsdienst nach der Ausführung einer bestimmten Phase anhalten und warten, bis die anderen Steuerungsdienste (oder eine bestimmte Anzahl von Containerdiensten) die Ausführung derselben bestimmten Phase beendet haben, bevor sie mit dem nächsten Zustand oder der nächsten Phase der Steuerungsroutine beginnen. Diese „Lockstep“-Ausführung kann in Situationen von Vorteil sein, in denen die Prozesssicherheit eine Rolle spielt.

[0194] Wie bereits in **Fig. 2** erwähnt, kann der SD-Netzwerkdienst 220 das logische oder virtuelle Netzwerk, das vom logischen Prozesssteuerungssystem 245 genutzt wird, verwalten und managen, das vom SD-Netzwerkdienst 220 über den physischen Knoten 208 implementiert werden kann. Der SD-Netzwerkdienst 220 kann im SDCS 200 Instanzen von Netzwerk-Geräte, wie z.B. virtuelle Router, virtuelle Firewalls, virtuelle Switches, virtuelle Schnittstellen, virtuelle Datendioden, usw., und Instanzen von Netzwerkdiensten, wie z.B. Paketprüfdienste, Zugriffs-Steuerungsdienste, Autorisierungsdienste, Autentifizierungsdienste, Verschlüsselungsdienste, Zertifizierungsautoritätsdienste, Schlüsselverwaltungsdienste, usw., einrichten und verwalten. Die Netzwerkdienste können als Dienste oder Microdienste implementiert werden.

[0195] Darüber hinaus kann der SD-Netzwerkdienst 220 Container, die die Sicherheitsanwendungen/-dienste ausführen, in andere Container einbetten, die andere Arten von Diensten ausführen. Zum Beispiel kann der SD-Netzwerkdienst 220 einen Sicherheitscontainer in einem Steuerungscontainer verschachteln, um Sicherheitsdienste im Zusammenhang mit der Steuerungsfunktionalität auszuführen. Der SD-Netzwerkdienst 220 kann auch Container, die Sicherheitsanwendungen/-dienste ausführen, in anderen Containern verschachteln, die Sicherheitsanwendungen/-dienste ausführen. Zum Beispiel kann der SD-Netzwerkdienst 220 einen Firewall-Container und einen Smart-Switch-Container innerhalb eines Router-Containers verschachteln.

[0196] Darüber hinaus kann der SD-Netzwerkdienst 220 N redundante Instanzen von Containern bereitstellen, die die Sicherheitsgeräte/-dienste innerhalb des SDCS 200 ausführen. Zum Beispiel kann der SD-Netzwerkdienst 220 eine erste Instanz eines Firewall-Containers einsetzen, um eingehende Datenpakete zu empfangen und ausgehende Datenpakete zu übertragen, und eine zweite Instanz des Firewall-Containers, um die eingehenden Datenpakete zu empfangen und ausgehende Datenpakete zu übertragen. Der SD-Netzwerkdienst 220 kann sowohl die erste als auch die zweite Instanz des Firewall-Containers einsetzen, um eingehende Datenpakete aus derselben Quelle (z.B. einem Steuerungsdienst) zu empfangen. Während jedoch die erste Instanz des Firewall-Containers die ausgehenden Datenpakete an ein entferntes System außerhalb des SDCS 200 weiterleiten kann, konfiguriert der SD-Netzwerkdienst 220 die zweite Instanz der Firewall nicht für die Weiterleitung der ausgehenden Datenpakete an das entfernte System. Stattdessen kann der SD-Netzwerkdienst 220 die zweite Instanz der Firewall so konfigurieren, dass sie die ausgehenden Datenpakete an ein Überwachungssystem innerhalb des SDCS 200 übermittelt oder dass sie dem Überwachungssystem innerhalb des SDCS 200 mitteilt, wie die eingehenden Datenpakete behandelt wurden. Auf diese Weise kann der SD-Netzwerkdienst 220 überwachen, ob die Firewall-Funktionalität ordnungsgemäß funktioniert.

[0197] **Fig. 20** zeigt ein Blockdiagramm mit Beispielen von Containern, Diensten und/oder Subsystemen, die mit der Netzwerksicherheit zusammenhängen. Wie in **Fig. 20** gezeigt, beinhaltet das SDCS einen Container, in dem ein Netzwerkdienst 1002

ausgeführt wird, der dem in **Fig. 2** gezeigten SD-Netzwerkdienst 220 ähnelt. Der Netzwerkdienst 1002 setzt eine erste Instanz eines Router-Containers 1004 und eine zweite Instanz eines Router-Containers 1006 ein und verwaltet sie. Der erste Router-Container 1004 führt einen ersten Sicherheitsdienst 1008 aus und der zweite Router-Container 1006 führt einen zweiten Sicherheitsdienst 1010 aus. Der Netzwerkdienst 1002 kann den ersten Router-Container 1004 einsetzen, um eine Verbindung zu einem erste-Einheit-Container 1012 mit einem ersten Tank-Container 1014 und einem ersten Steuer-Container 1016 herzustellen. Der Netzwerkdienst 1002 kann den ersten Router-Container 1004 auch einsetzen, um eine Verbindung zu einem ersten E/A-Server-Container 1018 herzustellen. Auf diese Weise kann der erste Router-Container 1004 die Kommunikation zwischen dem erste-Einheit-Container 1012 und dem ersten E/A-Server-Container 1018 erleichtern. Der erste Sicherheitsdienst 1008 kann einen ersten Satz von Sicherheitsregeln für das Routing der Kommunikation zwischen dem erste-Einheit-Container 1012 und dem ersten E/A Server Container 1018 beinhalten.

[0198] Der Netzwerkdienst 1002 kann den zweiten Router-Container 1006 einsetzen, um eine Verbindung zu einem zweite-Einheit-Container 1020 herzustellen, der einen ersten Mischer-Container 1022 und einen zweiten Steuer-Container 1024 hat. Der Netzwerkdienst 1002 kann den zweiten Router-Container 1006 auch einsetzen, um eine Verbindung zu einem zweiten E/A-Server-Container 1026 herzustellen. Auf diese Weise kann der zweite Router-Container 1006 die Kommunikation zwischen dem erste-Einheit-Container 1020 und dem zweiten E/A-Server-Container 1026 erleichtern. Der zweite Sicherheitsdienst 1010 kann einen zweiten Satz von Sicherheitsregeln für das Routing der Kommunikation zwischen dem zweite-Einheit-Container 1020 und dem zweiten E/A Server Container 1026 beinhalten.

[0199] Das SDCS kann auch einen Container beinhalten, der einen Zertifizierungsautoritätsdienst 1028 ausführt. Zusätzlich kann das SDCS physische oder logische Assets der Prozessanlage 10 beinhalten, die während der Laufzeit der Prozessanlage 10 genutzt werden können, um mindestens einen Bereich des industriellen Prozesses zu steuern, wie z.B. Feldgeräte, Steuerungen, Prozesssteuerungseinrichtungen, E/A-Geräte, Rechenknoten, Container, Dienste (z.B. Steuerungsdienste), Microdienste, etc. Die physischen oder logischen Assets können beim Zertifizierungsautoritätsdienst 1028 digitale Zertifikate anfordern, um ihre Authentizität bei der Kommunikation im SDCS nachzuweisen, z.B. Public Key Infrastructure (PKI) Zertifikate. Wenn ein physisches oder logisches Asset ein Zertifikat anfordert, erhält der Zertifizierungsautoritätsdienst 1028 Identifizierungsinformationen für das physische oder logische Asset und prüft die Identität des physischen oder logischen Assets anhand der Identifizierungsinformationen. Der Zertifizierungsautoritätsdienst 1028 generiert dann ein Zertifikat für das physische oder logische Asset, das einen kryptografischen öffentlichen Schlüssel oder eine andere Kennung für das physische oder logische Asset, eine Kennung für den Zertifizierungsautoritätsdienst 1028 und eine digitale Signatur für den Zertifizierungsautoritätsdienst 1028 beinhalten kann, um zu beweisen, dass das Zertifikat vom Zertifizierungsautoritätsdienst 1028 generiert wurde. Der Zertifizierungsautoritätsdienst 1028 stellt die Zertifikate dem physischen oder logischen Asset zur Verfügung, das die Zertifikate zu Authentifizierungszwecken bei der Kommunikation mit anderen Knoten oder Diensten innerhalb des SDCS verwenden kann. In einigen Implementierungen können die anderen Dienste die Kommunikation mit dem physischen oder logischen Asset mit dem kryptografischen öffentlichen Schlüssel für das physische oder logische Asset verschlüsseln, der in den Zertifikaten beinhaltet ist.

[0200] In einigen Implementierungen kann ein Nutzer innerhalb des SDCS ein digitales Zertifikat vom Zertifizierungsautoritätsdienst 1028 anfordern, z. B. ein Assetbetreiber, ein Konfigurationsingenieur und/oder anderes Personal, das mit der industriellen Prozessanlage 10 verbunden ist. Wenn der Nutzer die digitalen Zertifikate anfordert, kann er Identifikationsdaten wie seinen Namen, seine Adresse, seine Telefonnummer, seine Rolle innerhalb der industriellen Prozessanlage 10, einen Nutzernamen und ein Passwort usw. angeben. Der Zertifizierungsautoritätsdienst 1028 kann die Identität des Nutzers verifizieren, indem er z.B. die vom Nutzer erhaltenen Identifikationsdaten mit Identifikationsdaten des Nutzers vergleicht, die er aus anderen Quellen erhalten hat. Wenn der Zertifizierungsautoritätsdienst 1028 in der Lage ist, den Nutzer zu verifizieren, erzeugt der Zertifizierungsautoritätsdienst 1028 ein digitales Zertifikat und stellt es dem Nutzer zur Verfügung. Auf diese Weise kann der Nutzer das digitale Zertifikat vorlegen, um auf Knoten oder Dienste innerhalb des SDCS zuzugreifen und muss keine Anmeldeinformationen eingeben. In einigen Implementierungen kann der Zertifizierungsautoritätsdienst 1028 Autorisierungsinformationen für den Nutzer in die Zertifikate aufnehmen. Die SDCS kann dem Nutzer eine Autorisierungsstufe zuweisen, die auf der Rolle des Nutzers innerhalb der industriellen Prozessanlage 10 basiert. Der Zertifizierungsautoritätsdienst 1028 kann dann verschiedene Arten von Zertifikaten für verschiedene Autorisierungsstufen und/oder Rollen innerhalb der industriellen Prozessanlage 10 erzeugen. Auf diese Weise können Knoten oder Dienste, auf die der Nutzer zuzugreifen versucht, die Autorisierungsstufe und/oder die Rolle des Nutzers innerhalb der industriellen Prozessan-

lage 10 auf der Grundlage der Art der Zertifikate, die der Nutzer bereitstellt, bestimmen. Der Knoten oder Dienst kann dann auf der Grundlage der Autorisierungsstufe und/oder der Rolle des Nutzers innerhalb der industriellen Prozessanlage 10 feststellen, ob der Nutzer berechtigt ist, auf den Knoten oder Dienst zuzugreifen. In einigen Implementierungen kann der Nutzer je nach Autorisierungsstufe und/oder Rolle des Nutzers innerhalb der industriellen Prozessanlage 10 einen Teilzugriff auf den Knoten oder den Dienst erhalten. Dementsprechend kann der Knoten oder Dienst dem Nutzer den Zugriff auf einige Bereiche des Knotens oder Dienstes ermöglichen und den Zugriff des Nutzers auf andere Bereiche des Knotens oder Dienstes verhindern.

[0201] In einigen Implementierungen kann ein Nutzer durch eine Rolle definiert sein, die durch digitale Zertifikate gesichert ist. Beispielsweise kann eine Prozessmanagerrolle einer ersten Autorisierungsebene mit einem ersten Satz digitaler Zertifikate entsprechen, die sich von einer Betreiberrolle unterscheidet, die einer zweiten Autorisierungsebene mit einem zweiten Satz digitaler Zertifikate entspricht.

[0202] Die Sicherheitsdienste 1008, 1010 sind zwar in den Router-Containern 1004, 1006 beinhaltet, die in **Fig. 20** die Kommunikation zwischen den Steuerungsdiensten und den E/A-Diensten erleichtern, aber das ist nur ein Beispiel für eine Implementierung. Zusätzlich oder alternativ können Sicherheitsdienste in Containern verschachtelt sein, in denen andere Arten von Diensten ausgeführt werden, wie z.B. Steuerungsdienste, E/A-Dienste, etc. **Fig. 21** zeigt ein Blockdiagramm einer zusätzlichen oder alternativen Implementierung des SDCS in **Fig. 20**. Wie in **Fig. 21** dargestellt, setzt der Netzwerkdienst 1002 zusätzlich zum Einsatz eines ersten Sicherheitsdienstes 1008 und eines zweiten Sicherheitsdienstes 1010 innerhalb des ersten bzw. zweiten Router-Containers 1004, 1006 einen dritten Sicherheitsdienst 1102 innerhalb eines Containers (eines Sicherheitscontainers) ein, der in einem ersten Steuerungscontainer 1116 ausgeführt wird, und einen vierten Sicherheitsdienst 1104 innerhalb eines Containers (eines Sicherheitscontainers), der in einem zweiten Steuerungscontainer 1124 ausgeführt wird. Der dritte Sicherheitscontainer 1102 kann Inhalte haben, die Sicherheitsbedingungen definieren, wie z.B. eine Reihe von Sicherheitsregeln. Zusätzlich kann der vierte Sicherheitscontainer 1104 einen Inhalt haben, der Sicherheitsbedingungen definiert, wie z.B. eine Reihe von Sicherheitsregeln, die mit dem Inhalt des dritten Sicherheitscontainers 1102 identisch oder davon verschieden sein können. Der Inhalt kann auch die Steuerstrategie für den entsprechenden Steuerungscontainer beinhalten, wie z.B. die Steuerhistorie und die Speicherung.

[0203] Auf diese Weise kann der dritte Sicherheitsdienst 1102 einen dritten Satz von Sicherheitsregeln beinhalten, die spezifisch für den ersten Steuerungscontainer 1116 sind und nicht notwendigerweise für andere Dienste oder Knoten gelten, die mit dem Router-Container verbunden sind. Darüber hinaus kann der dritte Sicherheitsdienst 1102 die vom ersten Steuerungscontainer 1116 erzeugten Daten verschlüsseln, bevor sie über ein Kommunikationsnetz übertragen werden. Dies kann eine zusätzliche Sicherheitsschicht bieten, bevor die Daten einen Router-Container erreichen. Während die Sicherheitsdienste 1102 und 1104 in **Fig. 21** in Steuerungscontainern verschachtelt sind, können die Sicherheitsdienste in jedem geeigneten Container verschachtelt sein, wie z.B. in E/A-Server-Containern, Containern für Bedienerarbeitsplätze, usw.

[0204] **Fig. 22** zeigt ein detailliertes Blockdiagramm des ersten Router-Containers 1004 aus **Fig. 20**. Der Router-Container kann Sicherheitsanwendungen oder -dienste beinhalten, die in den Router-Container integriert sind. Darüber hinaus kann jede Sicherheitsanwendung oder jeder Dienst weitere Dienste beinhalten, die in ihm verschachtelt sind. Der Router-Container kann einen ersten Firewall-Container 1202 beinhalten, der einen ersten Sicherheitsdienst 1204 ausführt, einen ersten Datendioden-Container 1206, der einen zweiten Sicherheitsdienst 1208 ausführt, einen ersten Smart-Switch-Container 1210, der einen dritten Sicherheitsdienst 1212 ausführt, und einen Paketprüfungsdienst 1214.

[0205] Der erste Sicherheitsdienst 1204 kann einen ersten Satz von Sicherheitsregeln für den ersten Firewall-Container 1202 beinhalten, wie z.B. Whitelists oder Akzeptanzlisten, die den Empfang/ die Übertragung von Daten durch vorbestimmte Knoten oder Dienste erlauben, während andere Verbindungstypen oder Ports verhindert werden. Der erste Satz von Sicherheitsregeln kann nur zulassen, dass autorisierter Datenverkehr vom ersten Router-Container 1004 übertragen wird. Zum Beispiel kann der erste Sicherheitsdienst 1204 verhindern, dass Daten von externen Quellen an die Prozessanlage 10 zu einem Steuerungscontainer gesendet werden.

[0206] Der zweite Sicherheitsdienst 1208 kann den Datenverkehr aus dem SDCS zu einem entfernten System herauslassen und den Datenverkehr (z.B. Daten, die von einem entfernten System oder anderen Systemen übertragen oder gesendet werden) am Eindringen in das SDCS hindern. Dementsprechend unterstützt der zweite Sicherheitsdienst 1208 nur einen unidirektionalen Datenfluss von einem virtuellen Eingangsport zu einem virtuellen Ausgangsport über die Software, z.B. indem er alle am virtuellen Ausgangsport (z.B. von einem entfernten System) empfangenen Nachrichten verwirft oder blockiert und/oder indem er alle an den virtuellen Eingang-

sport adressierten Nachrichten verwirft oder blockiert (z.B. von einem entfernten System an Knoten oder Dienste im SDCS adressiert). Der zweite Sicherheitsdienst 1208 kann auch Daten verschlüsseln, die vom SDCS an ein entferntes System übertragen werden.

[0207] Der dritte Sicherheitsdienst 1208 kann eine Netzwerkadresse für einen Knoten oder Dienst ermitteln, der ein Datenpaket empfangen soll, und kann das Datenpaket über die Netzwerkadresse an den Knoten oder Dienst übertragen. Wenn z.B. ein Steuerungscontainer über den Router-Container Daten an einen E/A-Server-Container sendet, ermittelt der dritte Sicherheitsdienst 1208 die Netzwerkadresse für den E/A-Server-Container und sendet die Daten über die Netzwerkadresse an den E/A-Server-Container. Der dritte Sicherheitsdienst 1208 kann jedem der Knoten oder Dienste, die mit dem Router-Container verbunden sind, Netzwerkadressen zuweisen und kann die Netzwerkadressen ermitteln, die den Knoten oder Diensten zugewiesen sind, die Datenpakete empfangen sollen.

[0208] Der Paketinspektionsdienst 1214 kann ein Muster der Netzwerkdatenströme durch den Router-Container identifizieren, indem er die Paketinhalte untersucht, während sie durch den Router-Container fließen. Der Paketinspektionsdienst 1214 kann dann die bekannten Muster des Datenverkehrs verwenden, um festzustellen, ob ein bestimmter Dienst oder Knoten ein abnormales Verhalten zeigt. Der Paketprüfungsdienst 1214 kann dann Dienste oder Knoten als verdächtig identifizieren und sie einem Nutzer zur Aktion vorschlagen. Der Paketinspektionsdienst 1214 kann auch diagnostische Maßnahmen durchführen, um die wahrscheinliche Ursache für das abnormale Verhalten zu ermitteln. Obwohl der Router-Container in **Fig. 22** einen ersten Firewall-Container 1202, einen ersten Datendioden-Container 1206, einen ersten Smart-Switch-Container 1210 und einen Paketinspektionsdienst 1214 beinhaltet, handelt es sich hierbei nur um eine beispielhafte Implementierung zur Veranschaulichung. Der Router-Container kann alle geeigneten Sicherheitsanwendungen und/oder Dienste beinhalten.

[0209] In einigen Implementierungen kann der Netzwerkdienst mit jedem Steuerungsdienst, der innerhalb des SDCS läuft, Firewall-Dienste bereitstellen. Die Firewall-Dienste können in Containern ausgeführt werden, die in Containern verschachtelt sind, welche die entsprechenden Steuerungsdienste ausführen. In anderen Implementierungen werden die Firewall-Dienste in eigenständigen Containern ausgeführt, die den entsprechenden Steuerungsdiensten zugeordnet sind. Wie in **Fig. 23** dargestellt, setzt der Netzwerkdienst einen ersten Firewall-Container 1302 ein, um den Netzwerkverkehr zu und von einem ersten Steuerungscontainer 1304 zu verwalten, und einen zweiten Firewall-Container 1308, um den Netzwerkverkehr zu und von einem zweiten Steuerungscontainer 1310 zu verwalten. Eine Steuerkonfigurationsdatenbasis 1306, die vom SD Speicherdienst 218 verwaltet werden kann, kann eine erste Steuerkonfiguration für den ersten Steuerungscontainer 1304 bereitstellen. Die Steuerkonfigurationsdatenbasis 13 06 kann dem ersten Firewall-Container 1302 auch einen ersten Satz angepasster Firewall-Regeln für den zugewiesenen ersten Steuerungscontainer 1304 zur Verfügung stellen. Zusätzlich kann die Steuerkonfigurationsdatenbasis 13 06 eine zweite Steuerkonfiguration für den zweiten Steuerungscontainer 1310 bereitstellen. Die Steuerkonfigurationsdatenbasis 13 06 kann dem zweiten Firewall-Container 1308 einen zweiten Satz angepasster Firewall-Regeln für den zugewiesenen zweiten Steuerungscontainer 1310 zur Verfügung stellen. In anderen Implementierungen kommuniziert ein Steuerungskonfigurationsdienst mit der Steuerkonfigurationsdatenbasis1306, um den Steuerungscontainern 1304, 1310 Steuerkonfigurationen und den Firewallcontainern 1302, 1308 angepasste Firewallregeln zur Verfügung zu stellen.

[0210] Der erste Satz von angepassten Firewall-Regeln kann zum Beispiel eine Whitelist oder Akzeptanzliste beinhalten, die es dem ersten Steuerungscontainer 1304 erlaubt, Daten zu einem ersten E/A-Server zu empfangen und zu übertragen, aber es dem ersten Steuerungscontainer 1304 nicht erlaubt, Daten zu/von anderen Knoten oder Diensten zu empfangen oder zu übertragen. In einem anderen Beispiel kann der erste Satz angepasster Firewall-Regeln eine Whitelist oder Akzeptanzliste beinhalten, die es dem ersten Steuerungscontainer 1304 erlaubt, Daten zu einer bestimmten Netzwerkadresse eines entfernten Systems außerhalb des SDCS zu empfangen und zu übertragen. In einem weiteren Beispiel kann der erste Satz angepasster Firewall-Regeln eine Whitelist oder Akzeptanzliste von Diensten oder Knoten beinhalten, die auf Daten aus dem ersten Steuerungscontainer 1304 zugreifen dürfen, und Dienste oder Knoten, die nicht in der Whitelist oder Akzeptanzliste beinhaltet sind, am Zugriff auf die Daten aus dem Steuerungscontainer hindern. Die angepassten Firewall-Regeln können insofern dynamisch sein, als die Firewall-Container 1302, 1308 auf der Grundlage zukünftiger Änderungen der Konfigurationen der Steuer-Container 1304, 1310 andere Firewall-Regeln von einem Steuerungskonfigurationsdienst erhalten können.

[0211] Wie bereits erwähnt, können die hier beschriebenen Sicherheitsdienste Paketprüfdienste, Zugriffs-Steuerungsdienste, Autorisierungsdienste, Autentifizierungsdienste, Verschlüsselungsdienste, Zertifizierungsautoritätsdienste, Schlüsselverwaltungsdienste usw. beinhalten. **Fig. 24** zeigt ein detailliertes Blockdiagramm eines Sicherheitscontainers

1404, der in einen Steuerungscontainer 1402 eingebettet ist, ähnlich der in **Fig. 21** gezeigten Konfiguration. Der Sicherheitscontainer 1404 kann einen Verschlüsselungsdienst 1406, einen Autentifizierungsdienst 1408 und einen Autorisierungsdienst 1410 beinhalten. Auf diese Weise kann der Sicherheitscontainer 1404 die vom Steuerungscontainer 1402 übertragenen Daten verschlüsseln. Der Sicherheitscontainer 1404 kann auch physische oder logische Assets oder Nutzer authentifizieren und/oder autorisieren, die versuchen, auf den Sicherheitscontainer 1402 zuzugreifen.

[0212] Wenn beispielsweise ein physischer oder logischer Asset oder Nutzer versucht, auf den Steuerungscontainer 1402 zuzugreifen, kann der Autentifizierungsdienst 1408 die Authentizität des physischen oder logischen Assets oder Nutzers, der versucht, auf den Steuerungscontainer 1402 zuzugreifen, verifizieren. Zum Beispiel kann der Autentifizierungsdienst 1408 ein digitales Zertifikat, das von einer Zertifizierungsstelle ausgestellt wurde, von dem physischen oder logischen Asset oder Nutzer erhalten, um die Authentizität des physischen oder logischen Assets oder Nutzers zu verifizieren. Das digitale Zertifikat kann einen kryptografischen öffentlichen Schlüssel oder einen anderen Identifikator für das physische oder logische Asset, einen Identifikator für den Zertifizierungsautoritätsdienst und eine digitale Signatur für den Zertifizierungsautoritätsdienst beinhalten, um zu beweisen, dass das Zertifikat vom Zertifizierungsautoritätsdienst erzeugt wurde. In einigen Implementierungen analysiert der Autentifizierungsdienst 1408 den Identifikator für den Zertifizierungsautoritätsdienst und die digitale Signatur für den Zertifizierungsautoritätsdienst, um festzustellen, ob die Zertifikate von dem Zertifizierungsautoritätsdienst generiert wurden. In anderen Implementierungen übermittelt der Autentifizierungsdienst 1408 die digitalen Zertifikate an einen Zertifizierungsautoritätsdienst im SDCS, um festzustellen, ob die Zertifikate von dem Zertifizierungsautoritätsdienst generiert wurden.

[0213] Wenn der Autentifizierungsdienst 1408 in der Lage ist, die Authentizität des physischen oder logischen Assets oder Nutzers zu verifizieren, kann der Autorisierungsdienst 1410 die Autorisierungsstufe des physischen oder logischen Assets oder Nutzers bestimmen. Ist der Autentifizierungsdienst 1408 hingegen nicht in der Lage, die Authentizität des physischen oder logischen Assets oder Nutzers zu verifizieren, kann der Autentifizierungsdienst 1408 den Zugriff auf den Steuerungscontainer 1402 verweigern.

[0214] In jedem Fall stellt der Autorisierungsdienst 1410 anhand der Autorisierungsstufe des physischen oder logischen Assets oder Nutzers fest, ob dieser zum Zugriff auf den Steuerungscontainer 1402 berechtigt ist. Wenn das physische oder logische Asset oder der Nutzer eine Autorisierungsstufe hat, die eine Mindestautorisierungsstufe für den Zugriff auf den Steuerungscontainer 1402 erreicht oder überschreitet, stellt der Autorisierungsdienst 1410 fest, dass das physische oder logische Asset oder der Nutzer berechtigt ist, auf den Steuerungscontainer 1402 zuzugreifen. Andernfalls kann der Autorisierungsdienst 1410 den Zugriff auf den Steuerungscontainer 1402 verweigern.

[0215] In einigen Implementierungen ist die Autorisierungsstufe des physischen oder logischen Assets oder Nutzers in den Zertifikaten beinhaltet. Verschiedene Arten von Zertifikaten können unterschiedliche Autorisierungsebenen und/oder Rollen innerhalb der industriellen Prozessanlage 10 angeben. Dementsprechend kann der Autorisierungsdienst 1410 die Autorisierungsebene für das physische oder logische Asset oder den Nutzer auf der Grundlage der Zertifikate bestimmen. In anderen Implementierungen bezieht der Autorisierungsdienst 1410 vorgespeicherte Autorisierungsstufen für physische oder logische Assets oder Nutzer von einer logischen Speicherressource und bestimmt die Autorisierungsstufe für das physische oder logische Asset auf der Grundlage der vorgespeicherten Autorisierungsstufen. In einigen Implementierungen kann das physische oder logische Asset oder der Nutzer auf der Grundlage der Autorisierungsstufe teilweisen Zugriff auf den Steuerungscontainer 1402 haben. Dementsprechend kann der Steuerungscontainer 1402 dem physischen oder logischen Asset oder Nutzer den Zugriff auf einige Bereiche des Steuerungscontainers 1402 ermöglichen und den Zugriff des physischen oder logischen Assets oder Nutzers auf andere Bereiche des Steuerungscontainers 1402 verhindern.

[0216] In jedem Fall kann der Verschlüsselungsdienst 1406 als Reaktion auf die Authentifizierung und Autorisierung eines physischen oder logischen Assets oder Nutzers die Daten vom Steuerungscontainer 1402 zum physischen oder logischen Asset oder Nutzer verschlüsseln, indem er den in den Zertifikaten beinhalteten öffentlichen kryptografischen Schlüssel verwendet. Das physische oder logische Asset oder der Nutzer kann dann die Daten mit dem kryptografischen privaten Schlüssel, der mit dem kryptografischen öffentlichen Schlüssel gepaart ist, entschlüsseln. Wenn das physische oder logische Asset oder der Nutzer nicht über den kryptografischen privaten Schlüssel verfügt, der mit dem kryptografischen öffentlichen Schlüssel gepaart ist, kann das physische oder logische Asset oder der Nutzer die Daten nicht entschlüsseln, was eine andere Form der Authentifizierung darstellt.

[0217] Zugriffs-Steuerungsdienste können die oben erwähnten Autorisierungs- oder Autentifizierungsdienste sowie Whitelists oder Akzeptanzlisten und/o-

der andere Dienste beinhalten, die es ermöglichen, dass Daten von vorbestimmten Knoten oder Diensten empfangen/übertragen werden können, während andere Knoten oder Dienste daran gehindert werden, Daten im Prozesssteuerungsnetzwerk zu empfangen oder zu übertragen. Ein Schlüsselverwaltungsdienst kann eine Aufzeichnung der kryptografischen öffentlichen Schlüssel speichern und/oder darauf zugreifen, die mit jedem physischen oder logischen Asset in der Prozessanlage 10 verbunden sind. In anderen Implementierungen ruft der Schlüsselverwaltungsdienst den Datensatz der kryptografischen öffentlichen Schlüssel aus einem Datenspeicher für ermittelte Objekte ab, wie weiter unten näher beschrieben. Wenn dann ein physisches oder logisches Asset authentifiziert werden muss, übermittelt das physische oder logische Asset seinen kryptografischen öffentlichen Schlüssel an einen Autentifizierungsdienst. Der Autentifizierungsdienst kann den Schlüsselverwaltungsdienst auffordern, den Datensatz aus dem Datenspeicher für ermittelte Objekte abzurufen, um festzustellen, ob der bereitgestellte kryptografische öffentliche Schlüssel für das physische oder logische Asset mit dem kryptografischen öffentlichen Schlüssel aus dem Datenspeicher für ermittelte Objekte übereinstimmt.

[0218] Der Schlüsselverwaltungsdienst kann auch kryptografische private Schlüssel und/oder PSKs für physische oder logische Assets in der Prozessanlage 10 speichern. Außerdem kann der Schlüsselverwaltungsdienst die Zertifikate für physische oder logische Assets in der Prozessanlage 10 speichern. Der Schlüsselverwaltungsdienst kann die Schlüssel und Zertifikate mit einem Passwort schützen und/oder verschlüsseln, so dass sich ein Nutzer oder ein physisches oder logisches Asset authentifizieren muss, bevor er Zugriff auf die entsprechenden Schlüssel oder Zertifikate erhält.

[0219] Im Beispiel des Router-Containers in **Fig. 22** kann der Router-Container die Kommunikation zwischen Knoten oder Diensten innerhalb des SDCS oder die Kommunikation zwischen einem Knoten oder Dienst innerhalb des SDCS und einem entfernten System außerhalb des SDCS erleichtern. **Fig. 25** zeigt ein Blockdiagramm eines beispielhaften Router-Containers 1502 zur Erleichterung der Kommunikation zwischen einem Knoten oder Dienst innerhalb des SDCS und einem entfernten System außerhalb des SDCS. Der Router-Container 1502 kann einen Feld-Gateway-Container 1504 beinhalten, der einen ersten Verschlüsselungsdienst 1506 ausführt, einen Datendioden-Container 1508, der einen zweiten Verschlüsselungsdienst 1510 ausführt, und einen Edge-Gateway-Container 1512, der einen Firewall-Dienst 1514 und einen Autentifizierungsdienst 1516 ausführt.

[0220] Der Feld-Gateway-Container 1504 kann mit Knoten oder Diensten in der Feldumgebung 12 der Prozessanlage kommunizieren, wie z.B. Prozess-Steuerungseinrichtungen, Feldgeräten, Steuerungsdienste, usw. Der Feld-Gateway-Container 1504 kann zum Beispiel einen Firewall-Dienst mit Firewall-Regeln beinhalten, um nur Verkehr von Knoten oder Diensten in der Feldumgebung 12 der Prozessanlage zuzulassen. Der Feld-Gateway-Container 1504 kann auch einen ersten Verschlüsselungsdienst 1506 ausführen, um Daten aus der Feldumgebung 12 der Prozessanlage zu verschlüsseln. Der Feld-Gateway-Container 1504 kann dann die Daten an den Datendioden-Container 1508 übertragen.

[0221] Der Datendiodencontainer 1508 kann den Datenverkehr aus dem Feld-Gateway-Container 1504 zu einem entfernten System ausgehen lassen und den Datenverkehr (z.B. der von einem entfernten System oder anderen Systemen übertragen oder gesendet wird) daran hindern, in den Feld-Gateway-Container 1504 einzudringen. Dementsprechend unterstützt der Datendioden-Container 1508 einen nur unidirektionalen Datenfluss vom Feld-Gateway-Container 1504 zum Edge-Gateway-Container 1512 über die Software, z.B. indem er alle am Edge-Gateway-Container 1512 (z.B. von einem entfernten System) empfangenen Nachrichten verwirft oder blockiert und/oder indem er alle an den Feld-Gateway-Container 1504 adressierten Nachrichten verwirft oder blockiert (z.B. adressiert an Knoten oder Dienste im SDCS von einem entfernten System). Der zweite Verschlüsselungsdienst 1510 kann zusätzlich oder alternativ zum ersten Verschlüsselungsdienst 1506 auch die Daten aus dem Feld Gateway Container 1504 verschlüsseln. Der Datendioden-Container 1508 kann dann die verschlüsselten Daten an den Edge-Gateway-Container 1512 übertragen.

[0222] In einigen Implementierungen kann der Datendiodencontainer 1508 während der Instanziierung vorübergehend einen Handshake (z.B. einen Austausch von Zertifikaten und Pre-Shared Keys / vorinstallierte Schlüssel) zwischen Entitäten (z.B. dem Feld-Gateway-Container 1504 und dem Edge-Gateway-Container 1512) ermöglichen, die über den Datendiodencontainer 1508 eingehende oder ausgehende Daten zur/von der Prozessanlage 10 übertragen, um verschlüsselte Verbindungen ordnungsgemäß herzustellen, wie z.B. in einer Datagram Transport Schicht Security (DTLS) oder anderen nachrichtenorientierten Sicherheitsprotokollen. Sobald der DTLS-Handshake abgeschlossen ist, wird die Verbindung hergestellt, und von diesem Zeitpunkt an unterstützt der Datendioden-Container 1508 für die verbleibende Dauer des Datendioden-Containers 1508 nur noch den unidirektionalen Datenfluss, beispielsweise vom Feld-Gateway-Container 1504 zum Edge-Gateway-Container 1512.

Wenn es zu Verbindungsproblemen zwischen den Entitäten am Eingangs- und Ausgangsende des Datendioden-Containers 1508 kommt, muss der Datendioden-Container 1508 möglicherweise neu gestartet werden, damit der DTLS-Handshake erneut stattfinden kann.

[0223] Der Edge-Gateway-Container 1512 kann mit entfernten Systemen außerhalb der Prozessanlage 10 kommunizieren. Der Edge-Gateway-Container 1512 kann einen Firewall-Dienst 1514 mit Firewall-Regeln beinhalten, um nur den Verkehr von bestimmten entfernten Systemen zuzulassen. Der Edge-Gateway-Container 1512 kann auch einen Autentifizierungsdienst ausführen, um ein entferntes System zu authentifizieren, das mit dem Edge-Gateway-Container 1512 kommuniziert. Der vom Edge-Gateway-Container 1512 an das entfernte System übermittelte Datenverkehr kann beispielsweise über ein SAS-Token (Shared Access Signature) gesichert werden, das über einen Token-Dienst verwaltet werden kann, der auf dem entfernten System 210 bereitgestellt wird. Der Edge-Gateway-Container 1512 authentifiziert den Token-Dienst und fordert ein SAS-Token an, das nur für eine begrenzte Zeit gültig sein kann, z. B. zwei Minuten, fünf Minuten, dreißig Minuten, höchstens eine Stunde usw. Der Edge-Gateway-Container 1512 empfängt und verwendet das SAS-Token, um eine AMQP-Verbindung (Advanced Message Queuing Protocol) zum entfernten System zu sichern und zu authentifizieren, über die Inhaltsdaten vom Edge-Gateway-Container 1512 zum entfernten System übertragen werden. Zusätzlich oder alternativ können andere Sicherheitsmechanismen verwendet werden, um die Datenübertragung zwischen dem Edge-Gateway-Container 1512 und dem entfernten System 210 zu sichern, z.B. X. 509 Zertifikate, andere Arten von Token, andere IOT-Protokolle wie MQTT (MQ Telemetry Transport) oder XMPP (Extensible Messaging and Presence Protocol) und ähnliches. Der Edge-Gateway-Container 1512 kann dann die Daten an das entfernte System übertragen.

[0224] Wie bereits erwähnt, kann ein physisches oder logisches Asset oder ein Nutzer zum Nachweis der Authentizität bei der Kommunikation im SDCS ein digitales Zertifikat von einem Zertifizierungsautoritätsdienst anfordern. **Fig. 26** zeigt ein detailliertes Blockdiagramm eines Zertifikate-Autorisierungscontainers 1602, der dem in **Fig. 20** gezeigten Zertifikate-Autorisierungscontainer 1028 ähnelt. Der Zertifikate-Autoritäts-Container 1602 kann einen Zertifikaterzeugungsdienst 1604 und einen Zertifikat-Verifizierungsdienst 1606 beinhalten.

[0225] Der Zertifikaterzeugungsdienst 1604 kann die digitalen Zertifikate für ein physisches oder logisches Asset beispielsweise nach Erhalt einer Anfrage des physischen oder logischen Assets erzeugen. Nach Erhalt der Anfrage erhält der Zertifikaterzeugungsdienst 1604 Identifizierungsinformationen für das physische oder logische Asset und verifiziert die Identität des physischen oder logischen Assets anhand der Identifizierungsinformationen. Die Anfrage kann beispielsweise den Namen des physischen oder logischen Assets, die Marke und das Modell des physischen oder logischen Assets, einen kryptografischen öffentlichen Schlüssel, der mit einem kryptografischen privaten Schlüssel verbunden ist, der sich im Besitz des physischen oder logischen Assets befindet, oder jede andere geeignete Identifikationsinformation beinhalten. Der Zertifikaterzeugungsdienst 1604 kann die Identität des physischen oder logischen Assets verifizieren, indem er beispielsweise die von dem physischen oder logischen Asset erhaltenen Identifizierungsinformationen mit Identifizierungsinformationen für das physische oder logische Asset vergleicht, die aus anderen Quellen stammen. Wenn der Zertifikaterzeugungsdienst 1604 die Identität des physischen oder logischen Assets nicht verifizieren kann, generiert der Zertifikaterzeugungsdienst 1604 keine Zertifikate für das physische oder logische Asset.

[0226] Wenn der Zertifikaterzeugungsdienst 1604 hingegen die Identität des physischen oder logischen Assets verifizieren kann, generiert der Zertifikaterzeugungsdienst 1604 ein Zertifikat für das physische oder logische Asset, das einen kryptografischen öffentlichen Schlüssel oder eine andere Kennung für das physische oder logische Asset, eine Kennung für den Zertifizierungsautoritätsdienst 1602, wie z. B. einen kryptografischen öffentlichen Schlüssel, und eine digitale Signatur für den Zertifizierungsautoritätsdienst 1602 beinhalten kann, um zu beweisen, dass das Zertifikat von dem Zertifizierungsautoritätsdienst 1602 generiert wurde. Der Zertifikaterzeugungsdienst 1604 stellt die Zertifikate dem physischen oder logischen Asset zur Verfügung, das die Zertifikate zu Authentifizierungszwecken bei der Kommunikation mit anderen Knoten oder Diensten innerhalb des SDCS verwenden kann. In einigen Implementierungen können die anderen Dienste die Kommunikation mit dem physischen oder logischen Asset mit dem öffentlichen kryptografischen Schlüssel für das physische oder logische Asset verschlüsseln, der in den Zertifikaten beinhaltet ist.

[0227] In einigen Implementierungen kann auch ein Nutzer innerhalb des SDCS ein digitales Zertifikat von dem Zertifikaterzeugungsdienst 1604 anfordern, z. B. ein Assetbetreiber, ein Konfigurationstechniker und/oder anderes mit der industriellen Prozessanlage 10 verbundenes Personal. Wenn der Nutzer die digitalen Zertifikate anfordert, kann er Identifikationsdaten angeben, z. B. seinen Namen, seine Adresse, seine Telefonnummer, seine Rolle innerhalb der industriellen Prozessanlage 10, einen Nutzernamen und ein Passwort usw. Der Zertifikaterzeu-

gungsdienst 1604 kann die Identität des Nutzers verifizieren, indem er z.B. die vom Nutzer erhaltenen Identifikationsinformationen mit Identifikationsinformationen für den Nutzer vergleicht, die er aus anderen Quellen erhalten hat.

[0228] Wenn der Zertifikaterzeugungsdienst 1604 den Nutzer nicht verifizieren kann, generiert der Zertifikaterzeugungsdienst 1604 keine Zertifikate für den Nutzer. Wenn der Zertifikaterzeugungsdienst 1604 den Nutzer hingegen verifizieren kann, generiert der Zertifikaterzeugungsdienst 1604 ein digitales Zertifikat für den Nutzer und stellt es ihm zur Verfügung. Auf diese Weise kann der Nutzer die digitalen Zertifikate bereitstellen, um auf Knoten oder Dienste innerhalb des SDCS zuzugreifen und muss keine Anmeldeinformationen eingeben. In einigen Implementierungen kann der Zertifikaterzeugungsdienst 1604 Autorisierungsinformationen für den Nutzer in die Zertifikate aufnehmen. Die SDCS kann dem Nutzer eine Autorisierungsstufe zuweisen, die auf der Rolle des Nutzers innerhalb der industriellen Prozessanlage 10 basiert. Der Zertifikaterzeugungsdienst 1604 kann dann verschiedene Arten von Zertifikaten für verschiedene Autorisierungsstufen und/oder Rollen innerhalb der industriellen Prozessanlage 10 generieren. Auf diese Weise können Knoten oder Dienste, auf die der Nutzer zuzugreifen versucht, die Autorisierungsstufe und/oder die Rolle des Nutzers innerhalb der industriellen Prozessanlage 10 auf der Grundlage der Art der Zertifikate, die der Nutzer bereitstellt, bestimmen.

[0229] Wenn ein physisches oder logisches Asset oder ein Nutzer versucht, auf einen Knoten oder Dienst im SDCS zuzugreifen, kann der Knoten oder Dienst eine Anfrage an den Zertifikat-Verifizierungsdienst 1606 stellen, um das physische oder logische Asset oder den Nutzer zu authentifizieren. Genauer gesagt kann das physische oder logische Asset oder der Nutzer ein Zertifikat an den Knoten oder Dienst übermitteln, der das Zertifikat an den Zertifikat-Verifizierungsdienst 1606 weiterleitet. In einigen Implementierungen analysiert der Zertifikat-Verifizierungsdienst 1606 die in den Zertifikaten beinhaltete Kennung für den Zertifizierungsautoritätsdienst und die in den Zertifikaten beinhaltete digitale Signatur für den Zertifizierungsautoritätsdienst, um festzustellen, ob die Zertifikate von dem Zertifizierungsautoritätsdienst generiert wurden. Der Zertifikat-Verifizierungsdienst 1606 kann zum Beispiel feststellen, ob der in den Zertifikaten beinhaltete kryptografische öffentliche Schlüssel der Zertifizierungsstelle mit dem kryptografischen öffentlichen Schlüssel der Zertifizierungsstelle übereinstimmt. Darüber hinaus kann der Zertifikat-Verifizierungsdienst 1606 feststellen, ob die digitale Signatur beweist, dass das Unternehmen, das die Zertifikate generiert, Eigentümer des kryptografischen privaten Schlüssels ist, der mit dem kryptografischen öffentlichen Schlüssel verbunden ist. Wenn beides zutrifft, kann der Zertifikat-Verifizierungsdienst 1606 feststellen, dass die Zertifikate vom Zertifizierungsautoritätsdienst erstellt wurden.

[0230] Dann kann der Zertifikat-Verifizierungsdienst 1606 dem Knoten oder Dienst mitteilen, dass das physische oder logische Asset oder der Nutzer authentifiziert worden ist. Zusätzlich oder alternativ kann der Zertifikat-Verifizierungsdienst 1606 dem Knoten oder Dienst einen Hinweis auf die Autorisierungsstufe des Nutzers geben, wenn die Zertifikate einen Hinweis auf die Autorisierungsstufe beinhalten.

[0231] **Fig. 27** zeigt ein Beispiel für Authentifizierungs- und Autorisierungsdienste, die in Knoten oder Diensten des SDCS beinhalten sein können, wie z.B. ein Steuerungscontainer und ein Container für einen Bedienerarbeitsplatz (z.B. ein virtueller Arbeitsplatz). Wie in **Fig. 27** gezeigt, beinhaltet ein Steuerungscontainer 1702 einen ersten Autentifizierungsdienst 1704 und ein Bedienerarbeitsplatzcontainer 1706 beinhaltet einen zweiten Autentifizierungsdienst 1708 und einen Autorisierungsdienst 1710.

[0232] Der Steuerungscontainer 1702 kann eine Zugriffsanfrage von einem physischen oder logischen Asset erhalten, wobei die Anfrage ein Zertifikat beinhaltet. Dementsprechend kann der erste Autentifizierungsdienst 1704 das physische oder logische Asset anhand der Zertifikate authentifizieren. In einigen Implementierungen kann der erste Autentifizierungsdienst 1704 die Zertifikate an einen Zertifizierungsautoritätsdienst weitergeben, z.B. an den Zertifizierungsautoritätsdienst 1602, wie in **Fig. 26** gezeigt, um das physische oder logische Asset zu authentifizieren. In jedem Fall kann der erste Autentifizierungsdienst 1704 nach der Authentifizierung des physischen oder logischen Assets den Zugriff auf den Steuerungscontainer 1702 ermöglichen. Andernfalls kann der erste Autentifizierungsdienst 1704 den Zugriff auf den Steuerungscontainer 1702 verweigern.

[0233] Der Bedienerarbeitsplatzcontainer 1706 kann eine Zugangsanfrage von einem Nutzer erhalten, wobei die Anfrage ein Zertifikat beinhaltet. Dementsprechend kann der zweite Autentifizierungsdienst 1708 den Nutzer anhand der Zertifikate authentifizieren. In einigen Implementierungen kann der zweite Autentifizierungsdienst 1708 die Zertifikate an einen Zertifizierungsautoritätsdienst weitergeben, wie z.B. an den Zertifizierungsautoritätsdienst 1602, wie in **Fig. 26** gezeigt, um den Nutzer zu authentifizieren. In jedem Fall kann der erste Autentifizierungsdienst 1704 nach der Authentifizierung des Nutzers eine Meldung an den Bedienerarbeitsplatzcontainer 1706 senden, dass der Nutzer authentifiziert worden ist.

[0234] Der Autorisierungsdienst 1710 stellt dann anhand der Autorisierungsstufe des Nutzers fest, ob der Nutzer berechtigt ist, auf den Bedienerarbeitsplatzcontainer 1706 zuzugreifen. Wenn die Autorisierungsstufe des Nutzers eine Mindestautorisierungsstufe für den Zugriff auf den Bedienerarbeitsplatzcontainer 1706 erreicht oder überschreitet, stellt der Autorisierungsdienst 1710 fest, dass der Nutzer berechtigt ist, auf den Bedienerarbeitsplatzcontainer 1706 zuzugreifen. Andernfalls kann der Autorisierungsdienst 1710 den Zugriff auf den Bedienerarbeitsplatzcontainer 1706 verweigern.

[0235] In einigen Implementierungen ist die Autorisierungsstufe des Nutzers in den Zertifikaten beinhaltet, verschiedene Arten von Zertifikaten für verschiedene Autorisierungsstufen und/oder Rollen innerhalb der industriellen Prozessanlage 10. Dementsprechend kann der Autorisierungsdienst 1710 die Autorisierungsstufe für den Nutzer auf der Grundlage der Zertifikate bestimmen. In anderen Implementierungen bezieht der Autorisierungsdienst 1710 vorgespeicherte Autorisierungsstufen für Nutzer aus einer logischen Speicherressource und bestimmt die Autorisierungsstufe für den Nutzer auf der Grundlage der vorgespeicherten Autorisierungsstufen. In einigen Implementierungen kann der Nutzer auf der Grundlage der Autorisierungsstufe teilweisen Zugriff auf den Bedienerarbeitsplatzcontainer 1706 haben. Dementsprechend kann der Bedienerarbeitsplatzcontainer 1706 dem Nutzer den Zugriff auf einige Bereiche des Bedienerarbeitsplatzcontainers 1706 ermöglichen und den Zugriff des Nutzers auf andere Bereiche des Bedienerarbeitsplatzcontainers 1706 verhindern.

[0236] Zusätzlich zur Verschlüsselung der Netzwerkkommunikation im SDCS verschlüsselt das SDCS die logischen Speicherressourcen. **Fig. 28** zeigt ein Blockdiagramm eines beispielhaften Speicherdienstes 1802, der einen Verschlüsselungsdienst 1804 und einen Autentifizierungsdienst 1806 beinhaltet.

[0237] Wenn der Speicherdienst 1802 logische Speicherressourcen im SDCS speichert, verschlüsselt der Verschlüsselungsdienst 1804 die in den logischen Speicherressourcen beinhalteten Daten. Wenn dann ein physisches oder logisches Asset oder ein Nutzer versucht, auf eine logische Speicherressource zuzugreifen, authentifiziert der Autentifizierungsdienst 1806 das physische oder logische Asset oder den Nutzer. Zum Beispiel kann der Autentifizierungsdienst 1806 das physische oder logische Asset oder den Nutzer auf der Grundlage eines Zertifikats für das physische oder logische Asset oder den Nutzer authentifizieren, das von einer Zertifizierungsstelle ausgestellt wurde. Wenn der Autentifizierungsdienst 1806 in der Lage ist, das physische oder logische Asset oder den Nutzer zu authentifizieren, kann der Speicherdienst 1802 die in der logischen Speicherressource beinhalteten Daten entschlüsseln und die entschlüsselte logische Speicherressource dem physischen oder logischen Asset oder dem Nutzer zur Verfügung stellen. Andernfalls entschlüsselt der Speicherdienst 1802 die Daten nicht für das physische oder logische Asset oder den Nutzer.

[0238] **Fig. 29** zeigt ein Flussdiagramm, das ein Beispielverfahren 1900 zur Sicherung eines Prozesssteuerungssystems einer Prozessanlage darstellt. Das Verfahren kann von einem Software-definierten Netzwerkdienst, einem Sicherheitscontainer oder einer geeigneten Kombination aus diesen ausgeführt werden.

[0239] Im Block 1902 erzeugt ein Software-definierter Netzwerkdienst einen Sicherheitsdienst, der so konfiguriert ist, dass er über einen Container auf einem Rechenknoten innerhalb des SDCS ausgeführt wird. Der Sicherheitsdienst kann beispielsweise einen virtuellen Router, eine virtuelle Firewall, einen virtuellen Switch, eine virtuelle Schnittstelle, eine virtuelle Datendiode, eine Paketprüfungsleistung, einen Zugriffs-Steuerungsdienst, einen Autorisierungsdienst, einen Autentifizierungsdienst, einen Verschlüsselungsdienst, einen Zertifizierungsautoritätsdienst, einen Schlüsselverwaltungsdienst oder jeden anderen geeigneten sicherheitsrelevanten Dienst beinhalten.

[0240] Im Block 1904 instanziiert der Software-definierte Netzwerkdienst eine Instanz des Sicherheitscontainers, um mit einem Steuerungscontainer zu arbeiten. Die Instanz des Sicherheitscontainers kann eine primäre Instanz sein. Der Software-definierte Netzwerkdienst kann auch N redundante Instanzen des Sicherheitscontainers instanziieren, um z.B. den Betrieb mit dem Steuerungscontainer zu simulieren, ohne den Zugriff auf den Steuerungscontainer oder den Datenfluss von diesem tatsächlich zu steuern. In einigen Implementierungen verschachtelt der Software-definierte Netzwerkdienst den Sicherheitscontainer in den Steuerungscontainer. In zusätzlichen oder alternativen Implementierungen bindet der Software-definierte Netzwerkdienst den Sicherheitscontainer an denselben Rechenknoten an wie den Rechenknoten, auf dem der Steuerungscontainer ausgeführt wird. In anderen Implementierungen ist der Sicherheitscontainer ein eigenständiger Container, der dem Steuerungscontainer zugeordnet ist.

[0241] Im Block 1906 weist der Software-definierte Netzwerkdienst dem Sicherheitscontainer Sicherheitsbedingungen in Übereinstimmung mit dem Steuerungscontainer zu. Zum Beispiel kann ein Steuerungskonfigurationsdienst eine Steuerkonfigu-

ration von einer Steuerkonfigurations-Speicherressource erhalten und die Steuerkonfiguration dem Steuerungscontainer zur Verfügung stellen. Die Steuerkonfigurations-Speicherressource kann auch einen Satz angepasster Firewall-Regeln für den Steuerungscontainer beinhalten. Der Software-definierte Netzwerkdienst kann den Satz benutzerdefinierter Firewall-Regeln für den Steuerungscontainer aus dem Steuerungskonfigurationsdienst beziehen und den Satz benutzerdefinierter Firewall-Regeln dem Sicherheitscontainer als Sicherheitsbedingungen zuweisen. Der Software-definierte Netzwerkdienst kann auch andere Sicherheitsbedingungen in Übereinstimmung mit dem Steuerungscontainer zuweisen, wie z.B. die Authentifizierung von physischen oder logischen Assets oder Nutzern, die versuchen, auf den Steuerungscontainer zuzugreifen, die Anforderung, dass Nutzer eine Autorisierungsstufe haben müssen, die eine Mindestschwellen-Autorisierungsstufe übersteigt oder erfüllt, die Verhinderung des Zugriffs von entfernten Systemen außerhalb der Prozessanlage 10 oder die Verhinderung von eingehenden Daten von entfernten Systemen außerhalb der Prozessanlage 10.

[0242] In einigen Implementierungen kann der Software-definierte Netzwerkdienst dem Sicherheitscontainer alternative oder zusätzliche Sicherheitsbedingungen zuweisen, um den Inhalt des Sicherheitscontainers zu aktualisieren. Beispielsweise kann der Software-definierte Netzwerkdienst zu einem ersten Zeitpunkt dem Sicherheitscontainer einen ersten Satz von Sicherheitsregeln zuweisen. Zu einem späteren Zeitpunkt kann der Software-definierte Netzwerkdienst dann eine aktualisierte Steuerkonfiguration für den Steuerungscontainer erhalten. Der Software-definierte Netzwerkdienst kann auch aktualisierte Firewall-Regeln für den Steuerungscontainer aufgrund der Änderung der Steuerkonfiguration erhalten und kann die aktualisierten Firewall-Regeln dem Sicherheitscontainer als Sicherheitsbedingungen zuweisen.

[0243] Im Block 1908 kontrolliert der Sicherheitscontainer den Zugriff auf und/oder den Datenfluss von dem Steuerungscontainer auf der Grundlage der dem Sicherheitscontainer zugewiesenen Sicherheitsbedingungen. Zum Beispiel kann der Sicherheitscontainer verhindern, dass Knoten oder Dienste, die nicht in einer Whitelist oder Akzeptanzliste beinhaltet sind, mit dem Steuerungscontainer kommunizieren.

[0244] **Fig. 30** zeigt ein Flussdiagramm, das ein Beispielverfahren 2000 für rollenbasierte Autorisierung in einem SDCS darstellt. Das Verfahren kann von einem Sicherheitscontainer oder einem Autorisierungsdienst ausgeführt werden.

[0245] Im Block 2002 erhält ein Sicherheitsdienst, der über einen Container auf einem Rechenknoten innerhalb des SDCS ausgeführt wird, eine Anfrage von einem Nutzer, um auf einen anderen Dienst oder Knoten innerhalb des SDCS zuzugreifen, wie z.B. einen Steuerungscontainer. In einigen Implementierungen kann der Sicherheitsdienst die Anfrage von einem physischen oder logischen Asset der Prozessanlage 10 erhalten, das von dem Nutzer kontrolliert wird. In einigen Implementierungen kann die Anfrage auch ein vom Nutzer bereitgestelltes Zertifikat beinhalten, um die Authentizität des Nutzers zu verifizieren und Autorisierungsinformationen für den Nutzer zu beinhalten.

[0246] Im Block 2004 bestimmt der Sicherheitsdienst eine Autorisierungsstufe des Nutzers. Die Autorisierungsstufe des Nutzers kann zum Beispiel in den Zertifikaten beinhaltet sein. Verschiedene Arten von Zertifikaten können verschiedene Autorisierungsstufen und/oder Rollen innerhalb der industriellen Prozessanlage 10 angeben. Dementsprechend kann der Sicherheitsdienst die Autorisierungsstufe für den Nutzer auf der Grundlage der Zertifikate bestimmen. In anderen Implementierungen bezieht der Sicherheitsdienst vorgespeicherte Autorisierungsebenen für Nutzer aus einer logischen Speicherressource und bestimmt die Autorisierungsebene für das physische oder logische Asset auf der Grundlage der vorgespeicherten Autorisierungsebenen.

[0247] Im Block 2006 bestimmt der Sicherheitsdienst anhand der Autorisierungsstufe, ob der Nutzer zum Zugriff auf den anderen Dienst oder Knoten berechtigt ist. Wenn der Nutzer beispielsweise eine Autorisierungsstufe hat, die einer Mindestautorisierungsstufe für den Zugriff auf den anderen Dienst oder Knoten innerhalb des SDCS entspricht oder diese überschreitet, bestimmt der Sicherheitsdienst, dass der Nutzer berechtigt ist, auf den anderen Dienst oder Knoten zuzugreifen. Dementsprechend gibt der Sicherheitsdienst dem Nutzer den Zugriff auf den anderen Dienst oder Knoten, wie z.B. den Steuerungscontainer, frei (Block 2008). Andernfalls kann der Sicherheitsdienst den Zugriff auf den anderen Dienst oder Knoten verweigern (Block 2010).

[0248] **Fig. 31** zeigt ein Flussdiagramm, das ein Beispielverfahren 2100 zur Erzeugung eines digitalen Zertifikats durch einen Zertifizierungsautoritätsdienst zur Authentifizierung eines physischen oder logischen Assets der Prozessanlage 10 darstellt. Das Verfahren kann von einem Zertifizierungsautoritätsdienst ausgeführt werden.

[0249] Im Block 2102 erhält der Zertifizierungsautoritätsdienst eine Anfrage für ein Zertifikat von einem physischen oder logischen Asset der Prozessanlage 10. Nach Erhalt der Anfrage erhält der Zertifizie-

rungsautoritätsdienst Identifikationsinformationen für das physische oder logische Asset und prüft die Identität des physischen oder logischen Assets anhand der Identifikationsinformationen (Block 2104). Die Anfrage kann beispielsweise den Namen des physischen oder logischen Assets, die Marke und das Modell des physischen oder logischen Assets, einen kryptografischen öffentlichen Schlüssel, der mit einem kryptografischen privaten Schlüssel verknüpft ist, der sich im Besitz des physischen oder logischen Assets befindet, oder jede andere geeignete Identifikationsinformation beinhalten. Der Zertifizierungsautoritätsdienst kann die Identität des physischen oder logischen Assets verifizieren, indem er beispielsweise die von dem physischen oder logischen Asset erhaltenen Identifizierungsinformationen mit Identifizierungsinformationen für das physische oder logische Asset vergleicht, die aus anderen Quellen stammen. Ist der Zertifizierungsautoritätsdienst nicht in der Lage, die Identität des physischen oder logischen Assets zu verifizieren, erstellt der Zertifizierungsautoritätsdienst keine Zertifikate für das physische oder logische Asset.

[0250] Kann der Zertifizierungsautoritätsdienst hingegen die Identität des physischen oder logischen Assets verifizieren, generiert er ein Zertifikat für das physische oder logische Asset, das einen kryptografischen öffentlichen Schlüssel oder eine andere Kennung für das physische oder logische Asset, eine Kennung für den Zertifizierungsautoritätsdienst, wie z. B. einen kryptografischen öffentlichen Schlüssel, und eine digitale Signatur für den Zertifizierungsautoritätsdienst beinhalten kann, um zu beweisen, dass das Zertifikat vom Zertifizierungsautoritätsdienst generiert wurde (Block 2106). Der Zertifizierungsautoritätsdienst stellt die Zertifikate dem physischen oder logischen Asset zur Verfügung, das die Zertifikate zur Authentifizierung bei der Kommunikation mit anderen Knoten oder Diensten innerhalb des SDCS verwenden kann (Block 2108). In einigen Implementierungen können die anderen Dienste die Kommunikation mit dem physischen oder logischen Asset verschlüsseln, indem sie den in den Zertifikaten beinhalteten öffentlichen kryptografischen Schlüssel für das physische oder logische Asset verwenden.

[0251] **Fig. 32** zeigt ein Flussdiagramm, das ein Beispielverfahren 2200 zur Authentifizierung eines physischen oder logischen Assets der Prozessanlage 10 darstellt. Das Verfahren kann von einem Sicherheitsdienst, einem Autentifizierungsdienst oder einer geeigneten Kombination aus diesen ausgeführt werden.

[0252] Im Block 2202 erhält ein Sicherheitsdienst, der über einen Container auf einem Rechenknoten innerhalb des SDCS ausgeführt wird, eine Anfrage zum Zugriff auf einen anderen Dienst oder Knoten innerhalb des SDCS von einem physischen oder logischen Asset. Die Anfrage kann ein Zertifikat beinhalten, das von dem physischen oder logischen Asset bereitgestellt wird, um die Authentizität des physischen oder logischen Assets zu verifizieren.
Im Block 2204 prüft ein Autentifizierungsdienst, der über einen Container auf einem Rechenknoten innerhalb des SDCS ausgeführt wird, die Authentizität des physischen oder logischen Assets anhand der Zertifikate. Beispielsweise kann der Autentifizierungsdienst eine in den Zertifikaten beinhaltete Kennung für den Zertifizierungsautoritätsdienst und die in den Zertifikaten beinhaltete digitale Signatur für den Zertifizierungsautoritätsdienst analysieren, um festzustellen, ob die Zertifikate von dem Zertifizierungsautoritätsdienst erzeugt wurden. In anderen Implementierungen stellt der Autentifizierungsdienst dem Zertifizierungsautoritätsdienst die Zertifikate zur Verfügung, um die Authentizität des physischen oder logischen Assets zu verifizieren.

[0253] Wenn der Autentifizierungsdienst in der Lage ist, die Authentizität des physischen oder logischen Assets oder Nutzers zu verifizieren (Block 2208), kann der Sicherheitsdienst den Zugriff auf den anderen Dienst oder Knoten ermöglichen. Ist der Autentifizierungsdienst hingegen nicht in der Lage, die Authentizität des physischen oder logischen Assets zu verifizieren, kann der Sicherheitsdienst den Zugriff auf den anderen Dienst oder Knoten verweigern (Block 2210).

[0254] Das SDCS kann auch einen Suchdienst beinhalten, der über einen Container auf einem Rechenknoten des SDCS ausgeführt wird. Der Suchdienst speichert eine Aufzeichnung der Identität, der Fähigkeiten und/oder des Standorts jedes physischen oder logischen Assets in der Prozessanlage 10, die während der Laufzeit der Prozessanlage 10 genutzt werden kann, um mindestens einen Bereich des industriellen Prozesses zu steuern, wie z.B. Feldgeräte, Steuerungen, Prozesssteuerungseinrichtungen, E/A-Geräte, Rechenknoten, Container, Dienste (z.B. Steuerungsdienste), Microdienste, etc.

[0255] In einigen Implementierungen kann der Suchdienst den Datensatz in einem Datenspeicher für ermittelte Objekte speichern. Das SDCS kann mehrere Instanzen des Suchdienst-Datenspeichers beinhalten, die zur Redundanz/Fehlertoleranz über mehrere Rechenknoten hinweg gespeichert sind. In anderen Implementierungen kann eine Instanz des Datenspeichers für ermittelte Objekte auf jedem Rechenknoten innerhalb des SDCS gespeichert sein, um den Zugriff zu erleichtern und zu beschleunigen.

[0256] In einigen Implementierungen kann der Suchdienst den Datensatz oder zumindest einen Bereich davon an einen E/A-Serverdienst zur Inbe-

triebnahme der physischen oder logischen Assets weitergeben. Wenn zum Beispiel ein physisches oder logisches Asset einem Netzwerk 22, 25, 30, 32, 35, 42-58 in der Prozessanlage 10 beitritt, kündigt das physische oder logische Asset seine Anwesenheit an. Die Ankündigung kann Parameter wie Identifikationsinformationen für das physische oder logische Asset und Standortinformationen für das physische oder logische Asset beinhalten, wie z.B. eine Netzwerkadresse zur Kommunikation mit dem physischen oder logischen Asset. Der Suchdienst oder ein anderer geeigneter Dienst kann die Ankündigung abrufen und die Identifikations- und Standortinformationen für das physische oder logische Asset an einen E/A-Serverdienst übertragen, um das physische oder logische Asset unter Verwendung der Identifikations- und Standortinformationen automatisch in Betrieb zu nehmen.

[0257] Fig. 33 zeigt ein Blockdiagramm von Beispielcontainern, Diensten und/oder Subsystemen, die mit der Erkennung zusammenhängen. Wie in **Fig. 33** dargestellt, beinhaltet das SDCS einen Container, der einen Suchdienst 2302 ausführt. Während der Suchdienst 2302 in **Fig. 33** innerhalb eines Containers (eines Discovery-Containers) ausgeführt wird, kann der Suchdienst 2302 in anderen Implementierungen auch ohne Container arbeiten. In einigen Implementierungen kann das SDCS auch mehrere Instanzen des Suchdienstes 2302 in mehreren Containern zur Redundanz beinhalten. In einigen Implementierungen kann der Suchdienst 2302 durch den SD-Netzwerkdienst 220 bereitgestellt werden oder in den SD-Netzwerkdienst 220 von **Fig. 2** eingebettet sein.

[0258] Das SDCS beinhaltet auch einen Datenspeicher 2304 für ermittelte Objekte, der eine logische Speicherressource ist, die einen Datensatz für jedes ermittelte physische oder logische Asset in der Prozessanlage 10 speichert. Nach der Entdeckung eines physischen oder logischen Assets kann der Suchdienst 2302 den Datensatz des physischen oder logischen Assets in dem Datenspeicher 2304 für ermittelte Objekte speichern.

[0259] Wenn ein neues physisches oder logisches Asset zu einem Netzwerk 22, 25, 30, 32, 35, 42-58 in der Prozessanlage 10 (hier auch als „Prozessanlagennetzwerk“ bezeichnet) hinzugefügt wird, kann das neue physische oder logische Asset seine Anwesenheit bekannt geben, indem es beispielsweise seine Netzwerkadresse an Knoten oder Dienste sendet, die mit dem Prozessanlagennetzwerk 22, 25, 30, 32, 35, 42-58 verbunden sind. In anderen Implementierungen kann das neue physische oder logische Asset seine Anwesenheit bekannt geben, indem es z.B. auf eine Multicast-Ankündigung eines bestimmten Knotens oder Dienstes antwortet, der mit dem Prozessanlagen-Netzwerk 22, 25, 30, 32, 35, 42-58 verbunden ist. In anderen Implementierungen kann das neue physische oder logische Asset seine Netzwerkadresse einer reservierten Punkt-zu-Punkt-Netzwerkadresse oder einer Multicast-Adresse bekannt geben. Das neue physische oder logische Asset kann seine Netzwerkadresse einmalig, periodisch, auf Anfrage oder auf jede andere geeignete Weise bekannt geben.

[0260] Ein physisches Asset in der Prozessanlage 10 kann ein physisches Hardwaregerät sein, das so konfiguriert ist, dass es mindestens einen Bereich des industriellen Prozesses während der Laufzeit der Prozessanlage 10 steuert, wie z.B. ein Feldgerät, eine Steuerung, eine Prozesssteuerungseinrichtung, ein E/A-Gerät, einen Rechenknoten usw. Das physische Hardwaregerät kann einen entsprechenden Satz von Prozessor- und/oder Prozessorkern-Ressourcen und Speicherressourcen beinhalten. Ein logisches Asset in der Prozessanlage 10 kann eine Software sein, die so konfiguriert ist, dass sie mindestens einen Bereich des industriellen Prozesses während der Laufzeit der Prozessanlage 10 steuert, z. B. ein Container, ein Dienst wie ein Steuerungsdienst, ein Microdienst usw. In einigen Implementierungen kann eine logische Anlage innerhalb einer physischen Anlage ausgeführt werden.

[0261] Der Suchdienst 2302 kann die Ankündigung erhalten und die Identität der physischen oder logischen Anlage anhand von Parametern der physischen oder logischen Anlage, die in der Ankündigung beinhaltet sind, bestimmen. Die Ankündigung kann eine YAML-Datei beinhalten, die jedes physische oder logische Asset definiert. Die YAML-Datei kann manuell oder automatisch generiert werden, z.B. wenn das SDCS zuvor in Betrieb genommen/konfiguriert wurde. In anderen Implementierungen beinhaltet die Ankündigung einen anderen Dateityp, wie z.B. eine JSON-Datei, eine XML-Datei oder eine andere Datenserialisierungsdatei.

[0262] Genauer gesagt kann die Ankündigung ein Asset-Tag des physischen oder logischen Assets, eine MAC-Adresse (Media Access Control) des physischen oder logischen Assets, eine Netzwerkadresse des physischen oder logischen Assets, einen kryptografischen Schlüssel für das physische oder logische Asset, eine Seriennummer für das physische oder logische Asset und/oder den Namen eines Dienstes oder Subsystems beinhalten, der mit dem physischen oder logischen Asset verbunden ist. Während einige der Parameter das physische oder logische Asset eindeutig identifizieren können, wie z.B. die MAC-Adresse, können andere Parameter, wie z.B. die Seriennummer, mehreren Assets mit derselben Marke und demselben Modell entsprechen. Dementsprechend kann der Suchdienst 2302 das physische oder logische Asset anhand jeder geeigneten Kombination der in der Ankündigung

beinhalteten Parameter identifizieren. Bei zwei physischen oder logischen Assets kann es sich beispielsweise um Ventile handeln, die dieselbe Seriennummer, also eine Teilenummer, haben. Die beiden Ventile können anhand einer Kombination aus der Seriennummer und den kryptografischen Schlüsseln der beiden Ventile identifiziert werden.

[0263] Das Asset-Tag kann ein Name oder eine Nummer sein, der/die dem physischen oder logischen Asset zugewiesen/konfiguriert wurde und der/die ein bestimmtes physisches oder logisches Asset innerhalb des SDCS eindeutig identifiziert oder ganz allgemein den Asset-Typ identifiziert. Handelt es sich bei dem physischen Asset beispielsweise um ein Steuerventil, kann das Asset-Tag „CTRL-VALVE“ lauten und die Prozessanlage 10 kann mehrere Steuerventile mit demselben Asset-Tag beinhalten. In anderen Implementierungen kann das Asset-Tag „CTRL-VALVE-01“ lauten, um dieses bestimmte Steuerventil eindeutig zu identifizieren, und andere Steuerventile können „CTRL-VALVE-02“, „CTRL-VALVE-03“ usw. sein. In einem anderen Beispiel, wenn das logische Asset ein Steuerungsdienst ist, kann das Asset-Tag „CTRL-SERV“ lauten und die Prozessanlage 10 kann mehrere Steuerungsdienste mit demselben Asset-Tag beinhalten. In anderen Implementierungen kann das Asset-Tag „CTRL-SERV-01“ lauten, um diesen bestimmten Steuerungsdienst eindeutig zu identifizieren, und andere Steuerungsdienste können „CTRL-SERV-02“, „CTRL-SERV-03“ usw. lauten.

[0264] Die MAC-Adresse kann die Adresse der Netzwerkkarte sein, die mit dem physischen oder logischen Asset arbeitet. Die MAC-Adresse kann physische Assets eindeutig identifizieren. Bei logischen Assets kann die MAC-Adresse jedoch für Dienste, die auf demselben Rechenknoten betrieben werden, gleich sein und sich ändern, wenn der Dienst auf einem anderen Rechenknoten betrieben wird. Dementsprechend kann in einigen Implementierungen die MAC-Adresse nicht zur Identifizierung eines logischen Assets verwendet werden oder die MAC-Adresse kann in Kombination mit anderen Parametern zur Identifizierung des logischen Assets verwendet werden.

[0265] Die Netzwerkadresse kann eine IP-Adresse oder eine andere Kennung für das physische oder logische Asset innerhalb des Prozessanlagen-Netzwerks 22, 25, 30, 32, 35, 42-58 sein. Die Seriennummer kann eine vom Hersteller zugewiesene Nummer sein, die die Marke und das Modell eines physischen Assets angibt, wie z.B. eine Teilenummer.

[0266] In einigen Implementierungen kann dem physischen oder logischen Asset ein asymmetrisches Schlüsselpaar zugewiesen werden, das einen kryptographischen privaten Schlüssel und einen kryptographischen öffentlichen Schlüssel beinhaltet. Das asymmetrische Schlüsselpaar kann von einem Nutzer oder dem Hersteller zugewiesen werden. Dann kann das physische oder logische Asset den kryptographischen privaten Schlüssel speichern, ohne ihn mit anderen Knoten oder Diensten zu teilen. Das physische oder logische Asset kann den kryptografischen öffentlichen Schlüssel zum Beispiel mit dem Suchdienst 2302 teilen, und der Suchdienst 2302 kann einen Datensatz speichern, der angibt, dass der kryptografische öffentliche Schlüssel zu dem bestimmten Asset gehört.

[0267] Wenn das physische oder logische Asset dann authentifiziert werden muss, stellt das physische oder logische Asset den kryptografischen öffentlichen Schlüssel einem Autentifizierungsdienst zur Verfügung. Wie weiter unten unter Bezugnahme auf **Fig. 34** gezeigt, kann der Autentifizierungsdienst in den Suchdienst eingebettet sein. In anderen Implementierungen ist der Autentifizierungsdienst in einem anderen Container des SDCS untergebracht, der mit dem Suchdienst kommuniziert. Der Autentifizierungsdienst ruft den Datensatz aus dem Suchdienst-Datenspeicher 2304 ab, um festzustellen, ob der bereitgestellte kryptografische öffentliche Schlüssel für das physische oder logische Asset mit dem kryptografischen öffentlichen Schlüssel aus dem Suchdienst-Datenspeicher 2304 übereinstimmt. Das physische oder logische Asset stellt dem Autentifizierungsdienst auch eine digitale Signatur zur Verfügung, um zu beweisen, dass das physische oder logische Asset im Besitz des kryptographischen privaten Schlüssels ist, der dem kryptographischen öffentlichen Schlüssel entspricht. Wenn der Autentifizierungsdienst feststellt, dass der bereitgestellte kryptografische öffentliche Schlüssel für das physische oder logische Asset mit dem kryptografischen öffentlichen Schlüssel übereinstimmt, der im Datenspeicher 2304 für ermittelte Objekte beinhaltet ist, und die digitale Signatur beweist, dass das physische oder logische Asset im Besitz des kryptografischen privaten Schlüssels ist, der dem kryptografischen öffentlichen Schlüssel entspricht, authentifiziert der Autentifizierungsdienst das physische oder logische Asset.

[0268] In anderen Implementierungen kann dem physischen oder logischen Asset ein Pre-Shared Key (PSK) zugewiesen werden, den das physische oder logische Asset mit dem Suchdienst 2302 teilt. Der Suchdienst 2302 kann den PSK in Verbindung mit dem physischen oder logischen Asset in dem Datenspeicher 2304 für ermittelte Objekte speichern. Wenn dann das physische oder logische Asset mit anderen Knoten oder Diensten kommuniziert, kann das physische oder logische Asset die Kommunikation mit dem PSK verschlüsseln. Der Suchdienst 2302 kann dann den PSK, der in Verbindung mit dem physischen oder logischen Asset gespeichert

ist, aus dem Datenspeicher 2304 für ermittelte Objekte abrufen, die Kommunikation entschlüsseln und die entschlüsselte Kommunikation an den anderen Knoten oder Dienst weiterleiten. Auf diese Weise ist das physische oder logische Asset authentifiziert, da es den PSK verwendet hat, der nur zwischen dem physischen oder logischen Asset und dem Suchdienst 2302 zur Verschlüsselung der Kommunikation freigegeben wurde.

[0269] Zusätzlich zur Bestimmung der Identität des physischen oder logischen Assets kann der Suchdienst 2302 den Standort des physischen oder logischen Assets innerhalb des SDCS bestimmen. Der Standort kann beispielsweise die Netzwerkadresse für das physische oder logische Asset sein, wie eine IP-Adresse oder eine andere Kennung für das physische oder logische Asset innerhalb des Prozessanlagen-Netzwerks 22, 25, 30, 32, 35, 42-58. Neben dem Netzwerkstandort kann der Standort auch den physischen Standort des physischen oder logischen Assets beinhalten, z.B. einen bestimmten Bereich der Prozessanlage 10, in dem sich ein physisches Asset befindet, oder einen physischen Standort eines Rechenknotens, der ein logisches Asset speichert und/oder ausführt. Der Suchdienst 2302 bestimmt den Standort des physischen oder logischen Assets anhand der in der Ankündigung beinhalteten Informationen, wie z.B. einer Netzwerkadresse oder einer Beschreibung eines physischen Standorts.

[0270] Darüber hinaus kann der Suchdienst 2302 eine Reihe von Fähigkeiten des physischen oder logischen Assets identifizieren, wie z.B. Prozessparameter, die von dem physischen oder logischen Asset bereitgestellt werden (z.B. ein prozentualer Öffnungsgrad eines Ventils, ein prozentualer Füllgrad eines Tanks, etc.), Dienste, die von dem physischen oder logischen Asset bereitgestellt werden (z. B. Authentifizierung, Autorisierung, Steuerung, Analyse, Speicherung usw.), und/oder Dienste, die für die Kommunikation mit dem physischen oder logischen Asset konfiguriert sind. Zum Beispiel kann das physische oder logische Asset zumindest einige der Fähigkeiten des physischen oder logischen Assets in der Ankündigung als primäre Variablen beinhalten. Der Suchdienst 2302 kann auch Fähigkeiten des physischen oder logischen Assets identifizieren, die nicht in der Ankündigung beinhaltet sind, d.h. kontextuelle Variablen. Genauer gesagt, kann der Suchdienst 2302 Kontextvariablen von einem Kontextwörterbuchdienst abrufen, der aus der Art des physischen oder logischen Assets einen Satz von Fähigkeiten ableitet. Der Suchdienst 2302 kann dem Kontextwörterbuchdienst die Identität des physischen oder logischen Assets mitteilen, und der Kontextwörterbuchdienst kann den Typ des physischen oder logischen Assets auf der Grundlage der Identität bestimmen. Anschließend stellt der Kontextwörterbuchdienst dem Suchdienst 2302 die aus der Art des physischen oder logischen Assets abgeleitete Menge an Fähigkeiten zur Verfügung. Der Kontextwörterbuchdienst wird im Folgenden unter Bezugnahme auf die **Fig. 34-36** näher beschrieben.

[0271] In einigen Implementierungen benachrichtigt der Suchdienst 2302 nach der Identifizierung eines physischen oder logischen Assets einen Prozesssteuerungskonfigurationsdienst über das neu ermittelte physische oder logische Asset zur Inbetriebnahme und/oder Aufnahme in die SDCS-Topologie. Ein Nutzer kann dann die Aufnahme des neu ermittelten physischen oder logischen Assets in die SDCS-Topologie beim Prozesssteuerungskonfigurationsdienst akzeptieren oder ablehnen. In einigen Implementierungen können neu ermittelte physische oder logische Assets auch automatisch vom Prozesssteuerungskonfigurationsdienst in die SDCS-Topologie aufgenommen werden.

[0272] In jedem Fall speichert der Suchdienst 2302 einen Datensatz des physischen oder logischen Assets einschließlich der Identität des physischen oder logischen Assets, des Standorts des physischen oder logischen Assets und/oder des Satzes von Fähigkeiten des physischen oder logischen Assets in dem Datenspeicher für ermittelte Objekte 2304. Auf diese Weise verwaltet der Datenspeicher 2304 einen Datensatz für jedes physische oder logische Asset innerhalb der Prozessanlage 10. Andere physische oder logische Assets können bestimmte Prozessparameter oder Dienstleistungen anfordern, und der Suchdienst 2302 kann das physische oder logische Asset identifizieren, das die angeforderten Prozessparameter oder Dienstleistungen für das anfordernde physische oder logische Asset bereitstellt. Der Suchdienst 2302 kann auch Standortinformationen für das physische oder logische Asset bereitstellen, das die angeforderten Prozessparameter oder Dienste bereitstellt, so dass das anfordernde physische oder logische Asset die angeforderten Prozessparameter oder Dienste erhalten kann. Darüber hinaus kann der Suchdienst 2302 einen Datensatz des physischen oder logischen Assets an einen E/A-Server oder ein E/A-Gerät zur Inbetriebnahme des physischen oder logischen Assets übermitteln, z.B. wenn es sich bei dem physischen oder logischen Asset um ein Feldgerät handelt.

[0273] Wenn der Datenspeicher 2304 für ermittelte Objekte beschädigt oder zerstört wird, kann der Suchdienst 2302 automatisch über das Prozessanlagennetzwerk 22, 25, 30, 32, 35, 42-58 eine Aufforderung an alle physischen oder logischen Assets innerhalb der Prozessanlage 10 senden, ihre Anwesenheit zu melden. Dann kann der Suchdienst 2302 den Datensatz jedes der physischen oder logischen Assets innerhalb der Prozessanlage 10 schnell wiederherstellen, ohne manuelle Eingaben

und ohne den Betrieb der Prozessanlage 10 unterbrechen zu müssen.

[0274] In einigen Implementierungen kann die Anfrage des Suchdienstes 2302 an die physischen oder logischen Assets, ihre Anwesenheit zu melden, an die physischen oder logischen Assets weitergeleitet werden, die Vermittler haben. Zum Beispiel kann das entfernte E/A-Asset 78 aus **Fig. 1** die Suchanfrage an jedes der Feldgeräte 70 weiterleiten, die mit dem entfernten E/A-Asset 78 kommunizieren. Die Feldgeräte 70 können dann auf die Suchanfrage antworten, indem sie ihre Anwesenheit dem entfernten E/A-Asset 78 mitteilen, das die Ankündigungen an den Suchdienst 2302 weiterleitet.

[0275] **Fig. 34** zeigt ein detailliertes Blockdiagramm eines beispielhaften Suchdienst-Containers 2402, der so konfiguriert ist, dass er einen Suchdienst ähnlich dem Suchdienst 2302 von **Fig. 33** ausführt. Der Suchdienst-Container 2402 beinhaltet einen Suchdienst 2404, der einen Autentifizierungsdienst 2406 ausführen kann, einen Kontext-Wörterbuch-Container 2408, der einen Kontext 2410 beinhalten kann, und einen Standortdienst 2412.

[0276] Der Suchdienst 2404 kann Ankündigungen von physischen oder logischen Assets erhalten, die dem Prozessanlagennetzwerk 22, 25, 30, 32, 35, 42-58 beitreten. Eine Ankündigung kann ein Asset-Tag des physischen oder logischen Assets, eine MAC-Adresse des physischen oder logischen Assets, eine Netzwerkadresse des physischen oder logischen Assets, einen kryptographischen Schlüssel für das physische oder logische Asset, eine Seriennummer für das physische oder logische Asset und/oder einen Namen eines Dienstes oder Subsystems, der mit dem physischen oder logischen Asset verbunden ist, beinhalten. Der Suchdienst 2404 kann die Identität des physischen oder logischen Assets auf der Grundlage dieser in der Ankündigung beinhalteten Parameter bestimmen.

[0277] Der Suchdienst 2404 kann auch den Standort des physischen oder logischen Assets innerhalb des SDCS bestimmen. Der Standort kann beispielsweise die Netzwerkadresse für das physische oder logische Asset sein, wie eine IP-Adresse oder eine andere Kennung für das physische oder logische Asset innerhalb des Prozessanlagen-Netzwerks 22, 25, 30, 32, 35, 42-58. Neben dem Netzwerkstandort kann der Standort auch den physischen Standort des physischen oder logischen Assets beinhalten, z.B. einen bestimmten Bereich der Prozessanlage 10, in dem sich ein physisches Asset befindet, oder einen physischen Standort eines Rechenknotens, der ein logisches Asset speichert und/oder ausführt. Der Suchdienst 2404 bestimmt den Standort des physischen oder logischen Assets anhand der in der Ankündigung beinhalteten Informationen, wie z.B. einer Netzwerkadresse oder einer Beschreibung eines physischen Standorts.

[0278] Darüber hinaus kann der Suchdienst 2404 eine Reihe von Fähigkeiten des physischen oder logischen Assets identifizieren, wie z.B. Prozessparameter, die von dem physischen oder logischen Asset bereitgestellt werden (z.B. ein Prozentsatz der Ventilöffnung, ein Prozentsatz der Tankfüllung usw.), Dienste, die von dem physischen oder logischen Asset bereitgestellt werden (z.B. Authentifizierung, Autorisierung usw.) und/oder Dienste, die für die Kommunikation mit dem physischen oder logischen Asset konfiguriert sind. Zum Beispiel kann das physische oder logische Asset zumindest einige der Fähigkeiten des physischen oder logischen Assets in der Ankündigung beinhalten. Der Suchdienst 2404 kann auch automatisch auf Fähigkeiten des physischen oder logischen Assets schließen, die nicht in der Ankündigung beinhaltet sind. Wenn es sich bei dem physischen oder logischen Asset beispielsweise um ein Feldgerät handelt, kann die Ankündigung primäre Variablen beinhalten, die aus dem Feldgerät abrufbar sind, wie z.B. die Massendurchflussrate eines Fluids. Der Suchdienst 2404 kann auch automatisch Kontextvariablen für das Feldgerät ableiten, wie z.B. die Geschwindigkeit und/oder die Dichte des Fluids. Wenn es sich bei dem physischen oder logischen Asset beispielsweise um ein altes Gerät handelt, kann es sein, dass das alte Gerät nicht so konfiguriert ist, dass es bestimmte Fähigkeiten anzeigt. Dementsprechend kündigt das Altgerät primäre Variablen an, und der Suchdienst 2404 schließt automatisch auf verbleibende Fähigkeiten oder kontextbezogene Variablen, die nicht in der Ankündigung beinhaltet sind.

[0279] In einem anderen Beispiel, wenn das physische oder logische Asset ein Feldgerät ist, kann das Feldgerät primäre Variablen in einer ereignisgesteuerten Datenschicht (EDDL) ankündigen, wie z.B. eine Ventilposition und einen Luftdruck im Ventil. Der Suchdienst 2404 kann automatisch kontextabhängige Variablen für das Feldgerät ableiten, wie z.B. Metriken über den Zustand des Ventils, Metriken über den Ventilweg usw.

[0280] Genauer gesagt, kann der Suchdienst 2404 diese Fähigkeiten aus einem Kontext-Wörterbuch-Container 2408 abrufen. Der Kontext-Wörterbuch-Container 2408 beinhaltet einen Kontext 2410, der eine Reihe von Fähigkeiten aus einer Art von physischem oder logischem Asset ableitet. Für jede Art von physischem oder logischem Asset kann der Kontext 2410 eine Liste aller Prozessparameter beinhalten, die von dem physischen oder logischen Asset bereitgestellt werden, alle Dienste, die von dem physischen oder logischen Asset ausgeführt werden, und alle Dienste innerhalb des SDCS, die das physi-

sche oder logische Asset zur Übermittlung von Informationen aufrufen.

[0281] Der Suchdienst 2404 kann die Identität des physischen oder logischen Assets an den Kontext-Wörterbuch-Container 2408 übermitteln, und der Kontext-Wörterbuch-Container 2408 kann den Typ des physischen oder logischen Assets auf der Grundlage der Identität bestimmen. Der Kontext-Wörterbuch-Container 2408 kann zum Beispiel eine Reihe von Regeln zur Bestimmung des Typs des physischen oder logischen Assets auf der Grundlage der Identität des physischen oder logischen Assets speichern. Genauer gesagt, kann der Kontext-Wörterbuch-Container 2408 das Asset-Tag, die Seriennummer oder den Namen eines Dienstes oder Subsystems analysieren, das mit dem physischen oder logischen Asset verbunden ist, um die Art des physischen oder logischen Assets zu bestimmen. Wenn das Asset-Tag für das physische oder logische Asset beispielsweise „CTRL-VALVE-01“ lautet, kann der Kontext-Wörterbuch-Container 2408 feststellen, dass der Typ des physischen oder logischen Assets ein Steuerventil ist. Der Kontext-Wörterbuch-Container 2408 kann eine Liste von physischen oder logischen Asset-Typen und Asset-Tags, Seriennummern, Namen oder Bereichen davon speichern, die jedem physischen oder logischen Asset-Typ entsprechen.

[0282] Anschließend leitet der Kontext-Wörterbuch-Container 2408 aus dem Typ des physischen oder logischen Assets unter Verwendung des Kontexts 2410 automatisch den Satz von Fähigkeiten ab und stellt dem Suchdienst 2404 den Satz von Fähigkeiten zur Verfügung, der aus dem Typ des physischen oder logischen Assets abgeleitet wurde. Der Suchdienst 2404 speichert dann einen Datensatz des physischen oder logischen Assets einschließlich der Identität des physischen oder logischen Assets, des Standorts des physischen oder logischen Assets und/oder des Satzes von Fähigkeiten des physischen oder logischen Assets in einem Datenspeicher für gefundene Objekte.

[0283] Wenn ein physisches oder logisches Asset den Zugriff auf einen Knoten oder Dienst innerhalb des SDCS beantragt, authentifiziert der Autentifizierungsdienst 2406 innerhalb des Suchdienstes 2404 das physische oder logische Asset. Zum Beispiel authentifiziert der Autentifizierungsdienst 2406 das physische oder logische Asset, indem er einen kryptographischen öffentlichen Schlüssel für das physische oder logische Asset abruft, der im Datenspeicher für ermittelte Objekte beinhaltet ist. Der Autentifizierungsdienst 2406 kann dann den abgerufenen kryptografischen öffentlichen Schlüssel für das physische oder logische Asset mit dem kryptografischen öffentlichen Schlüssel vergleichen, den das physische oder logische Asset in der Anfrage für den Zugriff auf den Knoten oder den Dienst angegeben hat, um festzustellen, ob es eine Übereinstimmung gibt. Der Autentifizierungsdienst 2406 kann auch eine digitale Signatur analysieren, die von dem physischen oder logischen Asset in der Anfrage für den Zugriff auf den Knoten oder den Dienst bereitgestellt wurde, um festzustellen, ob die digitale Signatur beweist, dass das physische oder logische Asset im Besitz des kryptographischen privaten Schlüssels ist, der dem kryptographischen öffentlichen Schlüssel entspricht. Wenn diese beiden Bedingungen erfüllt sind, kann der Autentifizierungsdienst 2406 das physische oder logische Asset authentifizieren.

[0284] In einem anderen Beispiel authentifiziert der Autentifizierungsdienst 2406 das physische oder logische Asset, indem er einen PSK für das physische oder logische Asset aus dem Datenspeicher für ermittelte Objekte abruft. Der Autentifizierungsdienst 2406 kann dann versuchen, die Anfrage für den Zugriff auf den Knoten oder Dienst mit Hilfe des abgerufenen PSK zu entschlüsseln. Wenn der Autentifizierungsdienst 2406 die Anfrage erfolgreich entschlüsselt, kann der Autentifizierungsdienst 2406 das physische oder logische Asset authentifizieren.

[0285] Der Autentifizierungsdienst 2406 ist zwar als Teil des Suchdienstes 2404 dargestellt, dies ist jedoch nur eine beispielhafte Implementierung zur Veranschaulichung. In anderen Implementierungen ist der Autentifizierungsdienst 2406 nicht in den Suchdienst 2404 eingebettet.

[0286] Der Ortungsdienst 2412 kann eine Anfrage nach dem Standort eines physischen oder logischen Assets von einem Knoten oder Dienst innerhalb des SDCS erhalten. Der Ortungsdienst 2412 kann dann einen Datensatz aus dem Datenspeicher für ermittelte Objekte über den Standort des physischen oder logischen Assets erhalten. Der Standort kann zum Beispiel die Netzwerkadresse des physischen oder logischen Assets sein, wie eine IP-Adresse oder eine andere Kennung für das physische oder logische Asset innerhalb des Prozessanlagennetzwerks 22, 25, 30, 32, 35, 42-58. Neben dem Netzwerkstandort kann der Standort auch den physischen Standort des physischen oder logischen Assets beinhalten, z.B. einen bestimmten Bereich der Prozessanlage 10, in dem sich ein physisches Asset befindet, oder einen physischen Standort eines Rechenknotens, der ein logisches Asset speichert und/oder ausführt. Der Ortungsdienst 2412 liefert dann als Antwort auf die Anfrage Standortinformationen für das physische oder logische Asset an den Knoten oder Dienst, der die Anfrage gestellt hat.

[0287] **Fig. 35** zeigt ein detailliertes Blockdiagramm eines beispielhaften Kontextwörterbuch-Containers 2502, der dem Kontextwörterbuch-Container 2408

von **Fig. 34** ähnelt. Wie der Kontext-Wörterbuch-Container 2408 beinhaltet der Kontext-Wörterbuch-Container 2502 einen Kontext-Wörterbuch-Dienst 2504 und einen Kontext 2508. Der Kontextwörterbuchdienst 2504 beinhaltet außerdem einen Dienst zur Identifizierung von Asset-Fähigkeiten 2506.

[0288] Der Asset-Fähigkeiten-Identifizierungsdienst 2506 kann den Typ des physischen oder logischen Assets auf der Grundlage der Identität des physischen oder logischen Assets bestimmen. Zum Beispiel kann der Asset-Fähigkeiten-Identifikationsdienst 2506 einen Satz von Regeln zur Bestimmung des Typs des physischen oder logischen Assets auf der Grundlage der Identität des physischen oder logischen Assets speichern. Genauer gesagt, kann der Asset-Fähigkeiten-Identifizierungsdienst 2506 das Asset-Tag, die Seriennummer oder den Namen eines Dienstes oder Subsystems analysieren, das mit dem physischen oder logischen Asset verbunden ist, um die Art des physischen oder logischen Assets zu bestimmen. Wenn der Asset-Tag für das physische oder logische Asset beispielsweise „CTRL-VALVE-01“ lautet, kann der Asset-Fähigkeiten-Identifizierungsdienst 2506 feststellen, dass es sich bei dem Typ des physischen oder logischen Assets um ein Steuerventil handelt. Der Asset-Fähigkeiten-Identifizierungsdienst 2506 kann eine Liste von physischen oder logischen Asset-Typen und Asset-Tags, Seriennummern, Namen oder Bereichen davon speichern, die jedem physischen oder logischen Asset-Typ entsprechen.

[0289] Zusätzlich oder alternativ kann der Asset-Fähigkeiten-Identifizierungsdienst 2506 die primären Variablen für das physische oder logische Asset analysieren, die in der Ankündigung beinhaltet sind, um den Typ des physischen oder logischen Assets zu bestimmen, wie z.B. die primären Variablen, die in einer EDDL beinhaltet sind. Wenn beispielsweise eine primäre Variable für das physische oder logische Asset die Ventilposition ist, kann der Asset-Fähigkeiten-Identifizierungsdienst 2506 feststellen, dass das physische oder logische Asset ein Ventil ist. Wenn eine primäre Variable für das physische oder logische Asset ein Steuerungsdienst ist, kann der Asset-Fähigkeiten-Identifizierungsdienst 2506 feststellen, dass das physische oder logische Asset ein Steuerungscontainer ist. Einige physische oder logische Assets können eine Kombination von Fähigkeiten beinhalten, z.B. eine Ventilstellungsfähigkeit und eine Steuerungsleistungsfähigkeit. In diesem Fall kann der Asset-Fähigkeiten-Identifizierungsdienst 2506 die Art des physischen oder logischen Assets auf der Grundlage der Kombination von Fähigkeiten bestimmen.

[0290] Der Asset-Fähigkeiten-Identifizierungsdienst 2506 kann dann die Fähigkeiten aus dem Typ des physischen oder logischen Assets unter Verwendung des Kontexts 2508 ableiten. Zum Beispiel kann die Ankündigung für ein bestimmtes physisches oder logisches Asset anzeigen, dass das physische oder logische Asset einen ersten Satz von Parametern für die Steuerung des physischen oder logischen Assets bereitstellen kann. Der Kontext 2508 kann außerdem zusätzliche Parameter für die Wartung des physischen oder logischen Assets angeben. In einem anderen Beispiel kann der Kontext 2508 Mechanismen für den Zugriff auf jeden der zusätzlichen Parameter oder Dienste beinhalten, z.B. Mechanismen für den Zugriff auf die Wartungsparameter. Ein Mechanismus für den Zugriff auf einen zusätzlichen Parameter oder Dienst kann das Format und/oder der Inhalt einer Anfrage sein, die an das physische oder logische Asset gestellt wird, um den zusätzlichen Parameter oder Dienst abzurufen. In einem anderen Beispiel kann der Mechanismus ein Bezugszeichen oder ein Identifikator sein, die bzw. der dem zusätzlichen Parameter oder Dienst entspricht und die bzw. der verwendet werden kann, um den zusätzlichen Parameter abzurufen oder das physische oder logische Asset den zusätzlichen Dienst ausführen zu lassen.

[0291] **Fig. 36** zeigt ein detailliertes Blockdiagramm eines Beispielkontextes 2602, der dem Kontext 2508 von **Fig. 35** ähnelt. Der Kontext 2602 kann eine Datentabelle 2604 beinhalten, die Gerätetypen mit Klassenkontexten assoziiert. Genauer gesagt, kann die Datentabelle 2604 Gerätetypen, primäre Variablen und kontextbezogene Variablen beinhalten. Wenn es sich bei dem Gerätetyp beispielsweise um ein Thermoelement handelt, kann die primäre Variable die Temperatur sein und die Kontextvariablen können Gerätezustandsmetriken für das Thermoelement und eine Gerätetoleranz beinhalten, die die Variabilität des Thermoelements angibt. Wenn es sich bei dem Gerätetyp um einen Massendurchflusssensor handelt, kann die primäre Variable der Massendurchfluss sein und die Kontextvariablen können die Fluidgeschwindigkeit, die Fluidschnelle und die Fluiddichte beinhalten. Wenn es sich bei dem Gerätetyp um ein Ventil handelt, können die primären Variablen die Ventilposition und der Luftdruck im Ventil sein. Zu den Kontextvariablen können Metriken zum Zustand des Ventils, Metriken zum Ventilhub, eine Betriebsart des Ventils wie Vollhubzyklus, kontinuierliche Drosselung, periodische Drosselung usw. sowie Zustände im Ventil wie Totbereich und Totzeit gehören. Darüber hinaus können die Kontextvariablen Dienste beinhalten, die das Ventil ausführen kann, wie z.B. einen Ventilüberwachungsdienst und/oder Dienste, die die primären oder kontextbezogenen Variablen des Ventils nutzen können.

[0292] Das SDCS kann auch einen Empfehlungsdienst beinhalten, der die primären und kontextuellen Variablen für ein physisches oder logisches Asset aus dem KontextWörterbuchdienst 2504 und/oder

dem Suchdienst 2404 bezieht und einem Nutzer während einer Konfiguration Merkmale empfiehlt. Wenn ein Nutzer beispielsweise ein neues Ventil für das SDCS konfiguriert, kann der Kontextwörterbuchdienst 2504 anhand der Kontextvariablen für das neue Ventil erkennen, dass es einen Rücklesewert gibt. Während der Nutzer das neue Ventil konfiguriert, kann der Empfehlungsdienst den Nutzer daran erinnern, dass es einen unbenutzten Rücklesewert für die Ventilposition gibt, der verfügbar ist, aber nicht benutzt wird, wenn der Nutzer versucht, die Konfiguration in den Prozesssteuerungskonfigurationsdienst zu übertragen. Auf diese Weise kann der Nutzer, wenn er die Fähigkeiten eines physischen oder logischen Assets nicht vollständig kennt, mit Hilfe des Empfehlungsdienstes die Fähigkeiten des physischen oder logischen Assets kennen lernen, ohne das Handbuch für jedes der im SDCS konfigurierten oder in Betrieb genommenen Assets lesen zu müssen.

[0293] **Fig. 37** zeigt ein Flussdiagramm, das ein Beispielverfahren 2700 zur Bereitstellung von Discovery-Software als Dienst in einer Prozessanlage 10 darstellt. Das Verfahren kann von einem Suchdienst ausgeführt werden.

[0294] Im Block 2702 erhält der Suchdienst eine Ankündigung, die auf das Vorhandensein eines physischen oder logischen Assets hinweist. Wenn ein neues physisches oder logisches Asset, wie z.B. ein Feldgerät, eine Prozesssteuerungseinrichtung, ein Rechenknoten, ein Container, ein Dienst, ein Microdienst usw. zum Prozessanlagennetzwerk 22, 25, 30, 32, 35, 42-58 hinzugefügt wird, kann das neue physische oder logische Asset seine Anwesenheit ankündigen, indem es z.B. seine Netzwerkadresse an Knoten oder Dienste sendet, die mit dem Prozessanlagennetzwerk 22, 25, 30, 32, 35, 42-58 verbunden sind. In anderen Implementierungen kann der Suchdienst eine Anfrage an alle physischen oder logischen Assets im Prozessanlagennetzwerk 22, 25, 30, 32, 35, 42-58 senden, um deren Anwesenheit anzukündigen.

[0295] Die Ankündigung kann einen identifizierenden Parameter für das physische oder logische Asset beinhalten, wie z.B. ein Asset-Tag des physischen oder logischen Assets, eine MAC-Adresse des physischen oder logischen Assets, eine Netzwerkadresse des physischen oder logischen Assets, einen kryptografischen Schlüssel für das physische oder logische Asset, eine Seriennummer für das physische oder logische Asset und/oder einen Namen eines Dienstes oder Subsystems, der mit dem physischen oder logischen Asset verbunden ist. Die Ankündigung kann auch eine Netzwerkadresse für das physische oder logische Asset oder jede andere geeignete Standortinformation für das physische oder logische Asset beinhalten, einschließlich physischer oder Netzwerk-Standortinformationen. Darüber hinaus kann die Ankündigung Fähigkeiten des physischen oder logischen Assets beinhalten, wie z.B. Prozessparameter, die das physische oder logische Asset bereitstellen kann, Dienste, die das physische oder logische Asset bereitstellen kann, oder Dienste, die mit dem physischen oder logischen Asset kommunizieren können.

[0296] Im Block 2704 ermittelt der Suchdienst die Identität des physischen oder logischen Assets auf der Grundlage der in der Ankündigung beinhalteten Identifizierungsparameter. In einigen Implementierungen ermittelt der Suchdienst die Identität des physischen oder logischen Assets anhand eines der Identifizierungsparameter, die das physische oder logische Asset eindeutig identifizieren (z.B. eine MAC-Adresse). In anderen Fällen ermittelt der Suchdienst die Identität des physischen oder logischen Assets auf der Grundlage einer Kombination der Identifizierungsparameter. Zum Beispiel kann die Seriennummer mehreren Assets derselben Marke und desselben Modells entsprechen. Dementsprechend kann der Suchdienst die Identität des physischen oder logischen Assets auf der Grundlage einer Kombination aus der Seriennummer und dem kryptografischen Schlüssel für das physische oder logische Asset bestimmen.

[0297] Im Block 2706 speichert der Suchdienst dann einen Datensatz des physischen oder logischen Assets in einem Datenspeicher für ermittelte Objekte. Der Datensatz kann einen Hinweis auf die Identität des physischen oder logischen Assets, einen Satz von Fähigkeiten des physischen oder logischen Assets und einen Standort des physischen oder logischen Assets innerhalb des SDCS beinhalten. Der Satz von Fähigkeiten des physischen oder logischen Assets kann die in der Ankündigung beinhalteten Fähigkeiten beinhalten. Die Menge der Fähigkeiten kann auch Fähigkeiten beinhalten, die vom Suchdienst automatisch abgeleitet werden und die nicht in der Ankündigung beinhaltet sind.

[0298] Genauer gesagt, kann der Suchdienst diese Fähigkeiten aus einem Kontext-Wörterbuch-Container abrufen. Der Kontext-Wörterbuch-Container beinhaltet einen Kontext, der eine Reihe von Fähigkeiten aus einem Typ von physischem oder logischem Asset ableitet. Für jede Art von physischem oder logischem Asset kann der Kontext eine Liste aller Prozessparameter beinhalten, die von dem physischen oder logischen Asset bereitgestellt werden, alle Dienste, die von dem physischen oder logischen Asset ausgeführt werden, und alle Dienste innerhalb des SDCS, die das physische oder logische Asset zur Übermittlung von Informationen aufrufen.

[0299] **Fig. 38** zeigt ein Flussdiagramm, das ein Beispielverfahren 2800 zum Ableiten von Informationen

über ein physisches oder logisches Asset einer Prozessanlage unter Verwendung eines Kontextwörterbuchs darstellt. Das Verfahren kann von einem Suchdienst ausgeführt werden.

[0300] Im Block 2802 erhält der Suchdienst eine Ankündigung, die auf das Vorhandensein eines physischen oder logischen Assets hinweist. Wenn ein neues physisches oder logisches Asset, wie z.B. ein Feldgerät, eine Prozesssteuerungseinrichtung, ein Rechenknoten, ein Container, ein Dienst, ein Microdienst usw. zum Prozessanlagennetzwerk 22, 25, 30, 32, 35, 42-58 hinzugefügt wird, kann das neue physische oder logische Asset seine Anwesenheit ankündigen, indem es z.B. seine Netzwerkadresse an Knoten oder Dienste sendet, die mit dem Prozessanlagennetzwerk 22, 25, 30, 32, 35, 42-58 verbunden sind. In anderen Implementierungen kann der Suchdienst eine Anfrage an alle physischen oder logischen Assets im Prozessanlagennetzwerk 22, 25, 30, 32, 35, 42-58 senden, um deren Anwesenheit anzukündigen.

[0301] Die Ankündigung kann einen identifizierenden Parameter für das physische oder logische Asset beinhalten, wie z.B. ein Asset-Tag des physischen oder logischen Assets, eine MAC-Adresse des physischen oder logischen Assets, eine Netzwerkadresse des physischen oder logischen Assets, einen kryptografischen Schlüssel für das physische oder logische Asset, eine Seriennummer für das physische oder logische Asset und/oder einen Namen eines Dienstes oder Subsystems, der mit dem physischen oder logischen Asset verbunden ist. Die Ankündigung kann auch eine Netzwerkadresse für das physische oder logische Asset oder jede andere geeignete Standortinformation für das physische oder logische Asset beinhalten, einschließlich physischer oder Netzwerk-Standortinformationen. Darüber hinaus kann die Ankündigung Fähigkeiten des physischen oder logischen Assets beinhalten, wie z.B. Prozessparameter, die das physische oder logische Asset bereitstellen kann, Dienste, die das physische oder logische Asset bereitstellen kann, oder Dienste, die mit dem physischen oder logischen Asset kommunizieren können.

[0302] Im Block 2804 ruft der Suchdienst zusätzliche Parameter oder Dienste ab, die mit dem physischen oder logischen Asset verbunden sind und die in der Ankündigung nicht als Fähigkeiten des physischen oder logischen Assets angegeben wurden. Genauer gesagt, kann der Suchdienst die zusätzlichen Parameter oder Dienste aus einem Kontext-Wörterbuch-Container abrufen.

[0303] Der Kontext-Wörterbuch-Container beinhaltet einen Kontext, der von einem Typ eines physischen oder logischen Assets auf einen Satz von Fähigkeiten schließt. Für jede Art von physischem oder logischem Asset kann der Kontext eine Liste aller von dem physischen oder logischen Asset bereitgestellten Prozessparameter, aller von dem physischen oder logischen Asset erbrachten Dienste und aller Dienste innerhalb des SDCS beinhalten, die das physische oder logische Asset zur Übermittlung von Informationen aufrufen.

[0304] Der Suchdienst kann die Identität des physischen oder logischen Assets an den Kontext-Wörterbuch-Container übermitteln, und der Kontext-Wörterbuch-Container kann anhand der Identität den Typ des physischen oder logischen Assets bestimmen.

[0305] Der Kontext-Wörterbuch-Container kann zum Beispiel eine Reihe von Regeln zur Bestimmung des Typs des physischen oder logischen Assets auf der Grundlage der Identität des physischen oder logischen Assets speichern. Genauer gesagt, kann der Kontext-Wörterbuch-Container das Asset-Tag, die Seriennummer oder den Namen eines Dienstes oder Subsystems analysieren, das mit dem physischen oder logischen Asset verbunden ist, um die Art des physischen oder logischen Assets zu bestimmen. Wenn das Asset-Tag für das physische oder logische Asset beispielsweise „CTRL-VALVE-01“ lautet, kann der Kontextwörterbuch-Container feststellen, dass es sich bei dem Typ des physischen oder logischen Assets um ein Steuerventil handelt. Der Kontext-Wörterbuch-Container kann eine Liste von physischen oder logischen Asset-Typen und Asset-Tags, Seriennummern, Namen oder Bereichen davon speichern, die jedem physischen oder logischen Asset-Typ entsprechen.

[0306] Anschließend leitet der Kontext-Wörterbuch-Container aus dem Typ des physischen oder logischen Assets unter Verwendung des Kontexts automatisch den Satz von Fähigkeiten ab und stellt dem Suchdienst den Satz von Fähigkeiten zur Verfügung, der aus dem Typ des physischen oder logischen Assets abgeleitet wurde. Zum Beispiel kann die Ankündigung für ein bestimmtes physisches oder logisches Asset anzeigen, dass das physische oder logische Asset einen ersten Satz von Parametern für die Steuerung des physischen oder logischen Assets bereitstellen kann. Der Kontext kann außerdem zusätzliche Parameter für die Wartung des physischen oder logischen Assets beinhalten. In einem anderen Beispiel kann der Kontext Mechanismen für den Zugriff auf jeden der zusätzlichen Parameter oder Dienste beinhalten, wie z.B. Mechanismen für den Zugriff auf die Wartungsparameter.

[0307] Im Block 2806 speichert der Suchdienst dann einen Datensatz des physischen oder logischen Assets in einem Datenspeicher für ermittelte Objekte. Der Datensatz kann einen Hinweis auf die Identität des physischen oder logischen Assets und die zusätzlichen Parameter oder Dienste beinhalten,

die mit dem physischen oder logischen Asset verbunden sind und nicht in der Ankündigung beinhaltet waren. Der Datensatz kann auch die in der Ankündigung beinhalteten Fähigkeiten beinhalten.

[0308] Fig. 39 zeigt ein Flussdiagramm, das ein Beispielverfahren 2900 zur Ableitung eines Satzes von Fähigkeiten von jedem Typ eines physischen oder logischen Assets in einer Prozessanlage und zur Bestimmung der Fähigkeiten eines ermittelten physischen oder logischen Assets darstellt. Das Verfahren kann von einem Kontext-Wörterbuchdienst ausgeführt werden.

[0309] Im Block 2902 speichert der Kontextwörterbuchdienst jede Art von physischem oder logischem Asset der Prozessanlage 10. Dann speichert der Kontextwörterbuchdienst für jede Art von physischem oder logischem Asset einen Satz von Fähigkeiten der Art des physischen oder logischen Assets (Block 2904). Der Satz von Fähigkeiten kann Parameter beinhalten, die von der Art des physischen oder logischen Assets abrufbar sind, und Dienste, die mit der Art des physischen oder logischen Assets verbunden sind, wie z.B. Dienste, die von dem physischen oder logischen Asset ausgeführt werden oder Dienste, die mit dem physischen oder logischen Asset kommunizieren. Der Kontextwörterbuchdienst kann anhand eines Kontexts entsprechende Fähigkeiten für jeden Typ von physischem oder logischem Asset ableiten.

[0310] Im Block 2906 erhält der Dienst des Kontextwörterbuchs dann eine Anfrage nach den Fähigkeiten eines bestimmten physischen oder logischen Assets. Die Anfrage kann Identifikationsinformationen für das physische oder logische Asset beinhalten, wie z.B. ein Asset-Tag, eine MAC-Adresse des physischen oder logischen Assets, eine Netzwerkadresse des physischen oder logischen Assets, einen kryptographischen Schlüssel für das physische oder logische Asset, eine Seriennummer für das physische oder logische Asset und/oder einen Namen eines Dienstes oder Subsystems, der mit dem physischen oder logischen Asset verbunden ist. Die Anfrage kann vom Suchdienst gestellt werden. In anderen Szenarien kann die Anfrage von einem Knoten oder Dienst innerhalb des SDCS gestellt werden, der versucht, ein bestimmtes physisches oder logisches Asset mit einer bestimmten Fähigkeit zu finden. In wieder anderen Szenarien kann die Anfrage von einem Knoten oder Dienst innerhalb des SDCS gestellt werden, der daran interessiert ist, auf Prozessparameter oder Dienste zuzugreifen, die von dem physischen oder logischen Asset bereitgestellt werden.

[0311] Als Antwort auf die Anfrage bestimmt der Kontextwörterbuchdienst den Typ des physischen oder logischen Assets auf der Grundlage der Identifikationsinformationen für das physische oder logische Asset (Block G2908). Der Kontext-Wörterbuchdienst kann zum Beispiel eine Reihe von Regeln zur Bestimmung des Typs des physischen oder logischen Assets auf der Grundlage der Identität des physischen oder logischen Assets speichern. Genauer gesagt kann der Kontextwörterbuchdienst das Asset-Tag, die Seriennummer oder den Namen eines Dienstes oder Subsystems analysieren, das mit dem physischen oder logischen Asset verbunden ist, um den Typ des physischen oder logischen Assets zu bestimmen. Der Kontextwörterbuchdienst kann eine Liste von physischen oder logischen Asset-Typen und Asset-Tags, Seriennummern, Namen oder Bereichen davon speichern, die jedem physischen oder logischen Asset-Typ entsprechen.

[0312] Im Block 2910 kann der Dienst des Kontextverzeichnisses dann aus dem Typ des physischen oder logischen Assets unter Verwendung des Kontexts den Satz von Fähigkeiten ableiten. Der Kontextwörterbuchdienst kann dann eine Antwort auf die Anfrage liefern, die den Satz an Fähigkeiten beinhaltet, der dem Typ des physischen oder logischen Assets entspricht.

[0313] In einigen Implementierungen wird der Kontextwörterbuchdienst über einen ersten Container ausgeführt, der in einem zweiten Container für einen Suchdienst verschachtelt ist. In anderen Implementierungen werden der Kontextwörterbuchdienst und der Suchdienst nicht in verschachtelten Containern ausgeführt.

[0314] Fig. 40 zeigt ein Flussdiagramm, das ein Beispielverfahren 3000 für die Fehlerbehebung von gefundenen Elementen in einer Prozessanlage 10 darstellt. Das Verfahren kann von einem Suchdienst ausgeführt werden.

[0315] Im Block 3002 wird ein Fehler in einem Datenspeicher für ermittelte Objekte festgestellt. Der Datenspeicher für ermittelte Objekte kann z.B. beschädigt oder zerstört sein oder es fehlen Datensätze von physischen oder logischen Assets. Außerdem kann der Datenspeicher für ermittelte Objekte z.B. aufgrund eines Energieausfalls zurückgesetzt worden sein. Als Reaktion auf die Erkennung des Fehlers sendet der Suchdienst eine Aufforderung an physische oder logische Assets innerhalb der Prozessanlage 10, ihre Anwesenheit zu melden (Block 3004).

[0316] Als Reaktion auf die Anfrage empfängt der Suchdienst Ankündigungen von das physische oder logische Assets in der Prozessanlage 10 (Block 3006). Jede Ankündigung kann einen identifizierenden Parameter für das physische oder logische Asset beinhalten, wie z.B. ein Asset-Tag des physischen oder logischen Assets, eine MAC-Adresse

des physischen oder logischen Assets, eine Netzwerkadresse des physischen oder logischen Assets, einen kryptographischen Schlüssel für das physische oder logische Asset, eine Seriennummer für das physische oder logische Asset und/oder einen Namen eines Dienstes oder Subsystems, der mit dem physischen oder logischen Asset verbunden ist. Die Ankündigung kann auch eine Netzwerkadresse für das physische oder logische Asset oder jede andere geeignete Standortinformation für das physische oder logische Asset beinhalten, einschließlich physischer oder Netzwerk-Standortinformationen. Darüber hinaus kann die Ankündigung Fähigkeiten des physischen oder logischen Assets beinhalten, wie z.B. Prozessparameter, die das physische oder logische Asset bereitstellen kann, Dienste, die das physische oder logische Asset bereitstellen kann, oder Dienste, die mit dem physischen oder logischen Asset kommunizieren können.

[0317] Im Block 3008 speichert der Suchdienst dann einen wiederhergestellten Datensatz der physischen oder logischen Assets in einem Datenspeicher für ermittelte Objekte. Für jedes physische oder logische Asset kann der wiedergefundene Datensatz einen Hinweis auf die Identität des physischen oder logischen Assets, einen Satz von Fähigkeiten des physischen oder logischen Assets und einen Standort des physischen oder logischen Assets innerhalb des SDCS beinhalten. Der Satz von Fähigkeiten des physischen oder logischen Assets kann die Fähigkeiten beinhalten, die in der Ankündigung beinhaltet sind. Der Satz von Fähigkeiten kann auch Fähigkeiten beinhalten, die vom Suchdienst automatisch abgeleitet werden und nicht in der Ankündigung beinhaltet sind. Auf diese Weise wird die Aufzeichnung der physischen oder logischen Assets automatisch empfangen, ohne dass eine manuelle Eingabe erforderlich ist.

[0318] Wie bereits erwähnt, kann der Suchdienst bei der Inbetriebnahme von physischen oder logischen Assets innerhalb der Prozessanlage 10 behilflich sein, so dass das SDCS physische oder logische Assets automatisch und ohne manuelle Eingaben in Betrieb nehmen kann. Das SDCS und insbesondere ein E/A-Serverdienst kann physische oder logische Assets in Betrieb nehmen, nachdem der Suchdienst die physischen oder logischen Assets ermittelt hat, dies ist jedoch nur ein Beispiel für eine Implementierung. In anderen Implementierungen können andere Dienste physische oder logische Assets innerhalb der Prozessanlage 10 identifizieren, wie z.B. ein Prozesssteuerungskonfigurationsdienst.

[0319] **Fig. 41** zeigt ein Flussdiagramm, das ein Beispielverfahren 3100 für die automatische Inbetriebnahme eines SDCS darstellt. Das Verfahren kann von einem Suchdienst, einem Prozesssteuerungskonfigurationsdienst, einem E/A-Serverdienst oder einer geeigneten Kombination dieser Dienste ausgeführt werden.

[0320] Im Block 3102 wird eine Ankündigung eingeholt, die das Vorhandensein eines physischen oder logischen Assets anzeigt. Wenn ein neues physisches oder logisches Asset, wie z.B. ein Feldgerät, eine Prozesssteuerungseinrichtung, ein Rechenknoten, ein Container, ein Dienst, ein Microdienst usw. zum Prozessanlagennetzwerk 22, 25, 30, 32, 35, 42-58 hinzugefügt wird, kann das neue physische oder logische Asset seine Anwesenheit ankündigen, indem es z.B. seine Netzwerkadresse an Knoten oder Dienste sendet, die mit dem Prozessanlagennetzwerk 22, 25, 30, 32, 35, 42-58 verbunden sind. In anderen Implementierungen kann der Suchdienst eine Anfrage an alle physischen oder logischen Assets im Prozessanlagennetzwerk 22, 25, 30, 32, 35, 42-58 senden, um deren Anwesenheit anzukündigen.

[0321] Die Ankündigung kann identifizierende Parameter für das physische oder logische Asset beinhalten, wie z.B. ein Asset-Tag des physischen oder logischen Assets, eine MAC-Adresse des physischen oder logischen Assets, einen kryptografischen Schlüssel für das physische oder logische Asset, eine Seriennummer für das physische oder logische Asset und/oder einen Namen eines Dienstes oder Subsystems, der mit dem physischen oder logischen Asset verbunden ist. Die Ankündigung kann auch eine Netzwerkadresse für das physische oder logische Asset oder jede andere geeignete Standortinformation für das physische oder logische Asset beinhalten, einschließlich physischer oder Netzwerk-Standortinformationen. Beispielsweise kann die Standortinformation auch den physischen Standort des physischen oder logischen Assets beinhalten, wie z.B. einen bestimmten Bereich der Prozessanlage 10, in dem sich ein physisches Asset befindet, oder einen physischen Standort eines Rechenknotens, der ein logisches Asset speichert und/oder ausführt.

[0322] Im Block 3104 werden die Identifizierungsparameter und die Standortparameter für das physische oder logische Asset an einen E/A-Serverdienst, wie den E/A-Serverdienst 242 aus **Fig. 2**, übermittelt. Der Suchdienst oder Prozesssteuerungskonfigurationsdienst kann jeden der in der Ankündigung beinhalteten Identifizierungsparameter für das physische oder logische Asset an den E/A-Serverdienst übermitteln oder eine Teilmenge der in der Ankündigung beinhalteten Identifizierungsparameter übermitteln, die zur eindeutigen Identifizierung des physischen oder logischen Assets verwendet werden können. Zusätzlich kann der Suchdienst oder der Prozesssteuerungskonfigurationsdienst Standortinformationen an den E/A-Serverdienst übermitteln, damit der

E/A-Serverdienst mit dem physischen oder logischen Asset kommunizieren kann.

[0323] Im Block 3106 kann der E/A-Serverdienst das physische oder logische Asset auf der Grundlage der Identifikations- und Standortinformationen automatisch in Betrieb nehmen. Die Inbetriebnahme kann Aktionen oder Aktivitäten beinhalten, wie z.B. das Verifizieren oder Bestätigen der Identität des physischen oder logischen Assets, das Erzeugen von Tags, die das physische oder logische Asset innerhalb der Prozessanlage 10 eindeutig identifizieren, und das Durchführen von Tests, um sicherzustellen, dass der E/A-Serverdienst mit dem physischen oder logischen Asset kommuniziert.

[0324] Der E/A-Serverdienst kann auf der Grundlage der Identifizierungsparameter für das physische oder logische Asset ein Tag zur eindeutigen Identifizierung des physischen oder logischen Assets erzeugen. Wie bereits erwähnt, können die Identifizierungsparameter für das physische oder logische Asset beispielsweise ein Asset-Tag wie „CTRL-VALVE“ beinhalten, und die Prozessanlage 10 kann mehrere Steuerventile mit demselben Asset-Tag beinhalten. Der E/A-Serverdienst kann das Tag für das Ventil auf der Grundlage einer Kombination aus dem Asset-Tag und dem kryptografischen öffentlichen Schlüssel für das Ventil erzeugen. Wenn zum Beispiel die letzten vier Zeichen des kryptografischen öffentlichen Schlüssels für das Ventil „xg4t“ lauten, kann das Tag „CTRL-VALVE-xg4t“ lauten.

[0325] In anderen Implementierungen kann der E/A-Serverdienst Tags für Steuerventile erzeugen, die die Zeichenfolge „CTRL-VALVE“ gefolgt von einer Zahl beinhalten, die nicht zur Identifizierung eines anderen Ventils in der Prozessanlage 10 verwendet wurde. Wenn es zum Beispiel vier Steuerventile gibt, können die Tags „CTRL-VALVE-01“, „CTRL-VALVE-02“, „CTRL-VALVE-03“ und „CTRL-VALVE-04“ lauten. Der E/A-Serverdienst kann feststellen, dass einem physischen oder logischen Asset noch kein eindeutiges Tag zugewiesen wurde, indem er die Identifizierungsparameter für das physische oder logische Asset mit den Identifizierungsparametern für physische oder logische Assets vergleicht, denen bereits Tags zugewiesen wurden. Wenn die Identifizierungsparameter nicht übereinstimmen, kann der E/A-Serverdienst dem physischen oder logischen Asset eine neue eindeutige Kennzeichnung zuweisen, z. B. „CTRL-VALVE-05“.

[0326] Ein weiteres Beispiel: Zwei physische oder logische Assets können Ventile sein, die dieselbe Seriennummer haben, also eine Teilenummer. Die beiden Ventile können anhand einer Kombination aus der Seriennummer und den kryptografischen Schlüsseln für die beiden Ventile eindeutig identifiziert werden. Dementsprechend kann der E/A-Serverdienst die Tags für jedes Ventil auf der Grundlage der Kombination aus Seriennummer und kryptografischen Schlüsseln für jedes Ventil erzeugen.

[0327] Anschließend kann der E/A-Serverdienst das Tag in Verbindung mit den Standortinformationen für das physische oder logische Asset in einem Datenspeicher speichern, der als Referenz für die Kommunikation mit dem physischen oder logischen Asset verwendet werden kann.

[0328] Um das physische oder logische Asset zu testen, kann der E/A-Serverdienst Daten an das physische oder logische Asset übertragen oder Informationen von dem physischen oder logischen Asset unter Verwendung der Standortinformationen anfordern. Wenn der E/A-Serverdienst erfolgreich mit dem physischen oder logischen Asset kommunizieren kann, kann der E/A-Serverdienst feststellen, dass das physische oder logische Asset erfolgreich in Betrieb genommen worden ist. In einigen Implementierungen kann der E/A-Serverdienst einen bestimmten Parameter von dem physischen oder logischen Asset anfordern (z.B. eine Massendurchflussrate) und Signaletiketten für bestimmte Parameter oder Dienste, die mit dem physischen oder logischen Asset verbunden sind, erzeugen und speichern. Ein Signal-Tag kann eine Kombination aus dem Tag für das physische oder logische Asset und einer Kennung für den jeweiligen Parameter oder Dienst beinhalten. In anderen Implementierungen speichert der E/A-Serverdienst keine Signal-Tags.

[0329] Um die Identität des physischen oder logischen Assets zu verifizieren oder zu bestätigen, kann der E/A-Serverdienst beispielsweise einen kryptografischen öffentlichen Schlüssel oder PSK für das physische oder logische Asset aus den Identifizierungsparametern erhalten. Der E/A-Serverdienst kann die Informationsanforderung mit dem kryptografischen öffentlichen Schlüssel oder PSK verschlüsseln. Wenn der E/A-Serverdienst eine Antwort auf die Anforderung vom physischen oder logischen Asset erhält, stellt der E/A-Serverdienst fest, dass das physische oder logische Asset die Anforderung mit dem kryptografischen öffentlichen Schlüssel oder PSK entschlüsseln konnte. Infolgedessen verifiziert der E/A-Serverdienst die Identität des physischen oder logischen Assets.

[0330] Wie bereits erwähnt, steuert oder verwaltet der System-Orchestrator 222 die Zuweisung der verschiedenen logischen Entitäten, einschließlich Containern, zu verschiedenen des Datenzentrums-Clusters 208 und schließlich zu einzelnen Rechengeräten, wie Servern (und sogar zu Prozessoren oder Kernen von Prozessoren in einem Server eines Daten-Clusters 208), und kann diese Zuweisung während des Laufzeitbetriebs des Steuerungs-

systems vornehmen, um den Betrieb des Steuerungssystems sicherzustellen, wenn verschiedene physische Geräte (wie Server) ausfallen, außer Betrieb genommen werden, überlastet werden, langsam laufen usw. Diese dynamische Zuweisung zur Laufzeit unterscheidet sich deutlich von früheren Steuerungssystemarchitekturen, bei denen die physischen Assets oder Rechengeräte, die ein logisches Element wie ein Steuerungsmodul oder eine Steuerungsroutine implementierten, vom Konfigurationssystem festgelegt wurden und sich während der Laufzeit nicht veränderten. In dieser neuen Systemarchitektur weiß ein Nutzer also möglicherweise nicht, wo ein bestimmtes logisches Element, wie z.B. eine Steuerung oder ein mit einer Steuerung verbundener Container, zu einem bestimmten Zeitpunkt ausgeführt oder implementiert wird, geschweige denn, dass er den Zustand oder die Leistungsstatistiken eines solchen logischen Elements (wie z.B. die Kommunikationsbandbreite oder die Nachrichtenraten) kennt oder leicht ermitteln kann. Darüber hinaus wird es für einen Nutzer nicht einfach sein, Leistungs- oder Gesundheitsindikatoren für das physische Gerät zu erhalten, in dem ein bestimmtes logisches Element gerade ausgeführt wird, wie z.B. Latenz, Effizienz, Last usw., da ein Nutzer nicht in der Lage sein wird, allein durch das Konfigurationssystem zu wissen, welche logischen Elemente gerade auf einem bestimmten physischen Gerät oder physischen Knoten zu einem bestimmten Zeitpunkt in Betrieb sind.

[0331] In vielen Fällen ist es jedoch wichtig, dass ein Nutzer, z.B. ein Bediener des Steuerungssystems, Wartungspersonal usw., den aktuellen Betriebsstatus eines oder mehrerer logischer Elemente des Steuerungssystems einsehen kann, um den aktuellen Betriebsstatus des Prozesssteuerungssystems zu sehen und/oder zu diagnostizieren oder um ein Problem innerhalb des Prozesssteuerungssystems zu diagnostizieren. Darüber hinaus muss ein Nutzer möglicherweise wissen, welche logischen Elemente momentan auf einem bestimmten physischen Gerät oder physischen Knoten ausgeführt werden, um Wartungs-, Aktualisierungs- oder andere Instandhaltungs- oder Reparaturarbeiten an diesem Gerät oder Knoten durchführen zu können. Darüber hinaus kann es, wie bereits erwähnt, wichtig sein, die aktuelle Konfiguration der logischen Elemente innerhalb der Anlage einfach zu visualisieren, einschließlich der Art und Weise, in der die logischen Elemente, z.B. die Container, des Prozesssteuerungssystems ineinander verschachtelt oder miteinander verbunden sind und/oder der Art und Weise, in der diese logischen Elemente mit bestimmten Hardwarekomponenten verbunden sind.

[0332] Zur Unterstützung eines Nutzers bei der Anzeige des aktuellen Laufzeitbetriebs eines Steuerungssystems, das die hier beschriebene neue Systemarchitektur verwendet, kann ein Visualisierungsdienst, bei dem es sich um einen der Dienste 240 von **Fig. 2** handeln kann, bereitgestellt werden, um eine oder mehrere Systemkonfigurations- und/oder Laufzeit-Visualisierungen für einen Nutzer (über eine Nutzer-Schnittstelle) zu generieren, um den Nutzer dabei zu unterstützen, die aktuell konfigurierten und betrieblichen Beziehungen zwischen den verschiedenen logischen und physischen Elementen des Steuerungssystems zu verstehen sowie einen oder mehrere Leistungsindikatoren für die logischen und physischen Elemente anzuzeigen. Insbesondere ist in **Fig. 42** ein Visualisierungsdienst (oder Nutzer Schnittstelle) 3202 dargestellt, der auf einem Computer Prozessor ausgeführt wird und der dazu dient, den Orchestrator 222 sowie eines oder mehrere der Orchestrator Subsysteme 252, 255, 258, 260 abzufragen oder anderweitig mit ihnen zu kommunizieren und zu jedem beliebigen Zeitpunkt festzustellen, welche logischen Elemente auf welchen physischen Geräten gehostet oder ausgeführt werden, zusätzlich zu verschiedenen Zustands- und/oder Leistungsstatistiken oder Indizes, die mit diesen logischen Elementen und/oder physischen Geräten verbunden sind. In einigen Fällen kann der Visualisierungsdienst 3202 zusätzlich mit einer Konfigurationsdatenbasis 3203 kommunizieren, um Konfigurationsinformationen über logische und physische Elemente zu erhalten und eine Konfigurations-/Laufzeitvisualisierung des Steuerungssystems (einschließlich der logischen und physischen Elemente) zu erstellen, die es einem Nutzer ermöglicht, Informationen über die verschiedenen Konfigurations- und Laufzeitdetails des aktuell konfigurierten Zusammenspiels zwischen den logischen Elementen (untereinander) und zwischen den logischen Elementen und den physischen Elementen des Steuerungssystems anzuzeigen. In einigen Fällen kann diese Konfigurationsschnittstelle es einem Nutzer ermöglichen, Konfigurationsdetails (wie z.B. Anheften und Verschachtelung von logischen und/oder physischen Elementen) eilig oder während der Laufzeit zu ändern.

[0333] **Fig. 42** zeigt den Visualisierungsdienst oder das Dienstprogramm 3202 (der/das auf einem Computerprozessor ausgeführt wird), der/das mit dem Orchestrator 222 von **Fig. 1** und, falls erforderlich, mit der Konfigurationsdatenbasis 3203 kommuniziert, um Konfigurations- und Laufzeitinformationen für die verschiedenen logischen und physischen Elemente zu ermitteln. Der Visualisierungsdienst 3202 kann Informationen vom Orchestrator 222 für aktive Visualisierungen abonnieren und/oder eine oder mehrere Abfragen an den Orchestrator 222 (und die Konfigurationsdatenbasis 3203) senden, wenn er eine Visualisierung für einen Nutzer über eine Nutzer-Schnittstelle 3204 erstellt. In jedem Fall wird der Visualisierungsdienst 3202 ausgeführt, um einem Nutzer über die Nutzer Schnittstelle 3204 (bei der

es sich um eine beliebige Art von Nutzer Schnittstelle handeln kann, wie z.B. einen Laptop, ein drahtloses Gerät, eine Telefonanwendung, eine Workstation usw.) sowohl logische als auch physische Informationen über das Steuerungssystem anzuzeigen und kann die Informationen über das Steuerungssystem auf interaktive Weise anzeigen, so dass der Nutzer in der Lage ist, die Konfiguration sowie die aktuelle Laufzeit der verschiedenen logischen Elemente innerhalb der Anlage und der physischen Elemente, denen diese logischen Elemente momentan zugeordnet sind, einzusehen. Insbesondere kann der Visualisierungsdienst 3202 dem Nutzer über die Nutzer Schnittstelle 3204 einen oder mehrere Bildschirme präsentieren, auf denen ein oder mehrere logische und/oder physische Elemente des Steuerungssystems angezeigt werden, und es dem Nutzer ermöglichen, eines der verschiedenen logischen und/oder physischen Elemente des Steuerungssystems, wie sie momentan implementiert sind, auszuwählen, um weitere Details über die Konfiguration und/oder Laufzeitinformationen anzuzeigen, die der Nutzer sehen möchte. Der Visualisierungsdienst 3202 erhält dann vom Orchestrator 222 Laufzeitinformationen für die ausgewählten logischen und/oder physischen Elemente, z.B. die Art und Weise, wie die logischen Elemente (z.B. Container, wie Steuerungscontainer) ineinander verschachtelt oder aneinander angeheftet sind, die Art und Weise, wie die logischen Elemente in oder auf verschiedenen physischen Elementen ausgeführt werden, und/oder einen oder mehrere Leistungsindikatoren, die den Betriebszustand oder die Leistung der logischen und/oder physischen Elemente im aktuellen Betrieb anzeigen. Der Visualisierungsdienst 3202 präsentiert dem Nutzer diese Informationen in einer oder mehreren Bildschirmanzeigen und kann es dem Nutzer in einigen Fällen ermöglichen, über eine Bildschirmanzeige zu interagieren, um andere Informationen zu sehen und den Betrieb des Steuerungssystems dynamisch zu ändern, indem ein oder mehrere logische Elemente anderen logischen Elementen oder physischen Elementen zugewiesen werden.

[0334] In einem Beispiel kann das Dienstprogramm 3202 zusätzlich zu den Laufzeitinformationen vom Orchestrator 222 Konfigurationsinformationen, wie z.B. eine Konfigurationshierarchie, von der Konfigurationsdatenbasis 3203 erhalten und dem Nutzer eine Konfigurationshierarchie (einschließlich sowohl Konfigurationsinformationen als auch Laufzeitzuweisungsinformationen) präsentieren, um es ihm zu ermöglichen, verschiedene konfigurierte Elemente des Steuerungssystems so zu sehen, wie sie gerade in der Anlage oder im Steuerungssystem betrieben oder ausgeführt werden. **Fig. 43** zeigt ein Beispiel für eine Konfigurations-/Laufzeithierarchie 3210, die einem Nutzer zur Verfügung gestellt werden kann. In diesem Fall beinhaltet die Hierarchie 3210 sowohl physische als auch logische Elemente in einer vertrauten Struktur und ermöglicht es dem Nutzer, in der Hierarchie 3210 nach unten zu gehen, um mehr Informationen über die logischen und physischen Elemente der oberen oder höheren Ebene zu erhalten, um mehr Informationen über die aktuelle Konfiguration und den aktuellen Betrieb des Systems während der Laufzeit zu erhalten. Insbesondere im Beispiel von **Fig. 43** zeigt die Hierarchie 3210 sowohl logische Elemente (einschließlich Containern, die mit den verschiedenen Steuer-, Subsystem- und E/A-Diensten verbunden sind) als auch physische Elemente (z. B. Datencluster, Rechenknoten usw.). Im Allgemeinen unterteilt das Software-definierte Steuerungssystem, wenn es konfiguriert ist, die physischen Knoten in Mikrodienste (Container) und führt diese Container dann auf einem oder mehreren Clustern von Rechenknoten aus, von denen einige während der Laufzeit vom Orchestrator 222 ausgewählt werden. Die Hierarchie 3210 in **Fig. 43** veranschaulicht diese Konfiguration, da die Hierarchie 3210 ein physisches Netzelement 3220 und ein Steuerungsnetzelement 3230 beinhaltet. Das physische Netzelement 3220 kann, wenn es erweitert wird, die physischen Verbindungen der physischen Elemente oder Geräte, die mit dem Software-definierten Steuerungssystem verbunden sind, einschließlich der Feldgeräte (Ventile, Transmitter usw.), der physischen E/A-Geräte, der Netzwerkschalter, des Datenzentrums-Clusters und seiner Komponenten, der Nutzer-Schnittstellen, der Historiker usw., in hierarchischer Weise detailliert auflisten. In einem Beispiel kann der Datenzentrums-Cluster jeweils eine Sammlung von physischen Knoten (d.h. eine Sammlung von Servern) beinhalten, wobei sich jeder Server in einem bestimmten Blade eines Racks von Servern befinden kann (die alle Teil desselben Clusters sein können oder auch nicht). Darüber hinaus kann jeder Server einen oder mehrere Prozessoren haben und jeder Prozessor kann einen oder mehrere Kerne haben, und alle diese verschiedenen Elemente können unter oder als Teil des physischen Netzwerkelements 3220 angegeben oder dargestellt werden. Darüber hinaus kann, falls gewünscht, jeder Knoten oder jedes Rack von Knoten mit einer oder mehreren bestimmten Energieversorgungen verbunden sein, so dass eine Energieversorgung ein ganzes Rack oder nur bestimmte Knoten in dem Rack versorgen kann, so dass die Knoten in einem einzigen Rack eine Energieversorgungsredundanz aufweisen können. In jedem Fall könnten diese und andere physische Konfigurationsinformationen in der Hierarchie 3210 unter dem physischen Netzwerk Element 3220 dargestellt werden.

[0335] In der Beispieldarstellung 3210 von **Fig. 43** beinhaltet das Element 3230 des Steuerungsnetzwerks verschiedene physische und logische Komponenten, darunter eine Nutzer-Schnittstelle (ProPlus-Station), ein E/A-Netzwerk (mit Tags), ein drahtloses E/A-Netzwerk und einen oder mehrere

Rechencluster (mit dem in **Fig. 43** gezeigten Rechencluster 1, der mit dem Bezugszeichen 3 235 gekennzeichnet ist). Darüber hinaus kann jeder Rechen-Cluster mehrere Knoten 3236 haben, die mit ihm oder darunter verbunden sind, wobei einer dieser Knoten 3236 in **Fig. 43** dargestellt ist. Die Elemente der oberen Ebene des Steuerungsnetzwerks 3230 sind also im Allgemeinen physische Elemente. Wie bereits beschrieben und in der Hierarchie 3210 dargestellt, können jedoch jedem Knoten 3236 verschiedene logische Elemente (z.B. Container) zugeordnet oder mit ihm verbunden sein, darunter z.B. Steuerungscontainer 3240, die verschiedene konfigurierte Steuerungen angeben (die logische Elemente in der SDCS-Architektur sind), Steuerungssubsystem-Container wie zugewiesene Module 3242, zugewiesene E/A-Container 3244, Container von Drittanbietern 3246, Bereichscontainer 3247, Historikercontainer 3248, usw. Der Kasten 3250 in **Fig. 43** verweist auf einige, aber nicht alle der in der Hierarchie 3210 angegebenen Container. Es sei darauf hingewiesen, dass die Hierarchie 3210 in **Fig. 43** sowohl konfigurierte Hardwarekomponenten als auch konfigurierte logische Elemente, einschließlich Container, darstellt. Noch wichtiger ist, dass die Hierarchie 3210 von **Fig. 43** die Art und Weise veranschaulicht, in der die verschiedenen darin dargestellten Container in andere Container und/oder physische Elemente unter den verschiedenen hierarchischen Schichten verschachtelt oder angeheftet sind. Zum Beispiel ist das zugewiesene Modul von Boiler_1 (3260) an den Container 940 der Steuerung 2 angeheftet (wie an mehreren Stellen in der Hierarchie 3210 durch das Bezugszeichen 3260 dargestellt) und der Drittanbieter-Container MaterialZusammensetzung ist an Steuerung 2 angeheftet (wie durch das Bezugszeichen 3262 angezeigt). Es versteht sich von selbst, dass die Container, die in der Hierarchie 3210 unterhalb eines anderen Containers aufgeführt sind, bei der Darstellung der Hierarchie 3210 in dem übergeordneten Container verschachtelt sind. Diese Verschachtelung kann ein Ergebnis der Anheftung des Elements oder ein Ergebnis der Laufzeitplatzierung des Elements durch den Orchestrator 222 sein. So kann die Hierarchie 3210 verwendet werden, um den konfigurierten Betrieb des Systems (in Bezug auf die Art und Weise, wie die Container untereinander oder mit bestimmten Hardwareelementen angeheftet sind) und den Laufzeitbetrieb des Systems (in Bezug auf die Art und Weise, wie Container in anderen Containern verschachtelt sind und in bestimmter Hardware oder physischen Komponenten ausgeführt werden) anzuzeigen. Darüber hinaus kann die Hierarchie 3210 die aktuelle Betriebskonfiguration des Steuerungssystems in Bezug auf logische Elemente anzeigen, die während des Laufzeitbetriebs zuweisbar sind, z.B. durch Darstellung der Steuerung oder des Moduls, dem ein bestimmter zuweisbarer Container momentan zugewiesen ist, und/oder des physischen Elements, dem ein bestimmter Container momentan zugewiesen ist.

[0336] Darüber hinaus kann die Hierarchie 3210 anzeigen, dass verschiedene Container vom Nutzer dynamisch zugewiesen werden können, z.B. durch die Interaktion der Elemente innerhalb der Hierarchie 3210. Zum Beispiel zeigt die Hierarchie 3210 von **Fig. 43** an, dass verschiedene Rezepte 3270 dynamisch zuweisbare Container sind. In einigen Fällen kann die Anwendung Nutzer Schnittstelle es einem Nutzer ermöglichen, einen Container (z.B. ein Rezept oder einen anderen dynamisch zuweisbaren Container) neu zuzuweisen, indem er das Element in der Hierarchie 3210 auswählt und das Element unter oder innerhalb einer neuen logischen oder physischen Einheit innerhalb der Hierarchie 3210 zieht und fallen lässt. Natürlich können auch andere Methoden zur dynamischen Neuzuweisung eines logischen Elements zu einem anderen logischen Element oder zu einem physischen Element verwendet werden (z.B. Dropdown-Menüs, neue Fenster usw.).

[0337] Wie in der Hierarchie 3210 von **Fig. 43** dargestellt, können Steuerelemente wie Bereiche, Einheiten, Ausrüstungsmodule und Module mit einem physischen Steuercluster verbunden werden. Einmal zugewiesen, bleibt ein Steuerungselement, zum Beispiel Einheit C-101, als Steuerstrategie zusammen. Da in diesem Beispiel die Einheit C-101 nicht angeheftet wurde, kann sie einem beliebigen Steuerungsknoten (Rechenknoten) zugewiesen werden. Die Einheit BOILER_1 hingegen wurde der Steuerung 2 zugeordnet. Wenn der Hardwareknoten, dem Steuerung 2 zugeordnet ist, ausfällt, wird alles, was an Steuerung 2 angeheftet ist, auf einen anderen Server oder Knoten mit freien Ressourcen migriert (basierend auf den Aktionen des Orchestrator 222). Dynamisch zuweisbare Steuerelemente hingegen können dynamisch einer beliebigen Steuerung mit freien Ressourcen zugewiesen werden.

[0338] Der gleiche Ansatz, der oben für Steuerobjekte beschrieben wurde, wird auch für Historie, Alarme & Ereignisse, Batch, kontinuierliche-Historiker und andere Subsystem-Container verwendet. Subsysteme werden in separaten Containern ausgeführt und können an Steuerung-/Rechenknoten angeheftet oder dynamisch zugewiesen werden. In Anlehnung an die obige Beschreibung werden also alle Subsysteme als Container behandelt. Als weitere Zuweisung können Steuerungselemente aus der Hierarchie der Steuerungsstrategien dem Rechencluster zugewiesen und dann an Rechenknoten angeheftet oder dynamisch zugewiesen werden (z.B. durch eine Drag & Drop-Technik in der Hierarchie 3210). Ähnlich können E/A-Container einem Rechencluster zugewiesen und dynamisch zugewiesen werden, da die Steuerelemente dynamisch

zugewiesen werden. Darüber hinaus können Micro-Container auf E/A-Geräten laufen.

[0339] In jedem Fall kann der Visualisierungsdienst 3202 die Hierarchie 3210 so erstellen, dass die Hierarchie 3210 (1) die dauerhaft konfigurierten (nicht veränderbaren oder angehefteten) Beziehungen zwischen physischen und logischen Elementen und zwischen logischen Elementen und anderen logischen Elementen anzeigt, (2) die temporär konfigurierten (vom Benutzer zuweisbaren oder während der Laufzeit dynamisch zuweisbaren) Beziehungen zwischen physischen und logischen Elementen und zwischen logischen Elementen und anderen logischen Elementen und (3) die während der Laufzeit oder aktuell vom Orchestrator 222 zugewiesenen Beziehungen zwischen physischen und logischen Elementen und zwischen logischen Elementen und anderen logischen Elementen. So kann die Hierarchie 3210 erstellt werden, um die Beziehungen zwischen den Containern und verschiedenen Hardwareelementen wie Knoten, Servern, Prozessoren, Kernen, Racks, Energieversorgungen usw. anzuzeigen, auf denen diese Container gerade ausgeführt werden, und wenn diese Beziehungen angeheftet sind. Darüber hinaus kann die Hierarchie 3210 verwendet werden, um dynamisch zuweisbare Container anzuzeigen und kann sogar vom Nutzer verwendet oder manipuliert werden, um eine Neuzuweisung von dynamisch zuweisbaren Containern während der Laufzeit durchzuführen. In diesem Fall wird der Visualisierungsdienst 3202 bei Erhalt einer Anweisung zur Neuzuweisung eines Containers an ein anderes logisches und/oder physisches Element den Orchestrator 222 über die Neuzuweisung informieren und der Orchestrator 222 wird die Neuzuweisung des Containers (und aller Container, die in dem neu zugewiesenen Container verschachtelt oder daran angeheftet sind) durchführen. Darüber hinaus kann die Hierarchie 3210 erstellt werden, um die Laufzeitkonfiguration (wie vom Orchestrator 222 durchgeführt) verschiedener logischer und physischer Elemente in Bezug zueinander anzuzeigen.

[0340] Natürlich kann der Visualisierungsdienst 3202 die Beziehungen zwischen logischen Elementen (z.B. Containern) und anderen logischen Elementen und/oder physischen Elementen auf andere Weise darstellen und kann auch wichtige Leistungs- und Diagnoseindikatoren beinhalten, die es dem Nutzer ermöglichen, den aktuellen Betriebszustand oder die Leistung des Steuerungssystems oder einer seiner verschiedenen Komponenten zu verstehen. Beispielsweise kann der Visualisierungsdienst 3202 von **Fig. 42** für einen Nutzer die aktuelle Konfiguration eines jeden physischen Elements (z.B. Knoten oder Server des Systems, wie alle Knoten eines bestimmten Rechenclusters) veranschaulichen, indem er die physischen Elemente in Verbindung mit den logischen Elementen (Containern) darstellt, die ihnen momentan zugeordnet sind oder auf ihnen laufen. In diesem Fall kann der Visualisierungsdienst 3202 auch Zustands-, Diagnose- und/oder Leistungsstatistiken oder -maße für physische Elemente abrufen und anzeigen, die beispielsweise von einem oder mehreren der Dienstprogramme 252, 255, 258, 260 von **Fig. 2** berechnet oder bestimmt werden. **Fig. 44** zeigt eine beispielhafte Nutzer-Schnittstelle oder Anzeige 3300, die vom Visualisierungsdienst 3202 erstellt werden kann, um einen Daten-Cluster 3310 mit drei Servern oder Knoten 3320 darin zu veranschaulichen. Die Anzeige 3300 zeigt auch eine Reihe von Containern oder Containertypen für jeden der Knoten 3320 und beinhaltet in diesem Fall einen Container Orchestratordienst 3330, eine Reihe von Steuerungscontainern 3332, einen Batch Executive Container 3334 und einen kontinuierlichen Historikercontainer 3336 in jedem der Knoten 3320. Obwohl in **Fig. 44** nicht dargestellt, kann der Visualisierungsdienst 3202 es einem Nutzer ermöglichen, in jeden der Knoten 3332 bis 3336 einzudringen, um die verschiedenen Container (z.B. Steuerungscontainer und alle Container, die in diesen Steuerungscontainern verschachtelt oder an diese angeheftet sind) und die Subsystemcontainer 3334 und 3336 zu sehen, um die logischen Elemente zu sehen, die momentan auf jedem der jeweiligen Server 3320 ausgeführt werden. Darüber hinaus kann der Visualisierungsdienst 3202 auf dem Display 3300 eine Reihe von Leistungsindikatoren 3340 für jeden der Server anzeigen, z.B. die aktuelle CPU-Auslastung, die Speichernutzung, die Netzwerkbandbreite und die Kerntemperatur. Natürlich sind dies nur einige wenige Beispiele für Diagnose- oder Leistungsindikatoren, die für jeden der Server oder Knoten 3320 ermittelt und angezeigt werden können, und es können auch andere Leistungs- und Diagnoseinformationen für die einzelnen Hardwareelemente (Server oder Knoten 3320) bereitgestellt werden. Darüber hinaus kann der Visualisierungsdienst 3202 andere Leistungsindikatoren anzeigen oder bereitstellen, wie z.B. einen Netzwerkstatus 3342 für das Kommunikationsnetzwerk im Cluster 3310 von **Fig. 44**, und er kann Leistungsindikatoren für logische Elemente anzeigen, wie z.B. einen Dienstcontainerstatus 3344 für eine Batch-Exekutive in einem der Server 3320.

[0341] Auch hier kann der Visualisierungsdienst 3202 es einem Nutzer ermöglichen, in jedes der Elemente 3330, 3332, 3334 und 3336 (oder andere Container wie Container von Drittanbietern usw., die als mit einem der Hardwareelemente 3320 verbunden angezeigt werden) einzudringen, um die logischen Elemente innerhalb dieser Container, die auf dem jeweiligen Server- oder Hardwareknoten ausgeführt werden, und einen oder mehrere Leistungs- oder Diagnoseindikatoren für jedes der Unterelemente anzuzeigen. Der Visualisierungsdienst 3202 kann auch Untereinheiten der physischen Elemente

anzeigen, die jede der Untereinheiten der logischen Elemente ausführen, wie z.B. bestimmte Server Prozessoren oder Kerne oder Blades oder Energieversorgungen, die mit den logischen Untereinheiten verbunden sind oder diese implementieren. Dieses Tool kann dem Nutzer somit großteilige Aktualisierungen des Gesamtsystems unter verschiedenen Gesichtspunkten liefern, z. B. aus einer logischen Sicht der Steuerungen und E/A und der zugehörigen Dienst-Container sowie aus einer physischen Sicht der Server und der physischen Ressourcenverwaltung, und es kann auch Diagnoseinformationen über die Leistung des Software-definierten Steuerungssystems oder eines Teils davon zu einem bestimmten Zeitpunkt liefern.

[0342] In einem anderen Fall kann der Visualisierungsdienst 3202 ein Diagramm der logischen Elemente oder Container des Systems oder eines Teilbereichs des Systems bereitstellen und die verschiedenen physischen Elemente anzeigen, auf denen diese logischen Elemente gerade laufen oder ausgeführt werden. **Fig. 45** zeigt eine Beispieldarstellung 3400, die verwendet werden kann, um ein logisches Element (in diesem Fall den Container Steuerung 1) und die Art und Weise, wie verschiedene logische Unterelemente des Containers Steuerung 1 zum aktuellen Zeitpunkt während der Ausführung des Steuerungssystems in der Hardware verteilt sind, zu veranschaulichen. So wird in der Beispieldarstellung 3400 von **Fig. 45** gezeigt, dass die logische Steuerung #1 drei redundante Steuerungscontainer (Steuerungscontainer #1) beinhaltet, wobei zu Redundanzzwecken eine erste der Steuerungscontainer #1 Instanzen auf einem physiischen Server 3430 ausgeführt wird und die zweite und dritte der Steuerungscontainer #1 Instanzen auf einem anderen physiischen Server 3432 ausgeführt werden. Darüber hinaus zeigt die Beispieldarstellung 3400 in **Fig. 45**, dass die logische Steuerung #1 (einschließlich der drei darin verschachtelten oder daran angehefteten Untercontainer) über eine Reihe von redundanten E/A-Servern oder E/A-Containern 3440 kommuniziert, die an einen Remote-E/A-Container 3442 gebunden sind. Die Beispieldarstellung 3400 zeigt auch an, welche der redundanten Steuerung #1 Instanzen gerade als aktive Steuerung oder Steuerungsinstanz arbeitet. Falls gewünscht, könnte die Beispieldarstellung 3400 von **Fig. 45** die einzelnen Hardwareelemente veranschaulichen, die momentan die redundanten E/A-Container 3440 implementieren, und/oder das Hardwaregerät, das momentan den Remote E/A-Container 3442 ausführt. Darüber hinaus kann der Visualisierungsdienst 3202 in der Beispieldarstellung 3400 eine beliebige Menge von Leistungsindikatoren für jedes der darin dargestellten logischen oder physischen Elemente bereitstellen. Natürlich ist **Fig. 45** nur ein einfaches Beispiel, und die Beispieldarstellung 3400 von **Fig. 45** könnte erweitert werden, um eine beliebige Menge logischer Elemente und die entsprechenden physischen Knoten oder Hardware zu zeigen, auf denen diese Elemente gerade laufen. Darüber hinaus können in dem Diagramm 3400 von **Fig. 45** für jedes der darin dargestellten logischen Elemente (und, falls gewünscht, der physischen Elemente) wichtige Leistungs- und Diagnoseindikatoren in beliebiger Weise angezeigt werden.

[0343] Fig. 46 zeigt eine weitere Visualisierungs- oder Bildschirmanzeige 3500, die vom Visualisierungsdienst 3202 bereitgestellt oder erstellt werden kann, um die aktuelle Betriebskonfiguration und Interaktion verschiedener logischer und physischer Assets innerhalb der Anlage oder des Steuerungssystems sowie verschiedene Leistungs- und/oder Diagnoseindikatoren für jedes angezeigte Element anzuzeigen. Die Bildschirmanzeige 3500 zeigt auf der rechten Seite eine Reihe von logischen Elementen, darunter, in diesem Beispiel, einen Software-definierten Steuerungssystemcontainer 3502, einen Batch Executive Container 3504 und einen kontinuierlichen Historikercontainer 3506. Das Diagramm oder die Bildschirmanzeige 3500 veranschaulicht, dass diese logischen Elemente über einen Bus 3510 mit einem E/A-Server 3512 verbunden sind, der seinerseits mit einer Reihe von Feldgeräten 3514 gekoppelt ist. Darüber hinaus zeigt die Bildschirmanzeige 3500 für jedes der logischen Elemente oder Container 3502, 3504 und 3506 verschiedene Leistungsindikatoren 3520 (die die Leistung der Elemente des Steuerungssystems im aktuellen Zustand anzeigen), darunter in diesem Beispiel ein Indikator für Nachrichten pro Sekunde, ein Indikator für die Speichernutzung, ein Indikator für die Netzwerkbandbreite und ein Indikator für die Fehlerrate. Darüber hinaus kann die Bildschirmanzeige 3500 in der Liste der Leistungsindikatoren 3520 auch physische Elemente beinhalten, die zur Implementierung der logischen Elemente verwendet werden, wie z.B. einen zugewiesenen physischen Knoten für jedes der zugehörigen logischen Elemente. Dieser Indikator für die physische Zuordnung könnte jedoch auch auf andere physische Hardware hinweisen, wie z.B. einen Server, einen Prozessor, einen Kern, ein Blade, eine Energieversorgung, usw. Die Bildschirmanzeige 3500 zeigt dieselben Leistungs- und Diagnoseindikatoren auch für den E/A-Server-Container 3512, könnte aber natürlich auch andere Leistungs- und Diagnoseindikatoren für dieses oder eines der darin dargestellten logischen Elemente liefern. Darüber hinaus zeigt das Diagramm 3500 die Leistungs- und Diagnoseindikatoren 3522 für den Bus 3510 in Form von Busbandbreite, Nachrichtendiagnose und Fehlerzuständen an und weist zusätzlich auf die physischen Netzwerkadapter hin, die den Bus 3510 bilden oder als solchen implementiert sind, über den die Container 3502, 3504 und 3506 mit dem E/A-Server-Container 3512 (der der eigentliche E/A-Server sein kann) kommunizieren. Natürlich können

auch andere Leistungs- und Diagnoseindikatoren ermittelt und angezeigt werden. So veranschaulicht die Bildschirmanzeige 3500 von **Fig. 46** wiederum die Art und Weise, in der verschiedene logische Elemente (Container) miteinander verbunden und in physischer Hardware implementiert sind, die diese logischen Elemente implementiert, und liefert Diagnose- oder Leistungsindikatoren für eines oder beide der logischen und physischen Elemente, aus denen dieser Teil des Steuerungssystems besteht, um einen Nutzer bei der Visualisierung des Betriebs des Software-definierten Steuerungssystems zu unterstützen.

[0344] In jedem dieser Beispiele kann die Nutzer Schnittstelle oder der Visualisierungsdienst 3202 die physischen und logischen Konfigurationen (und, falls gewünscht, die zugehörigen Leistungsdaten, die über verschiedene Diagnosedienste erhalten werden) zeigen oder veranschaulichen, während diese physischen und logischen Elemente vom Container-Orchestrator und der Software-definierten Networking Steuerung, die den gesamten Netzwerkverkehr durch das System verwaltet, implementiert werden. Darüber hinaus können einige oder alle der in diesen Diagrammen dargestellten Visualisierungen Farbdarstellungen verwenden, um bestimmte Zustandsstufen zu kennzeichnen, und Empfehlungssysteme bereitstellen, die dem Nutzer Maßnahmen empfehlen, um wahrgenommene oder erkannte Probleme innerhalb des visualisierten Software-definierten Steuerungssystems zu beheben. Es versteht sich von selbst, dass die **Abb. 43-46** nur einige Beispiele für Bildschirme darstellen, die verwendet werden könnten, um die Art und Weise anzuzeigen, in der verschiedene logische und physische Elemente zu einem bestimmten Zeitpunkt während der Laufzeit des Steuerungssystems interagieren und funktionieren, und dass stattdessen auch andere Visualisierungen verwendet werden könnten.

ANDERE ÜBERLEGUNGEN

[0345] Die hier beschriebenen Anwendungen, Module usw. können, wenn sie in Software implementiert sind, in jedem greifbaren, nicht transitorischen, computerlesbaren Speicher gespeichert werden, z.B. auf einer Magnetplatte, einer Laserplatte, einem Festkörperspeicher, einem Molekularspeicher oder einem anderen Speichermedium, in einem RAM oder ROM eines Computers oder Prozessors usw. Obwohl die hier beschriebenen Beispielsysteme neben anderen Komponenten auch Software und/oder Firmware beinhalten, die auf Hardware ausgeführt wird, sollte beachtet werden, dass diese Systeme lediglich illustrativ sind und nicht als einschränkend angesehen werden sollten. Es ist zum Beispiel denkbar, dass eine oder alle dieser Hardware-, Software- und Firmware-Komponenten ausschließlich in Hardware, ausschließlich in Software oder in einer beliebigen Kombination aus Hardware und Software verkörpert sind. Dementsprechend werden die hier beschriebenen Beispielsysteme zwar als in Software implementiert beschrieben, die auf einem Prozessor eines oder mehrerer Computergeräte ausgeführt wird, aber Fachleute, die sich mit der Materie auskennen, werden leicht erkennen, dass die angeführten Beispiele nicht die einzige Möglichkeit zur Implementierung solcher Systeme sind.

[0346] Während die vorliegende Erfindung unter Bezugnahme auf spezifische Beispiele beschrieben wurde, die lediglich der Veranschaulichung dienen und die Erfindung nicht einschränken sollen, wird es für den Fachmann offensichtlich sein, dass Änderungen, Ergänzungen oder Streichungen an den beschriebenen Ausführungsformen vorgenommen werden können, ohne vom Geist und Umfang der Erfindung abzuweichen.

[0347] Die besonderen Merkmale, Strukturen und/oder Eigenschaften einer bestimmten Ausführungsform können in jeder geeigneten Weise und/oder in jeder geeigneten Kombination mit einer und/oder mehreren anderen Ausführungsformen kombiniert werden, einschließlich der Verwendung von ausgewählten Merkmalen mit oder ohne entsprechende Verwendung anderer Merkmale. Darüber hinaus können viele Modifikationen vorgenommen werden, um eine bestimmte Anwendung, Situation und/oder ein bestimmtes Material an den wesentlichen Umfang oder Geist der vorliegenden Erfindung anzupassen. Es versteht sich, dass andere Variationen und/oder Modifikationen der hierin beschriebenen und/oder dargestellten Ausführungsformen der vorliegenden Erfindung im Lichte der hierin beinhalteten Lehren möglich sind und als Teil des Geistes oder des Umfangs der vorliegenden Erfindung betrachtet werden sollten. Bestimmte Aspekte der Erfindung werden hier als beispielhafte Aspekte beschrieben.

Patentansprüche

1. Industrielles Prozesssteuerungssystem, das Folgendes beinhaltet:
eine Vielzahl von Prozesssteuerungs-Feldgeräten, die zur Steuerung eines physischen Prozesses in einer industriellen Prozessanlage arbeiten;
eine Kommunikationsinfrastruktur, die die Vielzahl von Prozesssteuerungs-Feldgeräten kommunikativ mit einem Software-definierten Steuerungssystem verbindet, das Daten von der Vielzahl der Prozesssteuerungs-Feldgeräte empfängt und Anweisungen an die Vielzahl von Prozesssteuerungs-Feldgeräten sendet;
einen Datencluster, der eine Vielzahl von Rechenknoten beinhaltet, wobei der Datencluster das Software-definierte Steuerungssystem ausführt und jeder Rechenknoten Folgendes beinhaltet:

einen Prozessor, der ein Betriebssystem ausführt;
einen Speicher; und
eine Kommunikationsressource, die mit einem oder mehreren anderen Rechenknoten im Datencluster verbunden ist;
eine Vielzahl von instanziierten Containern, wobei jeder der Vielzahl von instanziierten Containern eine isolierte Ausführungsumgebung ist, die innerhalb des Betriebssystems eines der Vielzahl von Rechenknoten, auf dem der Container instanziiert ist, ausgeführt wird, wobei die Vielzahl von instanziierten Containern zusammenarbeitet, um die Ausführung einer Steuerstrategie in dem Software-definierten Steuerungssystem zu erleichtern;
wobei ein erster Container der Vielzahl von Containern an eine Komponente des Software-definierten Steuerungssystems angeheftet ist.

2. Industrielles Prozesssteuerungssystem nach Anspruch 1, wobei einer oder mehrere der Vielzahl instanziierter Container einer Ebene einer hierarchischen Struktur der industriellen Prozessanlage entsprechen oder einen Dienst beinhalten, der innerhalb des Containers ausgeführt wird.

3. Industrielles Prozesssteuerungssystem nach Anspruch 2, wobei der innerhalb des Containers ausgeführte Dienst einen der folgenden Dienste beinhaltet: einen E/A-Serverdienst, einen Steuerungsdienst, einen Historikerdienst, einen verteilten Alarmsubsystemdienst, einen Diagnosesubsystemdienst, einen Drittanbieterdienst, einen Sicherheitsdienst.

4. Industrielles Prozesssteuerungssystem nach einem der vorhergehenden Ansprüche, wobei die Komponente des Software-definierten Steuerungssystems ein weiterer aus der Vielzahl der Container ist.

5. Industrielles Prozesssteuerungssystem nach einem der vorhergehenden Ansprüche, wobei mindestens einer der Vielzahl von Containern innerhalb des ersten Containers instanziiert ist.

6. Industrielles Prozesssteuerungssystem nach einem der vorhergehenden Ansprüche, wobei der erste Container in mindestens einem der Vielzahl von Containern instanziiert ist.

7. Industrielles Prozesssteuerungssystem nach einem der vorhergehenden Ansprüche, wobei die Komponente eine der folgenden ist: ein Container, der innerhalb des ersten Containers instanziiert ist, ein Container, innerhalb dessen der erste Container instanziiert ist, der Daten-Cluster, ein Rechenknoten des Daten-Clusters, ein Prozessor eines Rechenknotens des Daten-Clusters, ein Prozessor-Kern eines Prozessors eines Rechenknotens des Daten-Clusters, Prozessor-Kern eines Prozessors eines Rechenknotens des Daten-Clusters.

8. Industrielles Prozesssteuerungssystem nach einem der vorhergehenden Ansprüche, wobei die Komponente eine der folgenden ist: ein Container, in dem ein Eingang/Ausgang (E/A)-Serverdienst ausgeführt wird, eines der mehreren Prozesssteuerungs-Feldgeräte, eine physische E/A-Schnittstelle, ein Rechenknoten oder ein Server innerhalb des Rechenknotens im Datencluster, eine Energieversorgung, die Energie für mindestens einen Bereich des Datenclusters bereitstellt, eine Energieversorgung, die Energie für mindestens einen Bereich des Datenclusters bereitstellt.

9. Industrielles Prozesssteuerungssystem nach einem der vorhergehenden Ansprüche, wobei die Steuerstrategie das Senden von Nachrichten an die mehreren Prozesssteuerungsfeldgeräte und das Empfangen von Nachrichten von den mehreren Prozesssteuerungsfeldgeräten beinhaltet.

10. Industrielles Prozesssteuerungssystem nach einem der vorhergehenden Ansprüche, wobei die Steuerstrategie das Empfangen von Prozessdaten von der Vielzahl der Prozesssteuerungsfeldgeräte, das Eingeben der empfangenen Daten in einen oder mehrere Regelkreise, um Steuerungsausgänge zu erzeugen, und das Übertragen der Steuerungsausgänge an die Vielzahl der Prozesssteuerungsfeldgeräte beinhaltet, um die Prozesssteuerungsfeldgeräte zu veranlassen, den physischen Prozess in der industriellen Prozessanlage zu steuern.

11. Industrielles Prozesssteuerungssystem nach einem der vorhergehenden Ansprüche, wobei ein zweiter Container, der einen Dienst ausführt, der mit einem im ersten Container ausgeführten Dienst identisch ist, an eine andere Komponente des Software-definierten Steuerungssystems angeheftet ist als die Komponente, an die der erste Container angeheftet ist.

12. Industrielles Prozesssteuerungssystem nach Anspruch 11, wobei die erste und die zweite Komponente eine der folgenden sind: unterschiedliche Prozessoren im Datencluster, unterschiedliche Rechenknoten im Datencluster, unterschiedliche Energieversorgungen, die Rechenknoten im Datencluster mit Energie versorgen.

Es folgen 46 Seiten Zeichnungen

Anhängende Zeichnungen

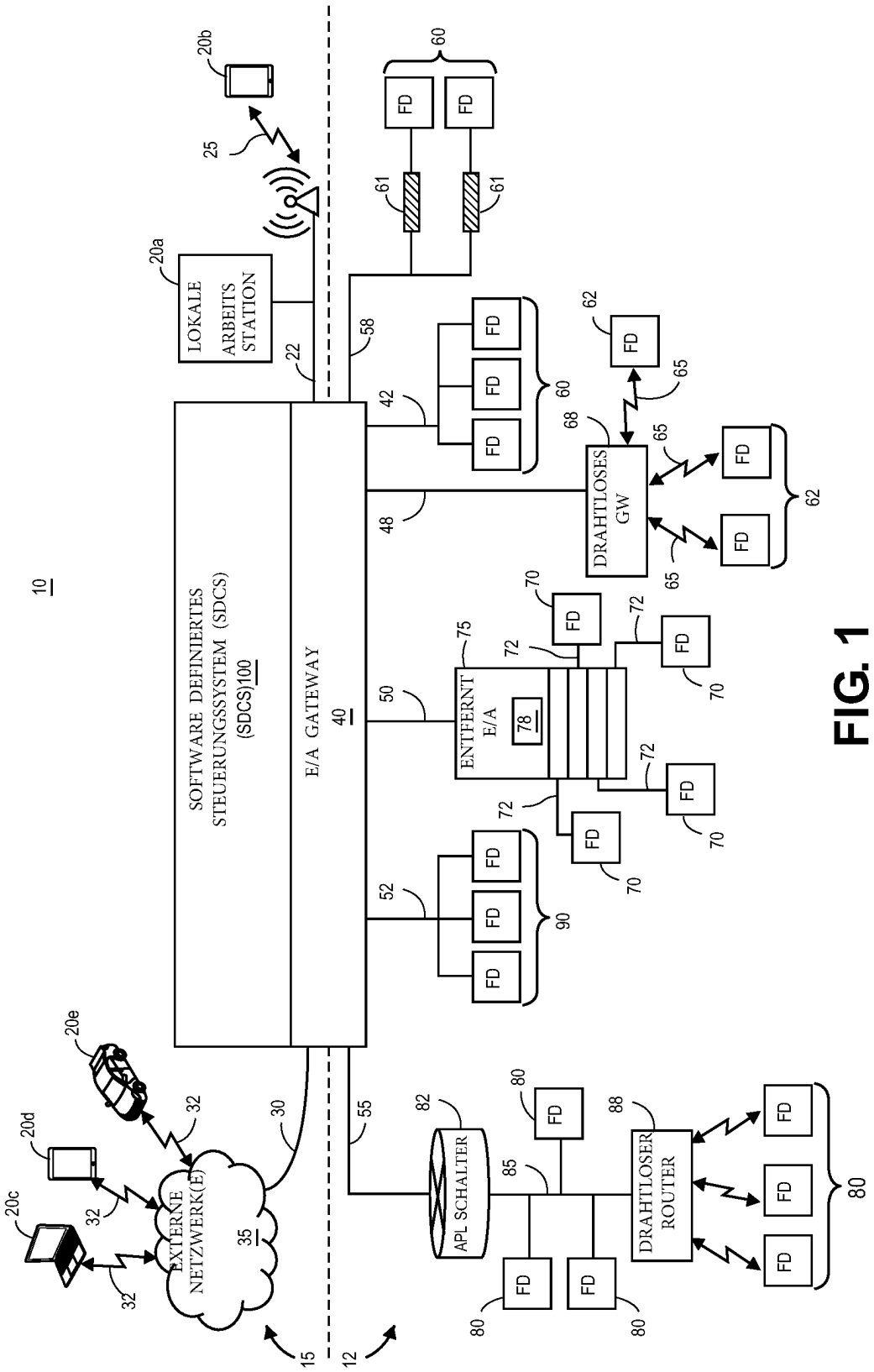


FIG. 1

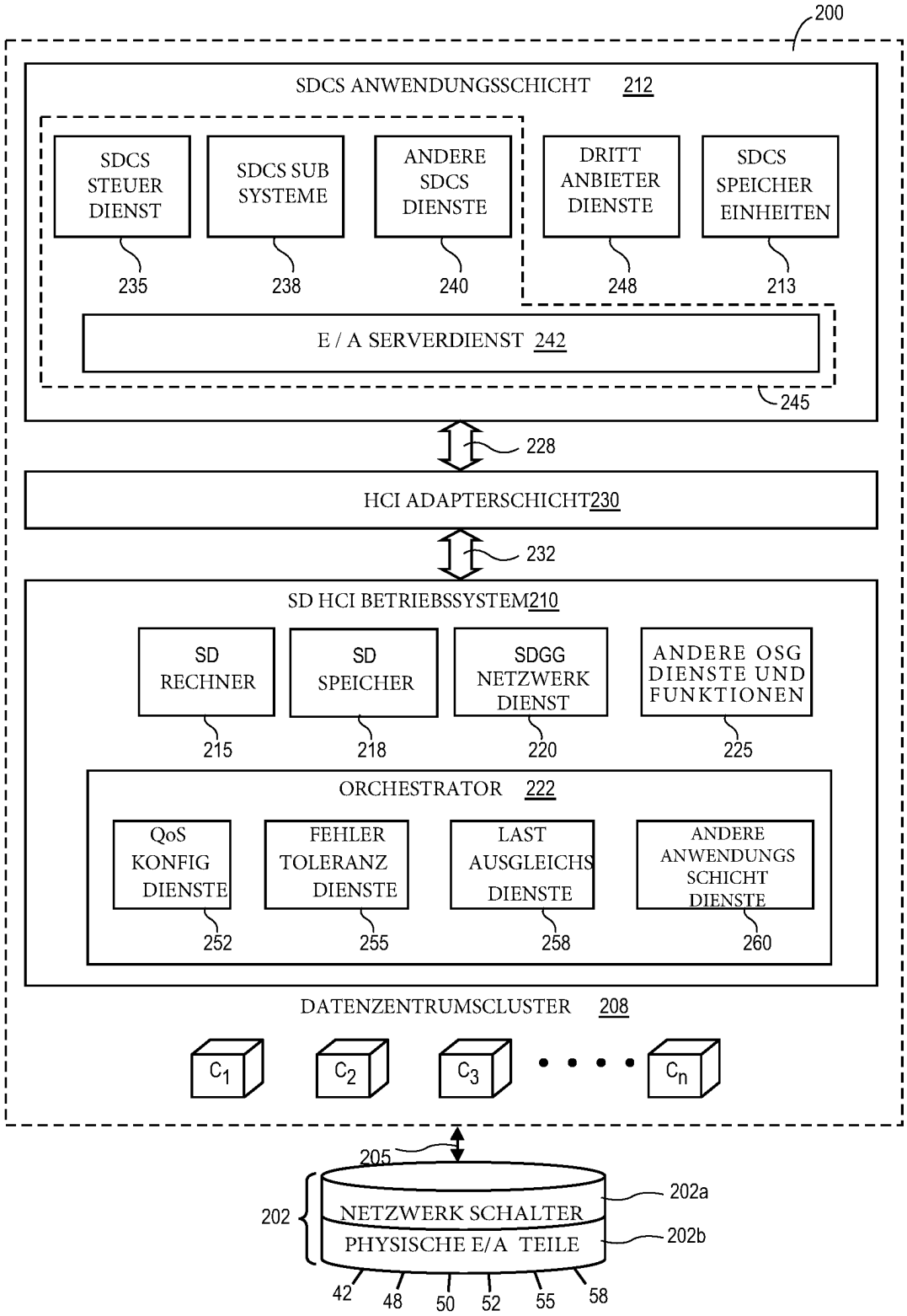

200
SDCS ANWENDUNGSSCHICHT 212
SDCS STEUER DIENST
SDCS SUB SYSTEME
ANDERE SDCS DIENSTE
DRITT ANBIETER DIENSTE
SDCS SPEICHER EINHEITEN
235
238
240
248
213
E / A SERVERDIENST 242
245
228
HCI ADAPTERSCHICHT230
232
SD HCI BETRIEBSSYSTEM210
SD RECHNER
SD SPEICHER
SDGG NETZWERK DIENST
ANDERE OSG DIENSTE UND FUNKTIONEN
215
218
220
225
ORCHESTRATOR 222
QoS KONFIG DIENSTE
FEHLER TOLERANZ DIENSTE
LAST AUSGLEICHS DIENSTE
ANDERE ANWENDUNGS SCHICHT DIENSTE
252
255
258
260
DATENZENTRUMSCLUSTER 208
C1
C2
C3
Cn
205
202
NETZWERK SCHALTER
PHYSISCHE E/A TEILE
202a
202b
42
48
50
52
55
58

FIG. 2

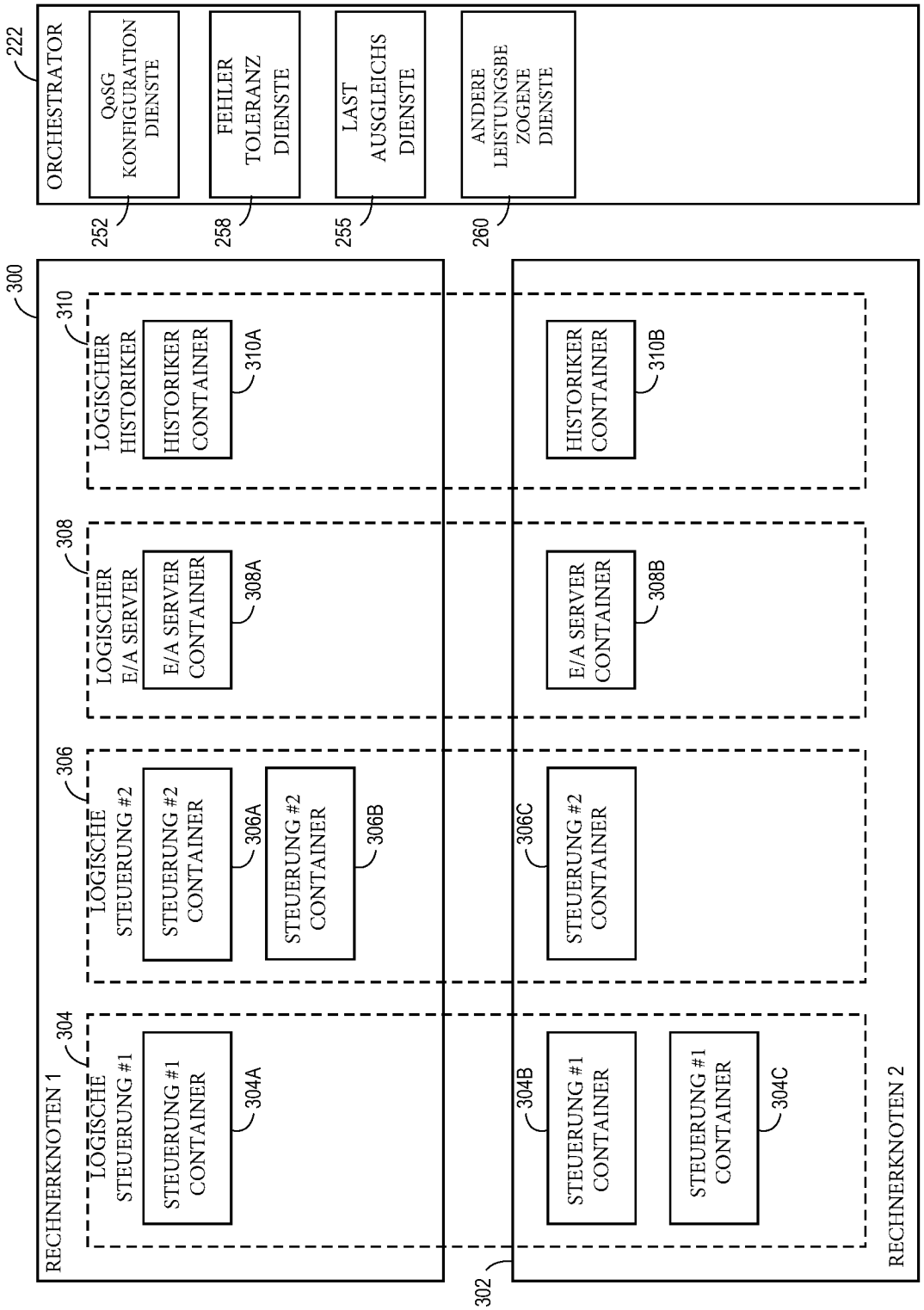

222
ORCHESTRATOR
QoSG KONFIGURATION DIENSTE
FEHLER TOLERANZ DIENSTE
LAST AUSGLEICHS DIENSTE
ANDERE LEISTUNGSBE ZOGENE DIENSTE
252
258
255
260
300
310
LOGISCHER HISTORIKER
HISTORIKER CONTAINER
310A
HISTORIKER CONTAINER
310B
308
LOGISCHER E/A SERVER
E/A SERVER CONTAINER
308A
E/A SERVER CONTAINER
308B
306
LOGISCHE STEUERUNG #2
STEUERUNG #2 CONTAINER
306A
STEUERUNG #2 CONTAINER
306B
306C
STEUERUNG #2 CONTAINER
304
LOGISCHE STEUERUNG #1
STEUERUNG #1 CONTAINER
304A
304B
STEUERUNG #1 CONTAINER
STEUERUNG #1 CONTAINER
304C
RECHNERKNOTEN 1
RECHNERKNOTEN 2
302

FIG. 3

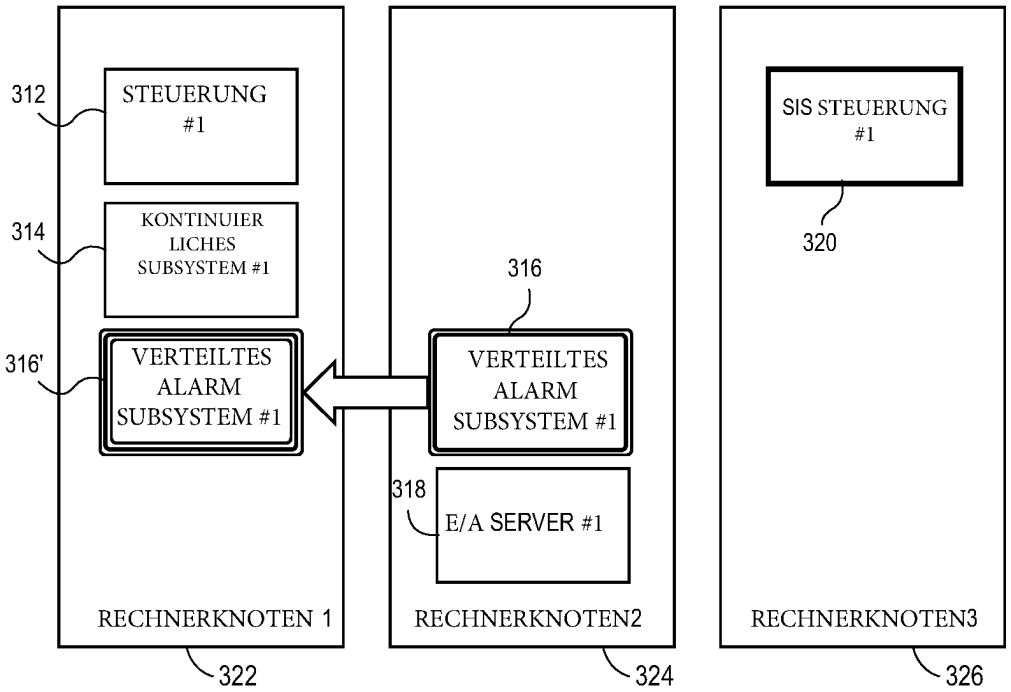

312
STEUERUNG #1
314
KONTINUIERLICHES SUBSYSTEM #1
316'
VERTEILTES ALARM SUBSYSTEM #1
316
VERTEILTES ALARM SUBSYSTEM #1
318
E/A SERVER #1
SIS STEUERUNG #1
320
RECHNERKNOTEN 1
322
RECHNERKNOTEN2
324
RECHNERKNOTEN3
326

FIG. 4A

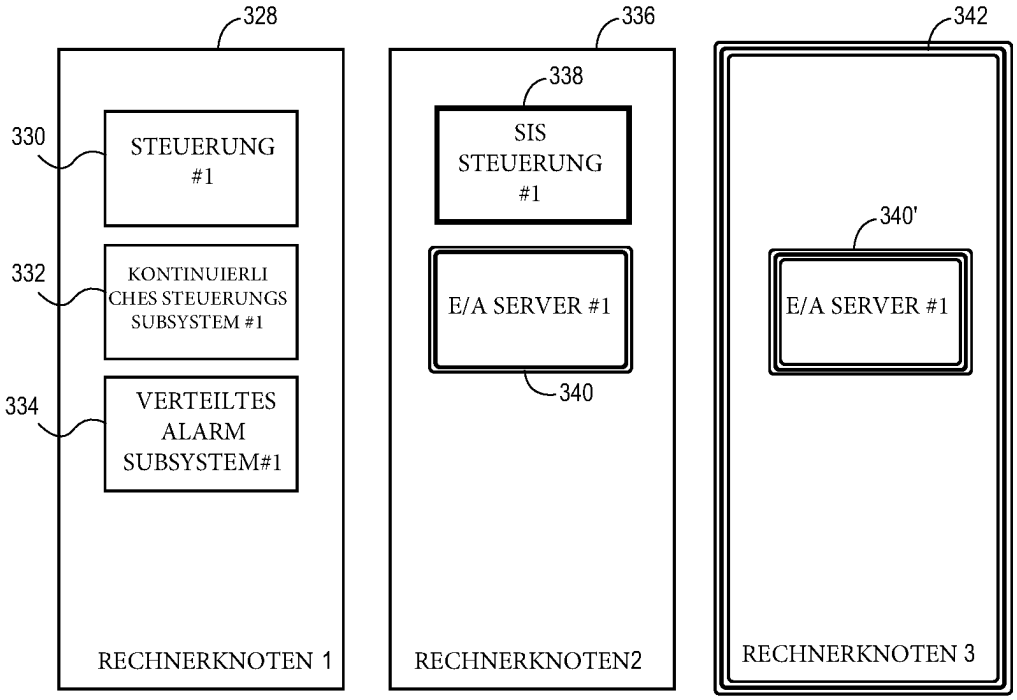

328
330
STEUERUNG #1
332
KONTINUIERLICHES STEUERUNGS SUBSYSTEM #1
334
VERTEILTES ALARM SUBSYSTEM#1
RECHNERKNOTEN 1
336
338
SIS STEUERUNG #1
E/A SERVER #1
340
RECHNERKNOTEN2
342
340'
E/A SERVER #1
RECHNERKNOTEN 3

FIG. 4B

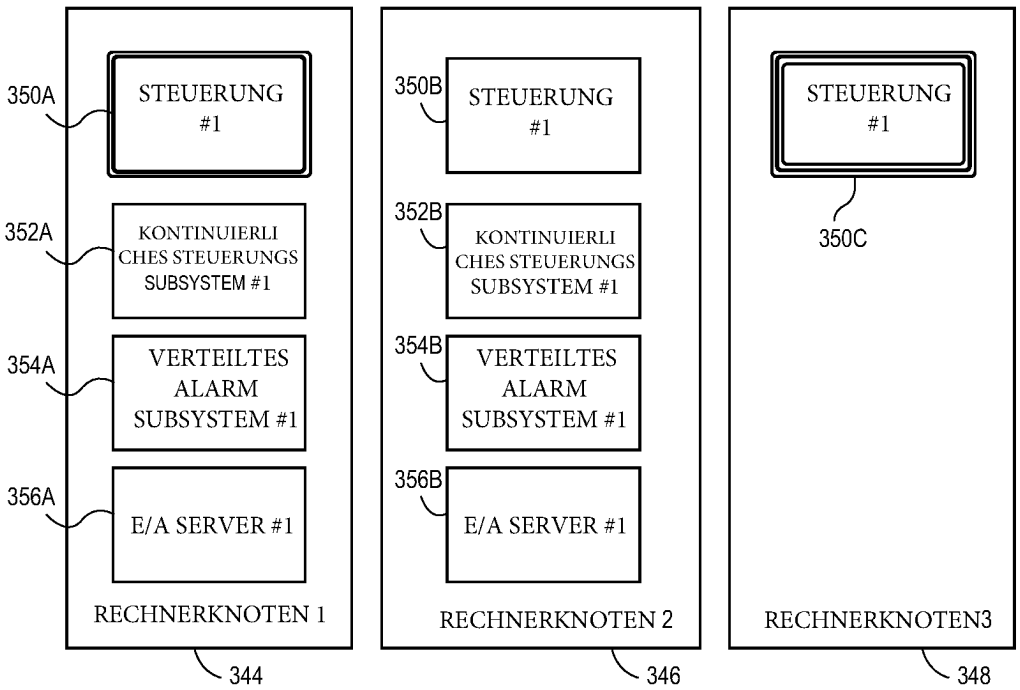

350A
STEUERUNG #1
352A
KONTINUIERLICHES STEUERUNGS SUBSYSTEM #1
354A
VERTEILTES ALARM SUBSYSTEM #1
356A
E/A SERVER #1
RECHNERKNOTEN 1
344
350B
STEUERUNG #1
352B
KONTINUIERLICHES STEUERUNGS SUBSYSTEM #1
354B
VERTEILTES ALARM SUBSYSTEM #1
356B
E/A SERVER #1
RECHNERKNOTEN 2
346
STEUERUNG #1
350C
RECHNERKNOTEN3
348

FIG. 5A

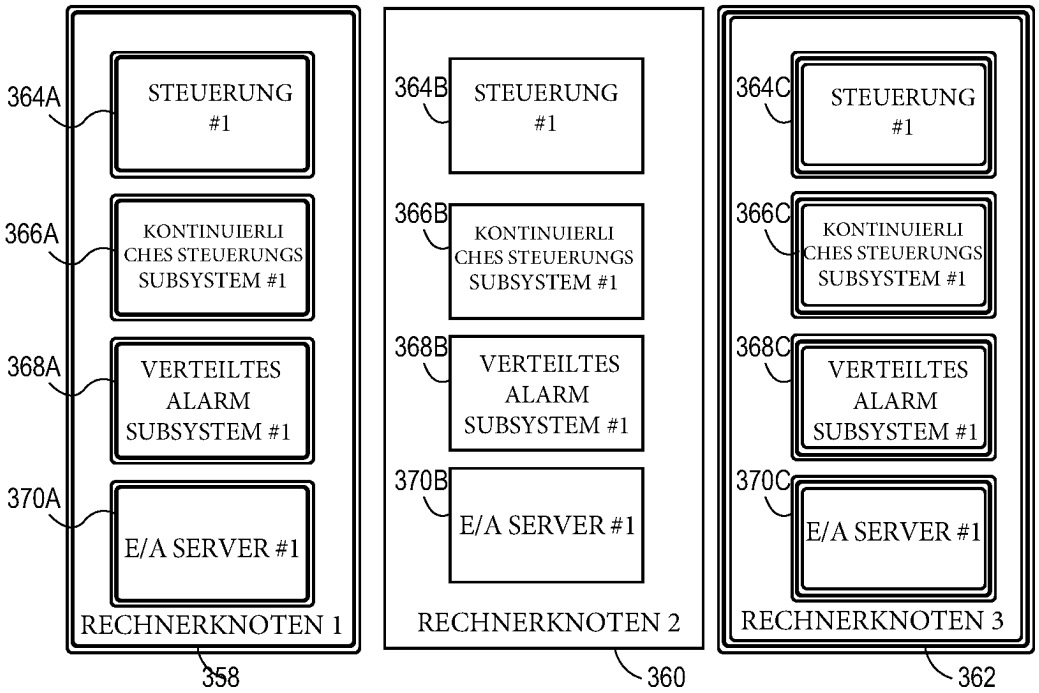

364A
STEUERUNG #1
366A
KONTINUIERLICHES STEUERUNGS SUBSYSTEM #1
368A
VERTEILTES ALARM SUBSYSTEM #1
370A
E/A SERVER #1
RECHNERKNOTEN 1
358
364B
STEUERUNG #1
366B
KONTINUIERLICHES STEUERUNGS SUBSYSTEM #1
368B
VERTEILTES ALARM SUBSYSTEM #1
370B
E/A SERVER #1
RECHNERKNOTEN 2
360
364C
STEUERUNG #1
366C
KONTINUIERLICHES STEUERUNGS SUBSYSTEM #1
368C
VERTEILTES ALARM SUBSYSTEM #1
370C
E/A SERVER #1
RECHNERKNOTEN 3
362

FIG. 5B

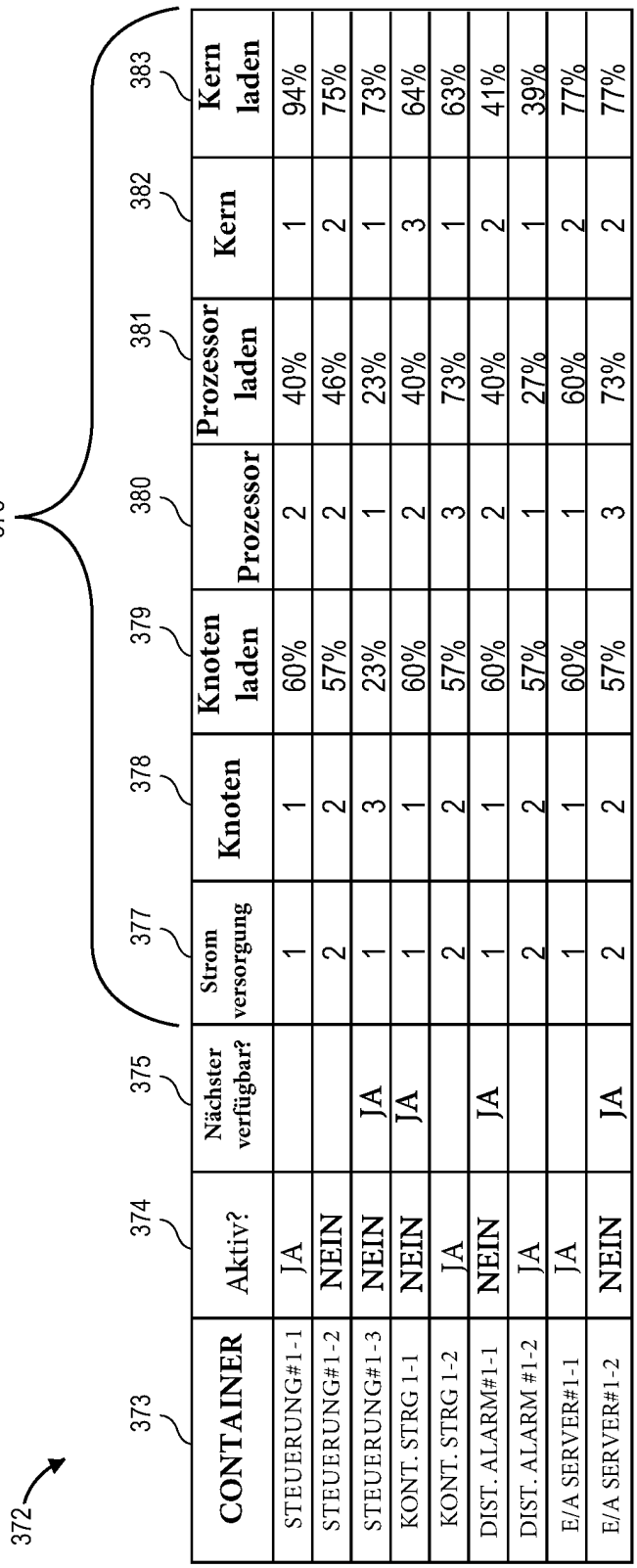

372
373
374
375
376
377
378
379
380
381
382
383
CONTAINER
Aktiv?
Nächster verfügbar?
Strom versorgung
Knoten
Knoten laden
Prozessor
Prozessor laden
Kern
Kern laden
STEUERUNG#1-1
JA
1
1
60%
2
40%
1
94%
STEUERUNG#1-2
NEIN
2
2
57%
2
46%
2
75%
STEUERUNG#1-3
NEIN
JA
1
3
23%
1
23%
1
73%
KONT. STRG 1-1
NEIN
JA
1
1
60%
2
40%
3
64%
KONT. STRG 1-2
JA
2
2
57%
3
73%
1
63%
DIST. ALARM#1-1
NEIN
JA
1
1
60%
2
40%
2
41%
DIST. ALARM #1-2
JA
2
2
57%
1
27%
1
39%
E/A SERVER#1-1
JA
1
1
60%
1
60%
2
77%
E/A SERVER#1-2
NEIN
JA
2
2
57%
3
73%
2
77%

FIG. 6

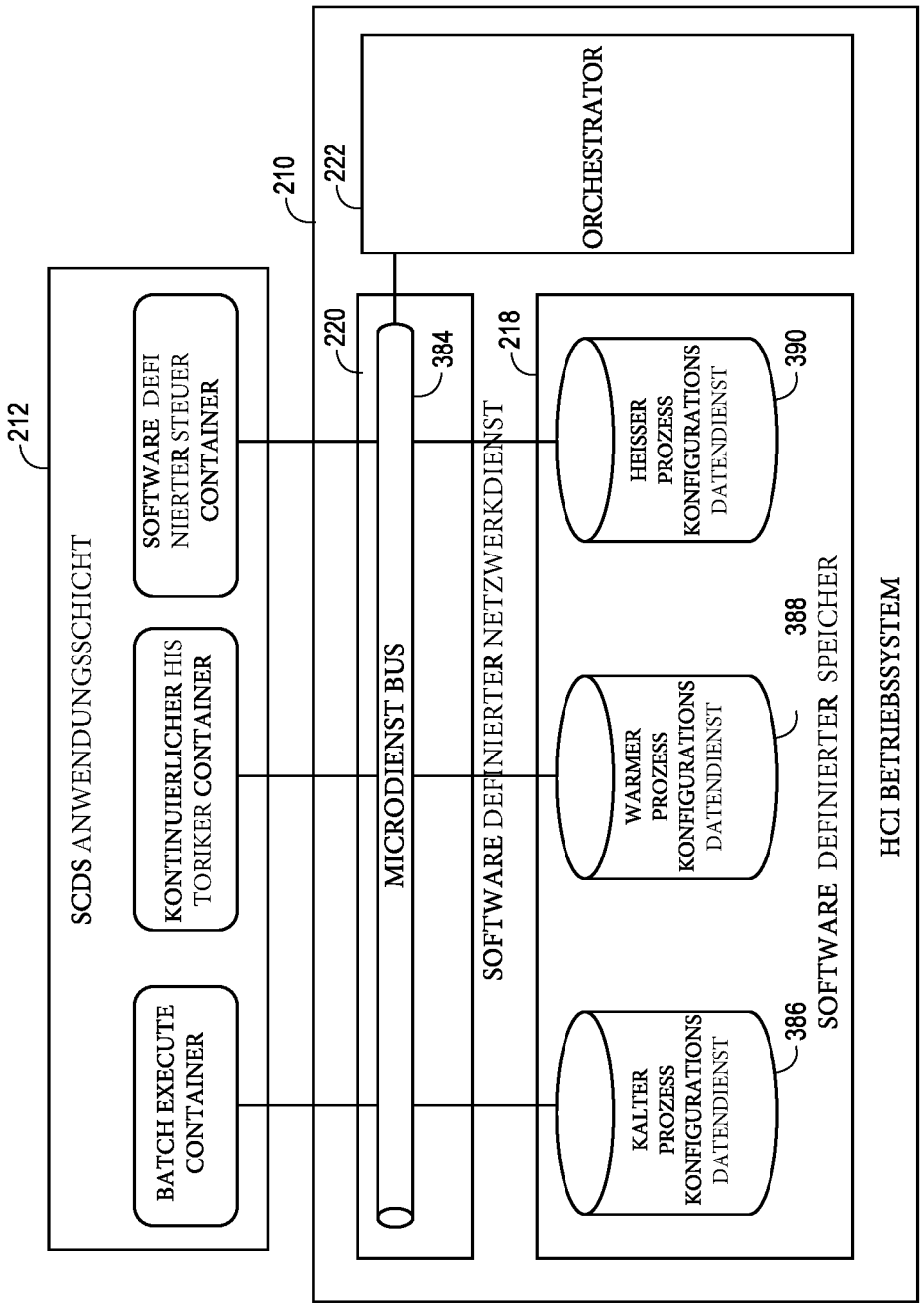

212
SCDS ANWENDUNGSSCHICHT
BATCH EXECUTE CONTAINER
KONTINUIERLICHER HISTORIKER CONTAINER
SOFTWARE DEFINIERTER STEUER CONTAINER
210
220
MICRODIENST BUS
384
222
ORCHESTRATOR
218
SOFTWARE DEFINIERTER NETZWERKDIENST
HEISSER PROZESS KONFIGURATIONS DATENDIENST
390
WARMER PROZESS KONFIGURATIONS DATENDIENST
388
KALTER PROZESS KONFIGURATIONS DATENDIENST
386
SOFTWARE DEFINIERTER SPEICHER
HCI BETRIEBSSYSTEM

FIG. 7

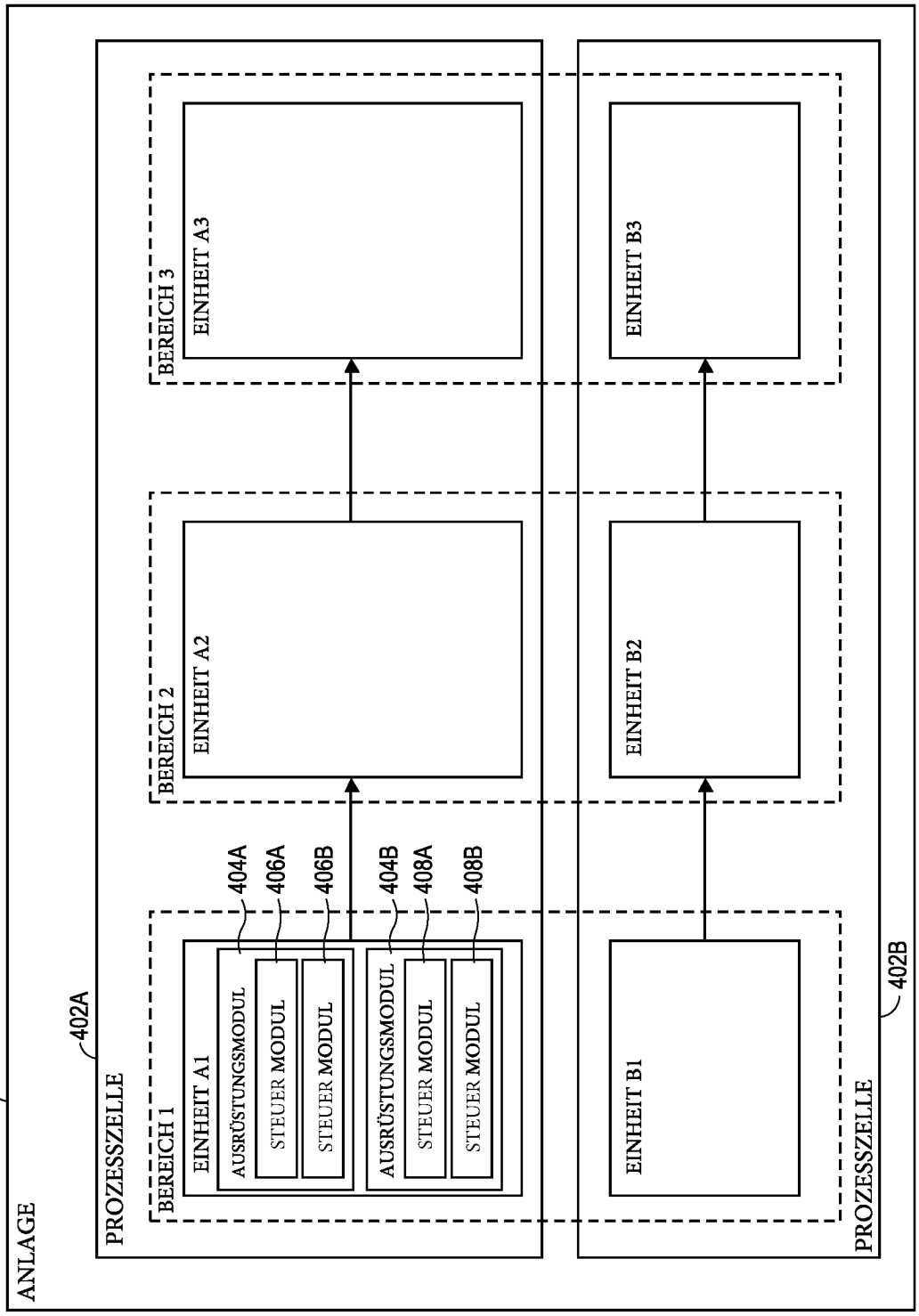

400
ANLAGE
402A
PROZESSZELLE
BEREICH 1
EINHEIT A1
AUSRÜSTUNGSMODUL
STEUER MODUL
STEUER MODUL
AUSRÜSTUNGSMODUL
STEUER MODUL
STEUER MODUL
404A
406A
406B
404B
408A
408B
BEREICH 2
EINHEIT A2
BEREICH 3
EINHEIT A3
EINHEIT B1
EINHEIT B2
EINHEIT B3
PROZESSZELLE
402B

FIG. 8

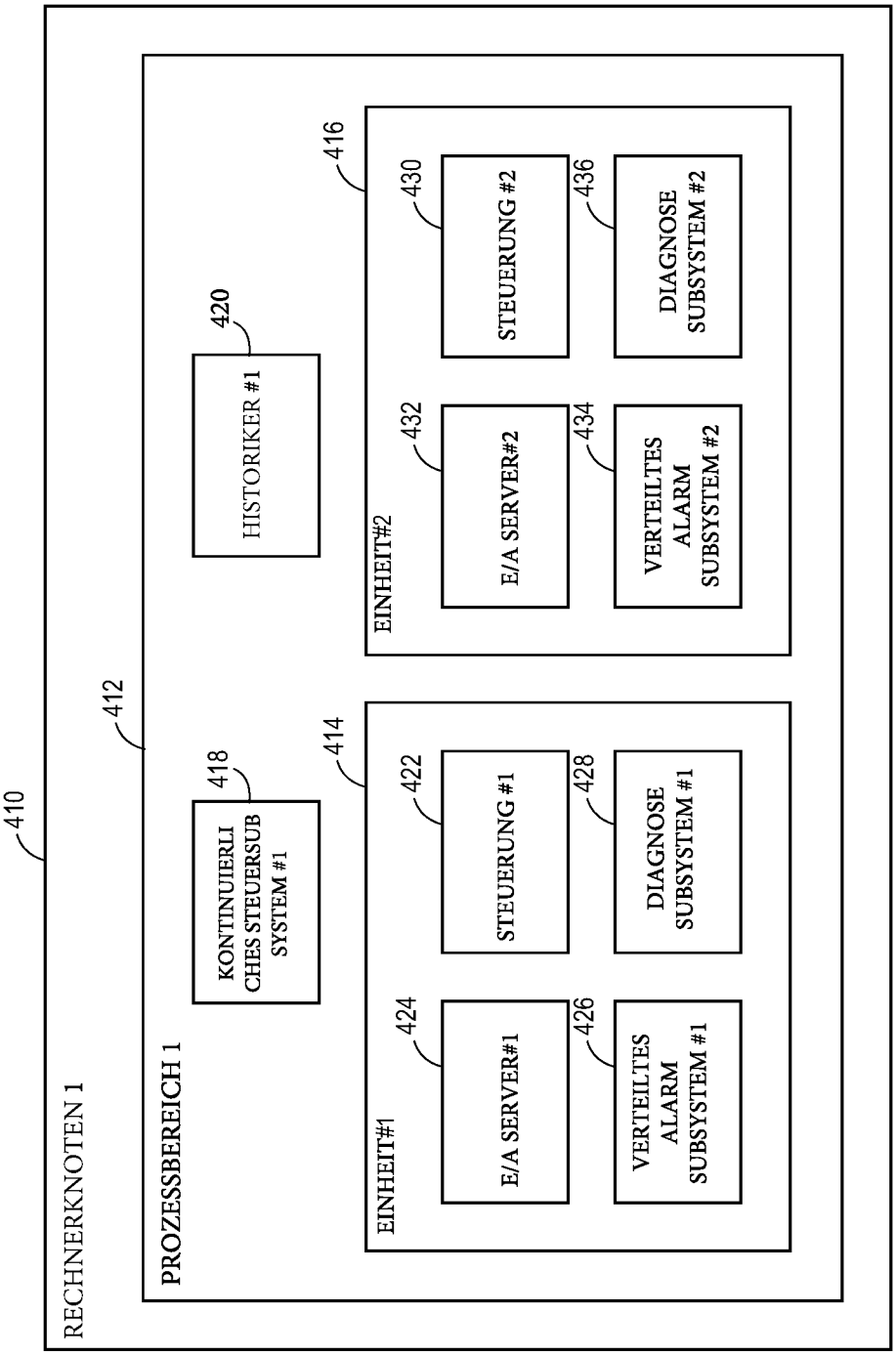

410
RECHNERKNOTEN 1
412
PROZESSBEREICH 1
418
KONTINUIERLICHES STEUERSUBSYSTEM #1
420
HISTORIKER #1
414
EINHEIT#1
422
STEUERUNG #1
428
DIAGNOSE SUBSYSTEM #1
424
E/A SERVER#1
426
VERTEILTES ALARM SUBSYSTEM #1
416
EINHEIT#2
430
STEUERUNG #2
436
DIAGNOSE SUBSYSTEM #2
432
E/A SERVER#2
434
VERTEILTES ALARM SUBSYSTEM #2

FIG. 9

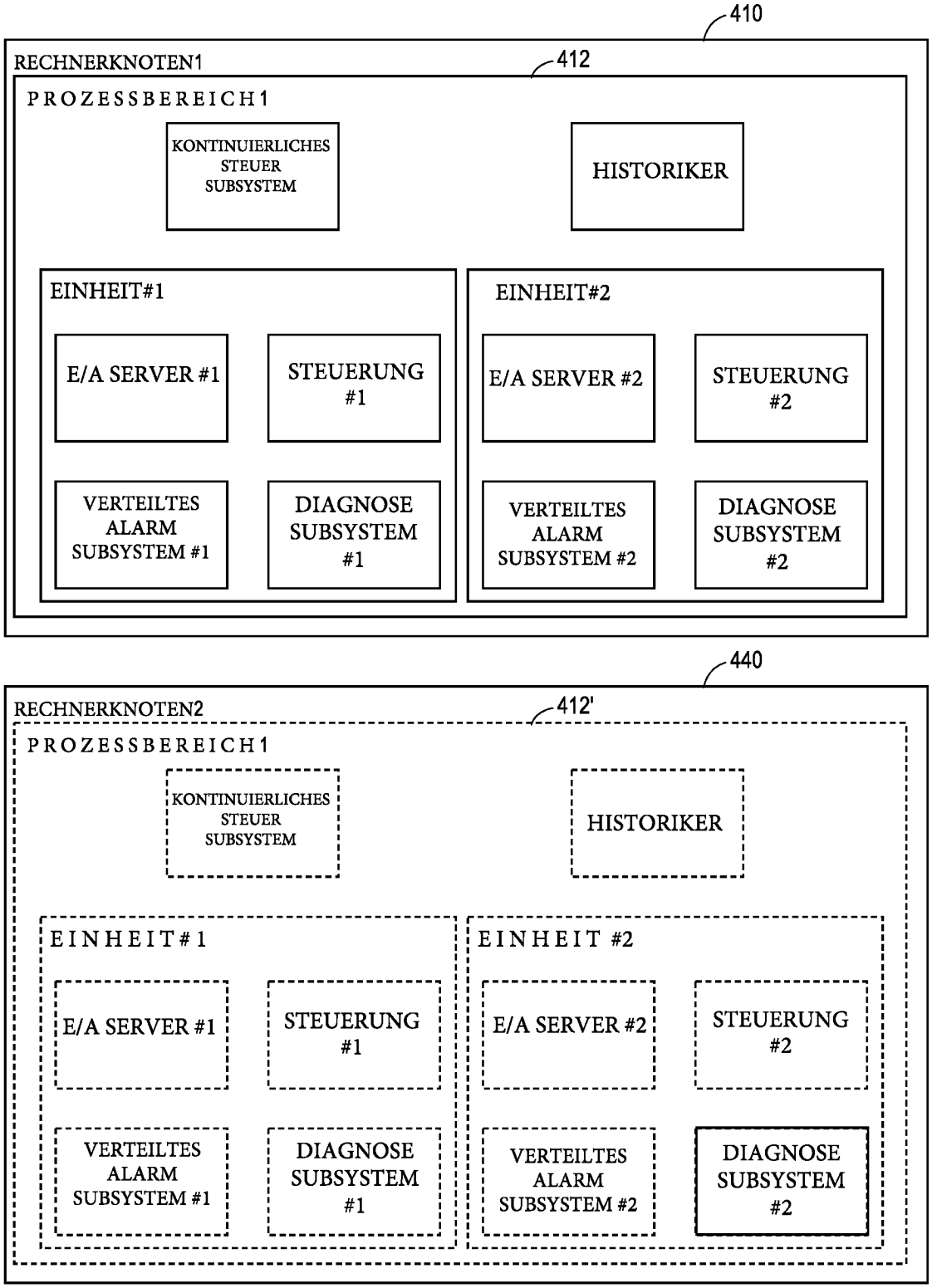

410
RECHNERKNOTEN1
412
PROZESSBEREICH1
KONTINUIERLICHES STEUER SUBSYSTEM
HISTORIKER
EINHEIT#1
E/A SERVER #1
STEUERUNG #1
VERTEILTES ALARM SUBSYSTEM #1
DIAGNOSE SUBSYSTEM #1
EINHEIT#2
E/A SERVER #2
STEUERUNG #2
VERTEILTES ALARM SUBSYSTEM #2
DIAGNOSE SUBSYSTEM #2
440
RECHNERKNOTEN2
412'
PROZESSBEREICH1
KONTINUIERLICHES STEUER SUBSYSTEM
HISTORIKER
EINHEIT#1
E/A SERVER #1
STEUERUNG #1
VERTEILTES ALARM SUBSYSTEM #1
DIAGNOSE SUBSYSTEM #1
EINHEIT #2
E/A SERVER #2
STEUERUNG #2
VERTEILTES ALARM SUBSYSTEM #2
DIAGNOSE SUBSYSTEM #2

FIG. 10

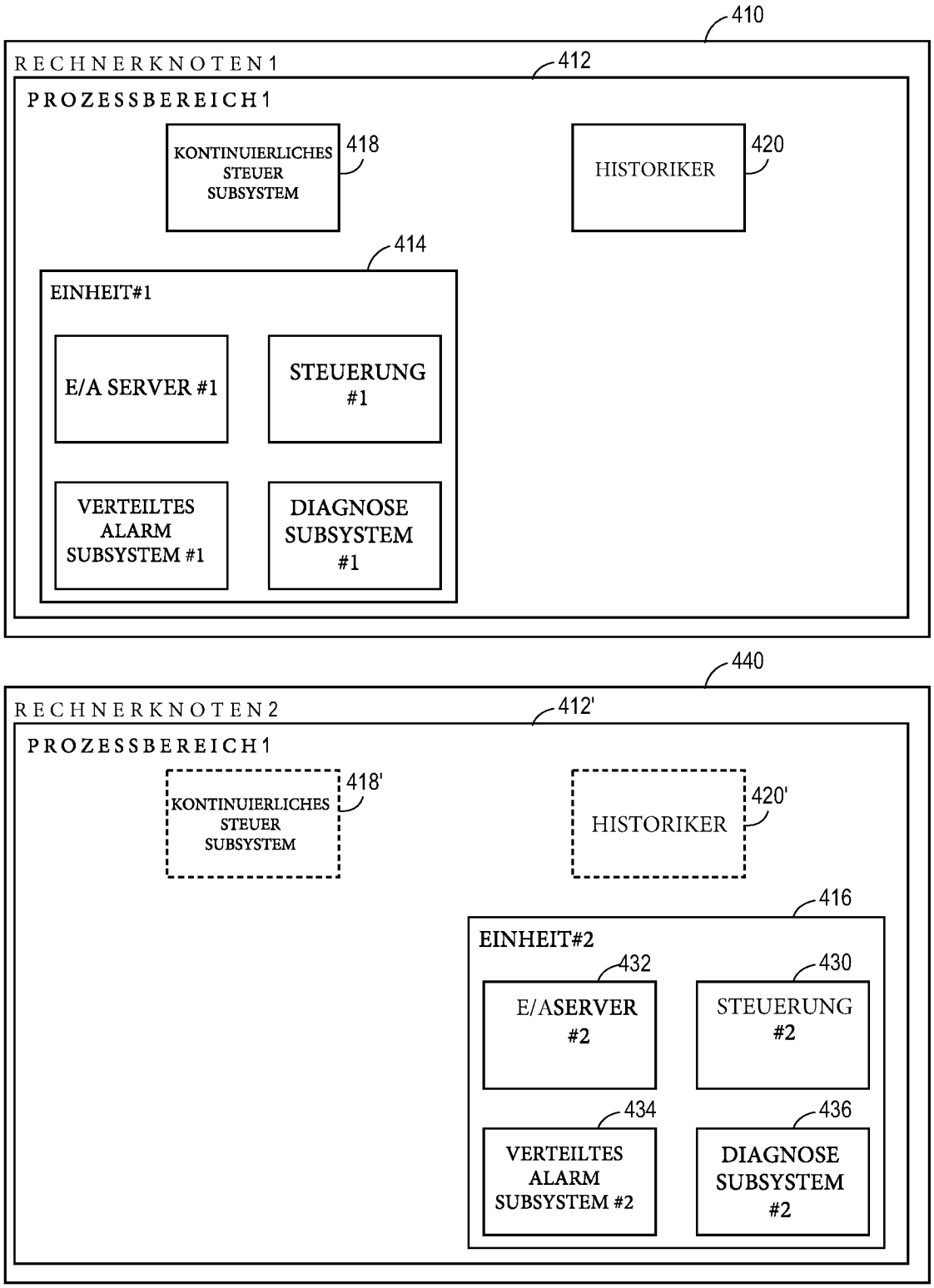

410
RECHNERKNOTEN 1
412
PROZESSBEREICH 1
KONTINUIERLICHES STEUER SUBSYSTEM
418
HISTORIKER
420
414
EINHEIT#1
E/A SERVER #1
STEUERUNG #1
VERTEILTES ALARM SUBSYSTEM #1
DIAGNOSE SUBSYSTEM #1
440
RECHNERKNOTEN 2
412'
PROZESSBEREICH 1
KONTINUIERLICHES STEUER SUBSYSTEM
418'
HISTORIKER
420'
416
EINHEIT#2
432
E/ASERVER #2
430
STEUERUNG #2
434
VERTEILTES ALARM SUBSYSTEM #2
436
DIAGNOSE SUBSYSTEM #2

FIG. 11

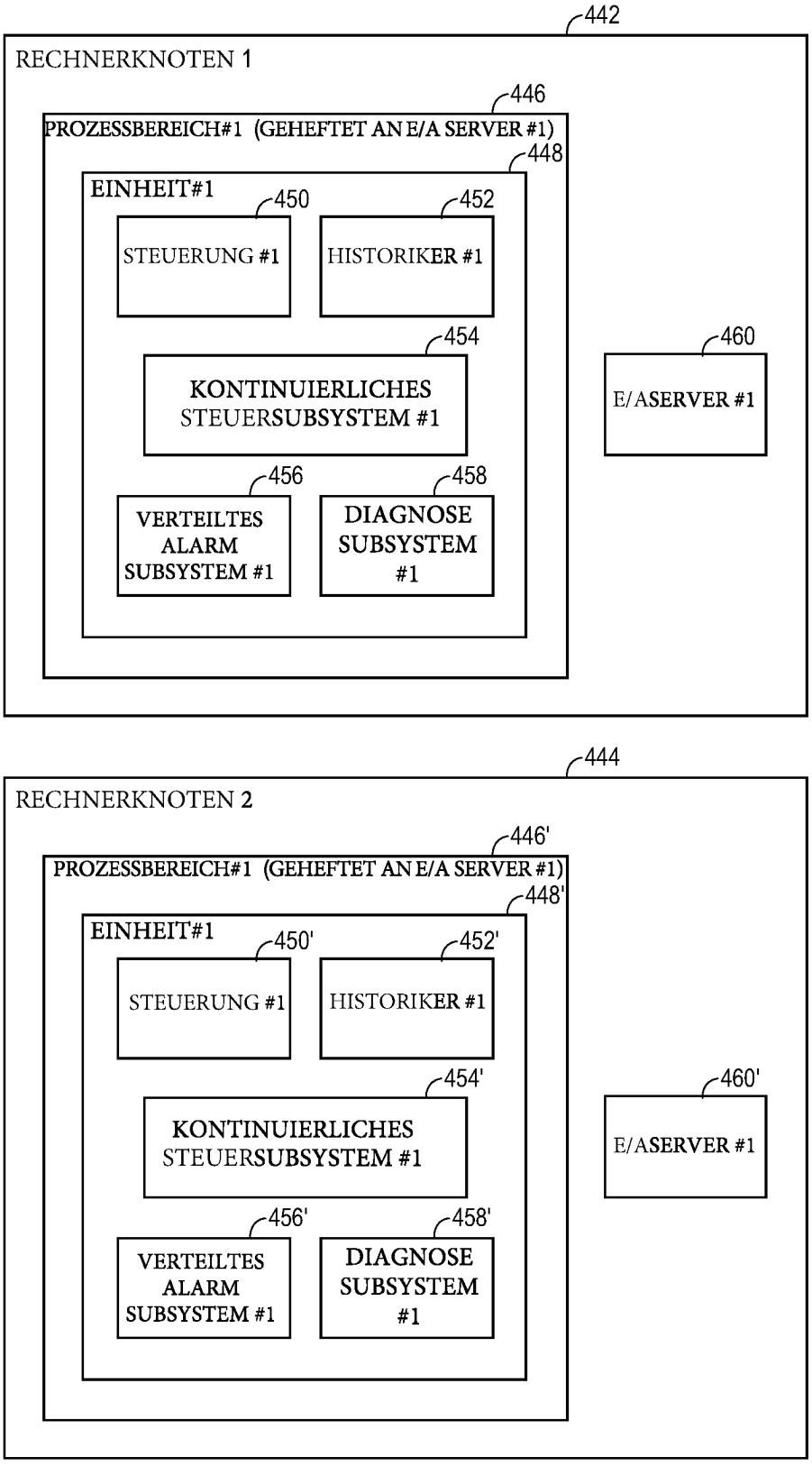

442
RECHNERKNOTEN 1
446
PROZESSBEREICH#1 (GEHEFTET AN E/A SERVER #1)
448
EINHEIT#1
450
STEUERUNG #1
452
HISTORIKER #1
454
KONTINUIERLICHES STEUERSUBSYSTEM #1
456
VERTEILTES ALARM SUBSYSTEM #1
458
DIAGNOSE SUBSYSTEM #1
460
E/ASERVER #1
444
RECHNERKNOTEN 2
446'
PROZESSBEREICH#1 (GEHEFTET AN E/A SERVER #1)
448'
EINHEIT#1
450'
STEUERUNG #1
452'
HISTORIKER #1
454'
KONTINUIERLICHES STEUERSUBSYSTEM #1
456'
VERTEILTES ALARM SUBSYSTEM #1
458'
DIAGNOSE SUBSYSTEM #1
460'
E/ASERVER #1

FIG. 12

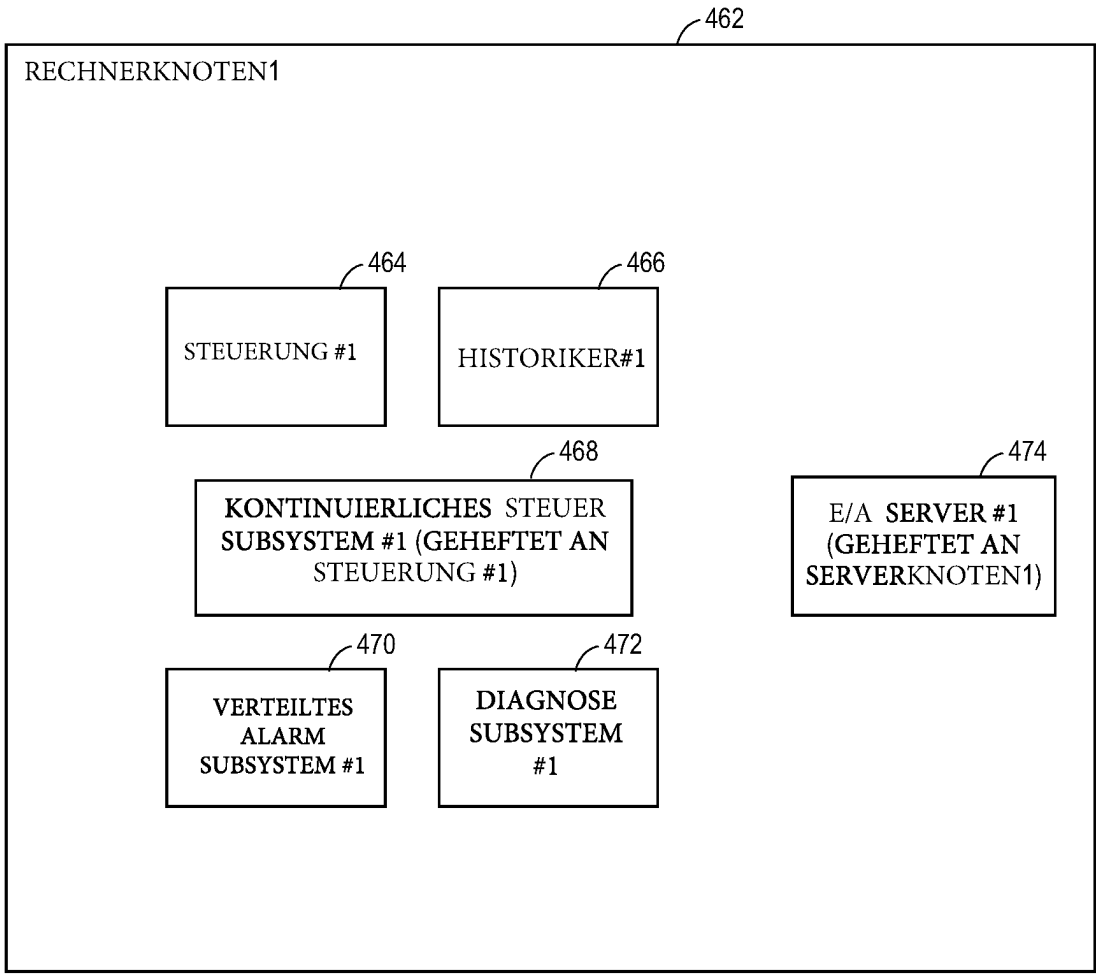

462
RECHNERKNOTEN1
464
STEUERUNG #1
466
HISTORIKER#1
468
KONTINUIERLICHES STEUER SUBSYSTEM #1 (GEHEFTET AN STEUERUNG #1)
474
E/A SERVER #1 (GEHEFTET AN SERVERKNOTEN1)
470
VERTEILTES ALARM SUBSYSTEM #1
472
DIAGNOSE SUBSYSTEM #1

FIG. 13

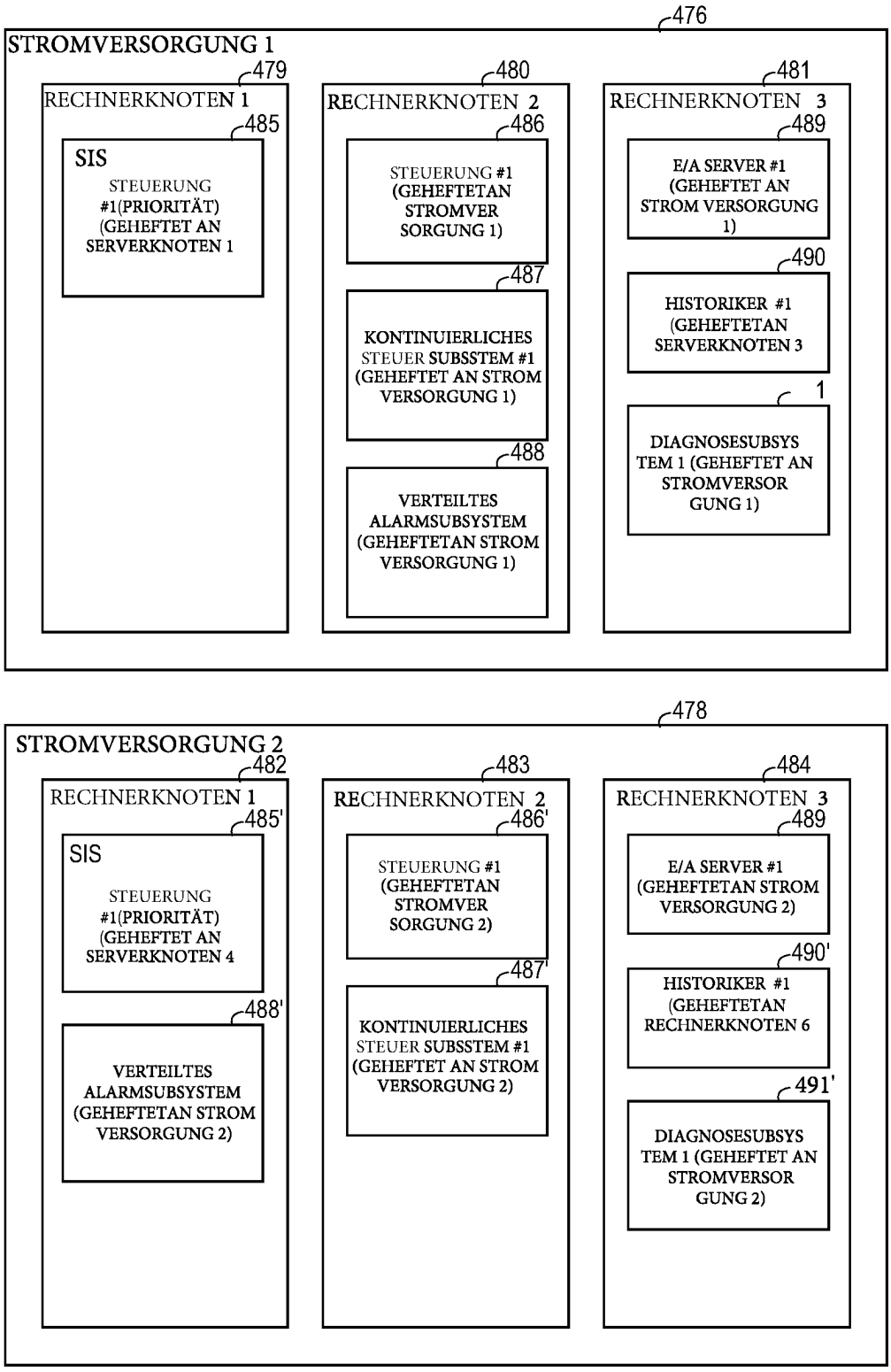

476
STROMVERSORGUNG 1
479
RECHNERKNOTEN 1
485
SIS
STEUERUNG #1(PRIORITÄT) (GEHEFTET AN SERVERKNOTEN 1
480
RECHNERKNOTEN 2
486
STEUERUNG #1 (GEHEFTETAN STROMVER SORGUNG 1)
487
KONTINUIERLICHES STEUER SUBSSTEM #1 (GEHEFTET AN STROM VERSORGUNG 1)
488
VERTEILTES ALARMSUBSYSTEM (GEHEFTETAN STROM VERSORGUNG 1)
481
RECHNERKNOTEN 3
489
E/A SERVER #1 (GEHEFTET AN STROM VERSORGUNG 1)
490
HISTORIKER #1 (GEHEFTETAN SERVERKNOTEN 3
1
DIAGNOSESUBSYS TEM 1 (GEHEFTET AN STROMVERSOR GUNG 1)
478
STROMVERSORGUNG 2
482
RECHNERKNOTEN 1
485'
SIS
STEUERUNG #1(PRIORITÄT) (GEHEFTET AN SERVERKNOTEN 4
488'
VERTEILTES ALARMSUBSYSTEM (GEHEFTETAN STROM VERSORGUNG 2)
483
RECHNERKNOTEN 2
486'
STEUERUNG #1 (GEHEFTETAN STROMVER SORGUNG 2)
487'
KONTINUIERLICHES STEUER SUBSSTEM #1 (GEHEFTET AN STROM VERSORGUNG 2)
484
RECHNERKNOTEN 3
489
E/A SERVER #1 (GEHEFTETAN STROM VERSORGUNG 2)
490'
HISTORIKER #1 (GEHEFTETAN RECHNERKNOTEN 6
491'
DIAGNOSESUBSYS TEM 1 (GEHEFTET AN STROMVERSOR GUNG 2)

FIG. 14

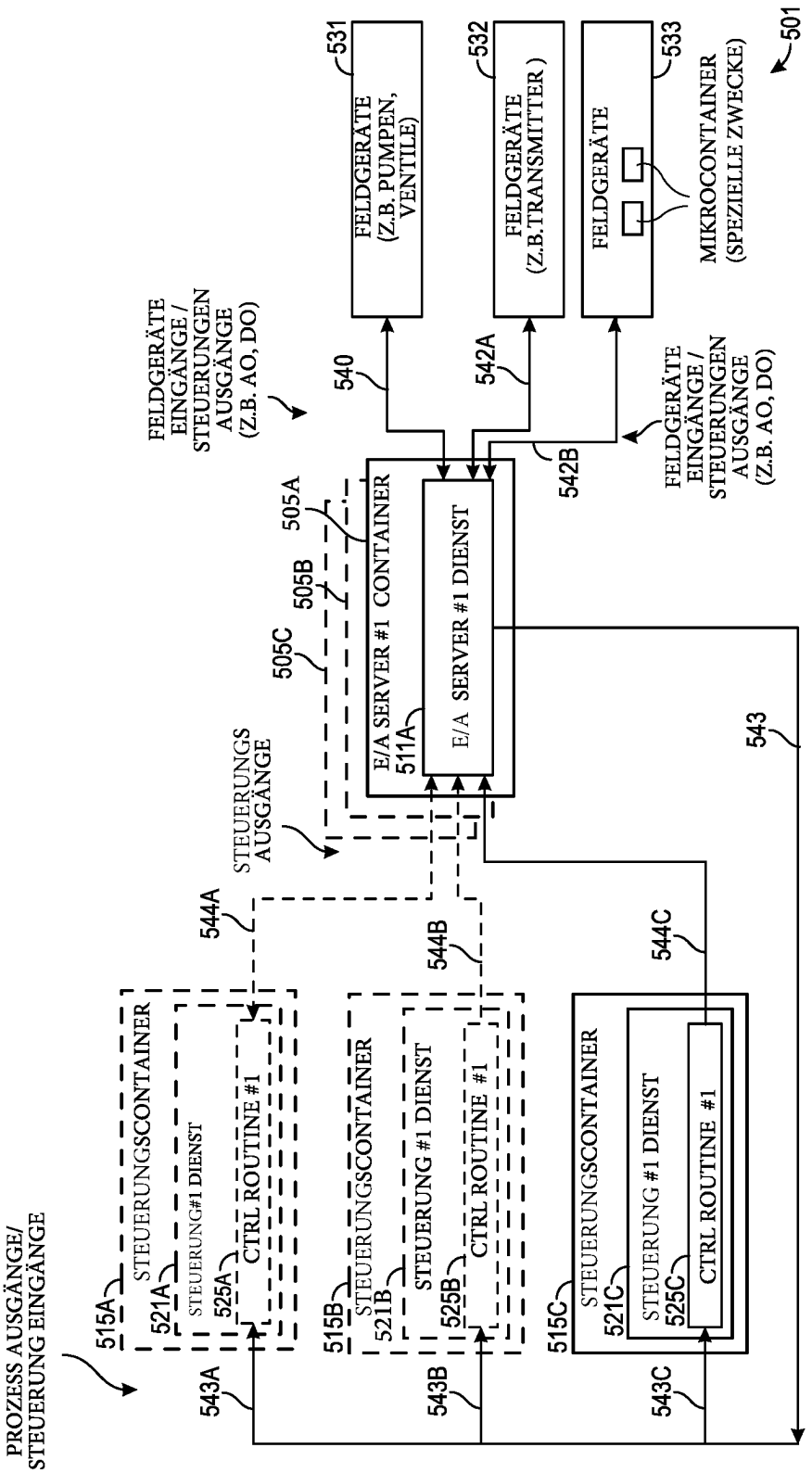

PROZESS AUSGÄNGE/
STEUERUNG EINGÄNGE
515A
STEUERUNGSCONTAINER
521A
STEUERUNG#1 DIENST
525A
CTRL ROUTINE #1
543A
515B
STEUERUNGSCONTAINER
521B
STEUERUNG #1 DIENST
525B
CTRL ROUTINE #1
543B
515C
STEUERUNGSCONTAINER
521C
STEUERUNG #1 DIENST
525C
CTRL ROUTINE #1
543C
544A
544B
544C
STEUERUNGS
AUSGÄNGE
505A
505B
505C
E/A SERVER #1 CONTAINER
511A
E/A SERVER #1 DIENST
543
FELDGERÄTE
EINGÄNGE /
STEUERUNGEN
AUSGÄNGE
(Z.B. AO, DO)
540
542A
542B
531
FELDGERÄTE
(Z.B. PUMPEN,
VENTILE)
532
FELDGERÄTE
(Z.B.TRANSMITTER)
533
FELDGERÄTE
MIKROCONTAINER
(SPEZIELLE ZWECKE)
501
FELDGERÄTE
EINGÄNGE /
STEUERUNGEN
AUSGÄNGE
(Z.B. AO, DO)

FIG. 15

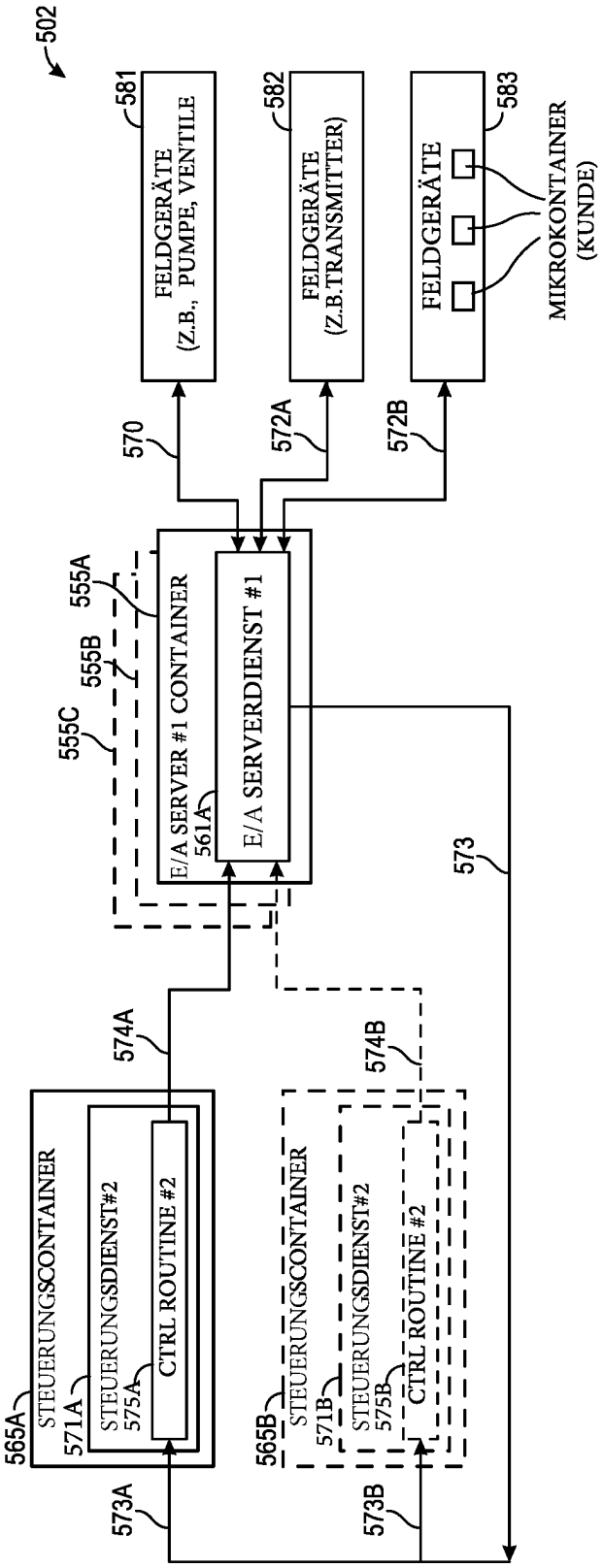


FIG. 15
(FORTSETZUNG)

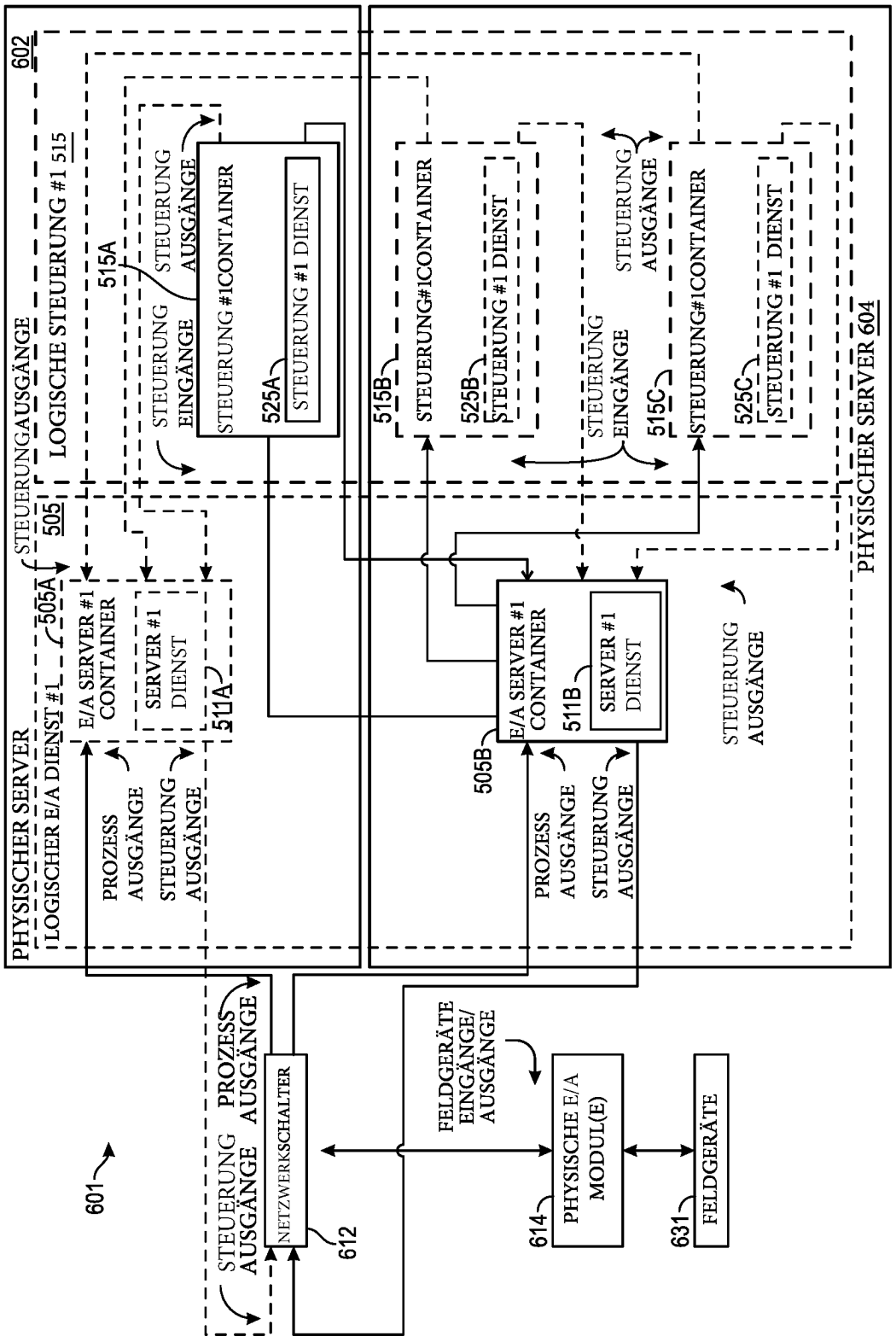

601
602
PHYSISCHER SERVER
LOGISCHER E/A DIENST #1 505
505A
E/A SERVER #1 CONTAINER
SERVER #1 DIENST
511A
PROZESS AUSGÄNGE
STEUERUNG AUSGÄNGE
STEUERUNGAUSGÄNGE
LOGISCHE STEUERUNG #1 515
515A
STEUERUNG EINGÄNGE
STEUERUNG AUSGÄNGE
STEUERUNG #1CONTAINER
525A
STEUERUNG #1 DIENST
505B
E/A SERVER #1 CONTAINER
511B
SERVER #1 DIENST
PROZESS AUSGÄNGE
STEUERUNG AUSGÄNGE
515B
STEUERUNG#1CONTAINER
525B
STEUERUNG #1 DIENST
STEUERUNG EINGÄNGE
515C
STEUERUNG AUSGÄNGE
STEUERUNG#1CONTAINER
525C
STEUERUNG #1 DIENST
STEUERUNG AUSGÄNGE
PHYSISCHER SERVER 604
STEUERUNG AUSGÄNGE
PROZESS AUSGÄNGE
NETZWERKSCHALTER
612
FELDGERÄTE EINGÄNGE/ AUSGÄNGE
614
PHYSISCHE E/A MODUL(E)
631
FELDGERÄTE

FIG. 16

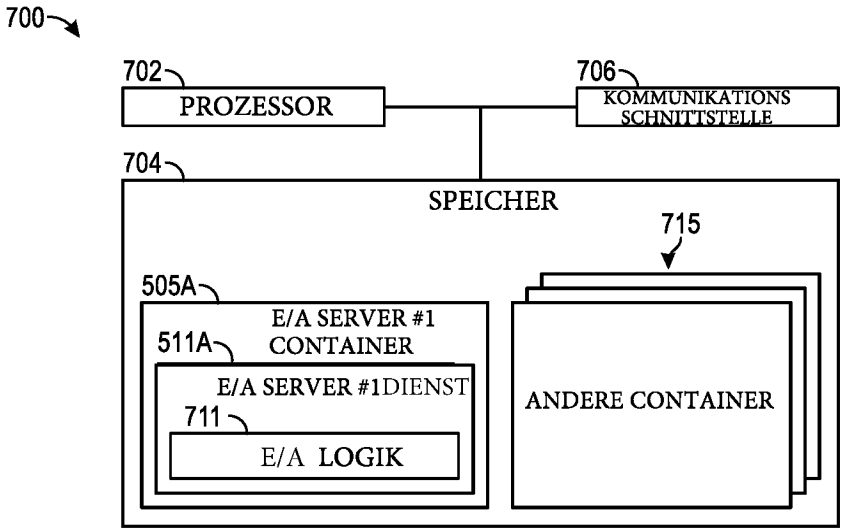

700
702
PROZESSOR
706
KOMMUNIKATIONS SCHNITTSTELLE
704
SPEICHER
715
505A
E/A SERVER #1 CONTAINER
511A
E/A SERVER #1DIENST
711
E/A LOGIK
ANDERE CONTAINER

FIG. 17

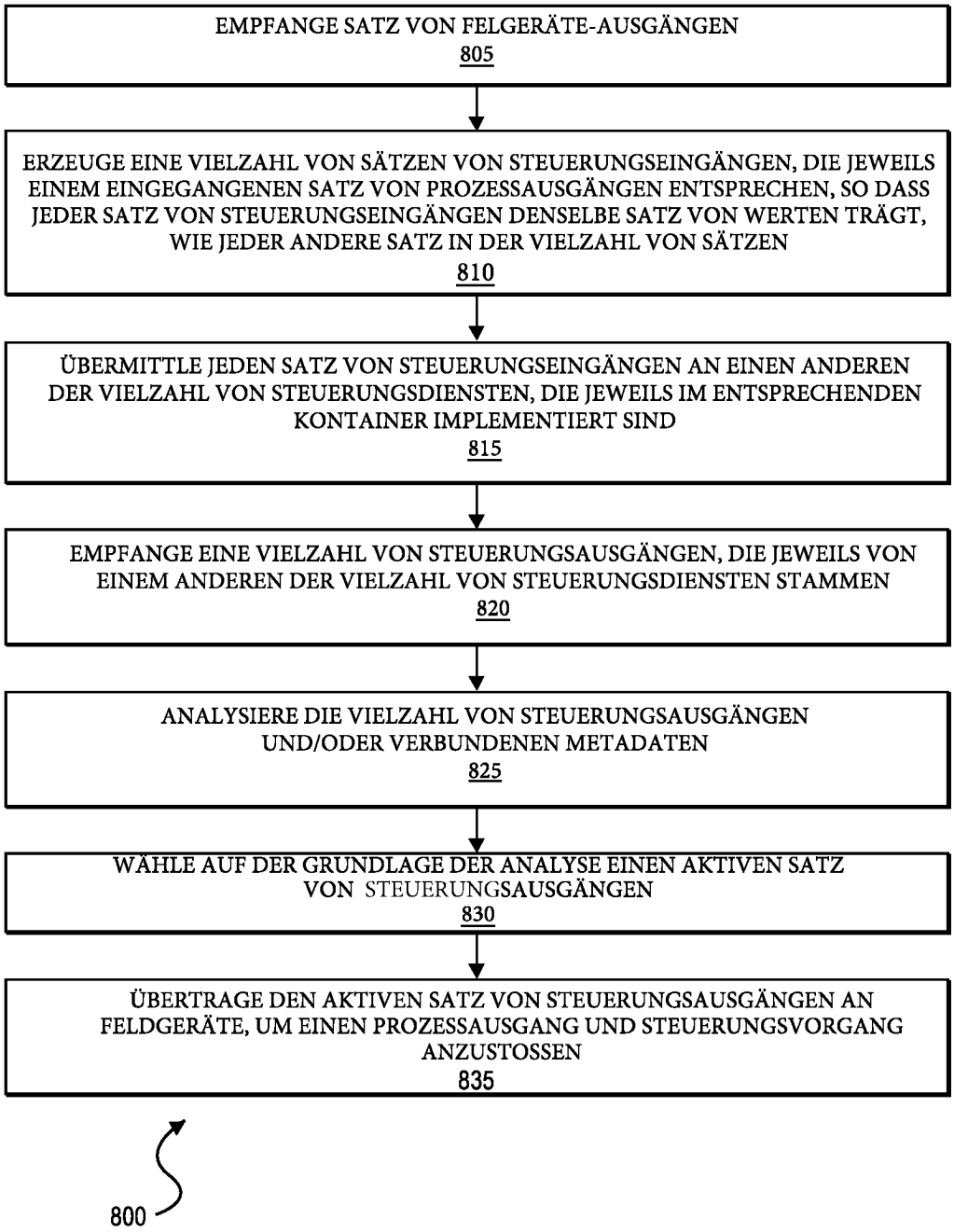

EMPFANGE SATZ VON FELGERÄTE-AUSGÄNGEN
805
ERZEUGE EINE VIELZAHL VON SÄTZEN VON STEUERUNGSEINGÄNGEN, DIE JEWEILS EINEM EINGEGANGENEN SATZ VON PROZESSAUSGÄNGEN ENTSPRECHEN, SO DASS JEDER SATZ VON STEUERUNGSEINGÄNGEN DENSELBE SATZ VON WERTEN TRÄGT, WIE JEDER ANDERE SATZ IN DER VIELZAHL VON SÄTZEN
810
ÜBERMITTLE JEDEN SATZ VON STEUERUNGSEINGÄNGEN AN EINEN ANDEREN DER VIELZAHL VON STEUERUNGSDIENSTEN, DIE JEWEILS IM ENTSPRECHENDEN KONTAINER IMPLEMENTIERT SIND
815
EMPFANGE EINE VIELZAHL VON STEUERUNGSAUSGÄNGEN, DIE JEWEILS VON EINEM ANDEREN DER VIELZAHL VON STEUERUNGSDIENSTEN STAMMEN
820
ANALYSIERE DIE VIELZAHL VON STEUERUNGSAUSGÄNGEN UND/ODER VERBUNDENEN METADATEN
825
WÄHLE AUF DER GRUNDLAGE DER ANALYSE EINEN AKTIVEN SATZ VON STEUERUNGSAUSGÄNGEN
830
ÜBERTRAGE DEN AKTIVEN SATZ VON STEUERUNGSAUSGÄNGEN AN FELDGERÄTE, UM EINEN PROZESSAUSGANG UND STEUERUNGSVORGANG ANZUSTOSSEN
835
800

FIG. 18

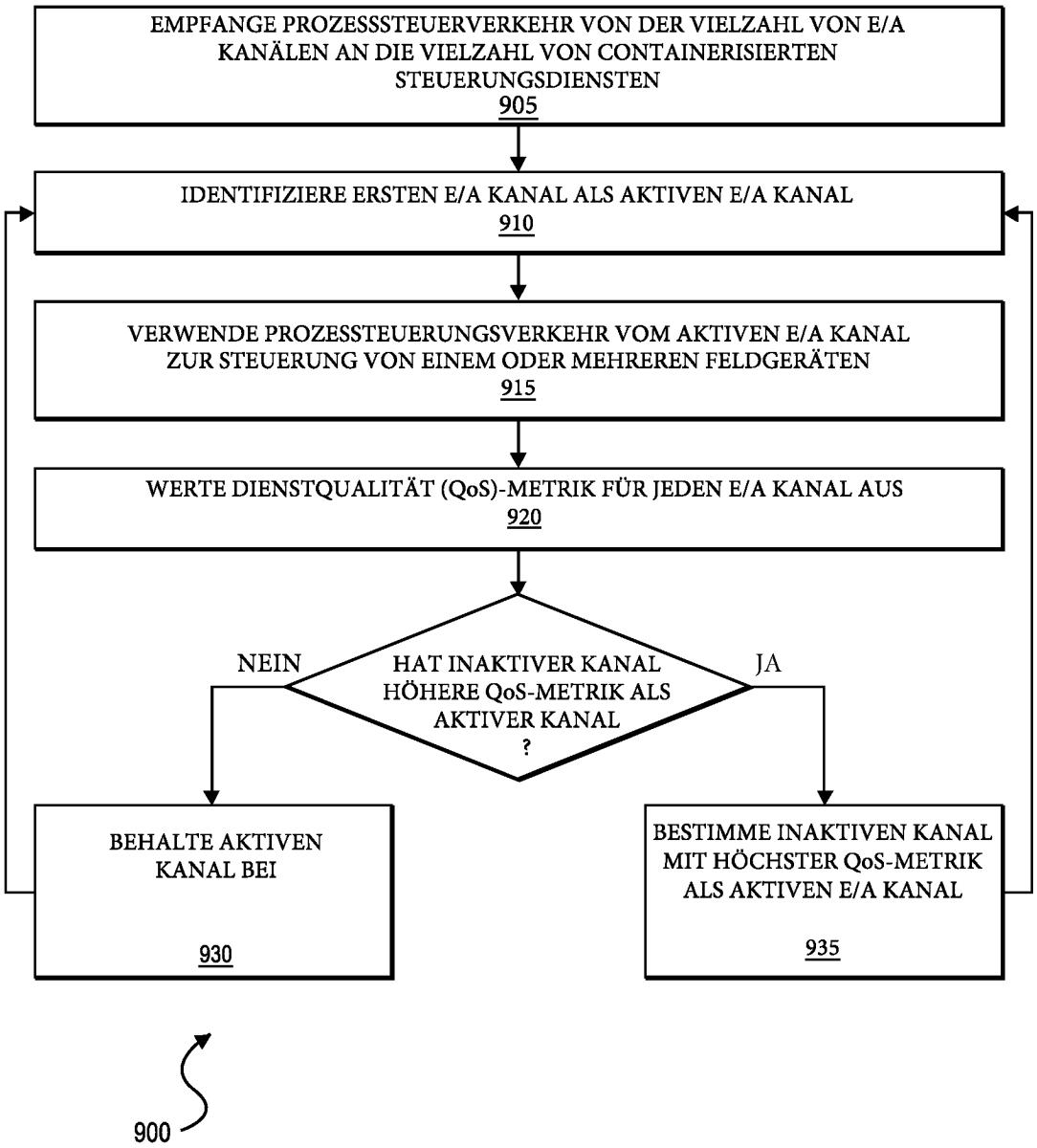

EMPFANGE PROZESSSTEUERVERKEHR VON DER VIELZAHL VON E/A KANÄLEN AN DIE VIELZAHL VON CONTAINERISIERTEN STEUERUNGSDIENSTEN
905
IDENTIFIZIERE ERSTEN E/A KANAL ALS AKTIVEN E/A KANAL
910
VERWENDE PROZESSTEUERUNGSVERKEHR VOM AKTIVEN E/A KANAL ZUR STEUERUNG VON EINEM ODER MEHREREN FELDGERÄTEN
915
WERTE DIENSTQUALITÄT (QoS)-METRIK FÜR JEDEN E/A KANAL AUS
920
HAT INAKTIVER KANAL HÖHERE QoS-METRIK ALS AKTIVER KANAL ?
NEIN
JA
BEHALTE AKTIVEN KANAL BEI
930
BESTIMME INAKTIVEN KANAL MIT HÖCHSTER QoS-METRIK ALS AKTIVEN E/A KANAL
935
900

FIG. 19

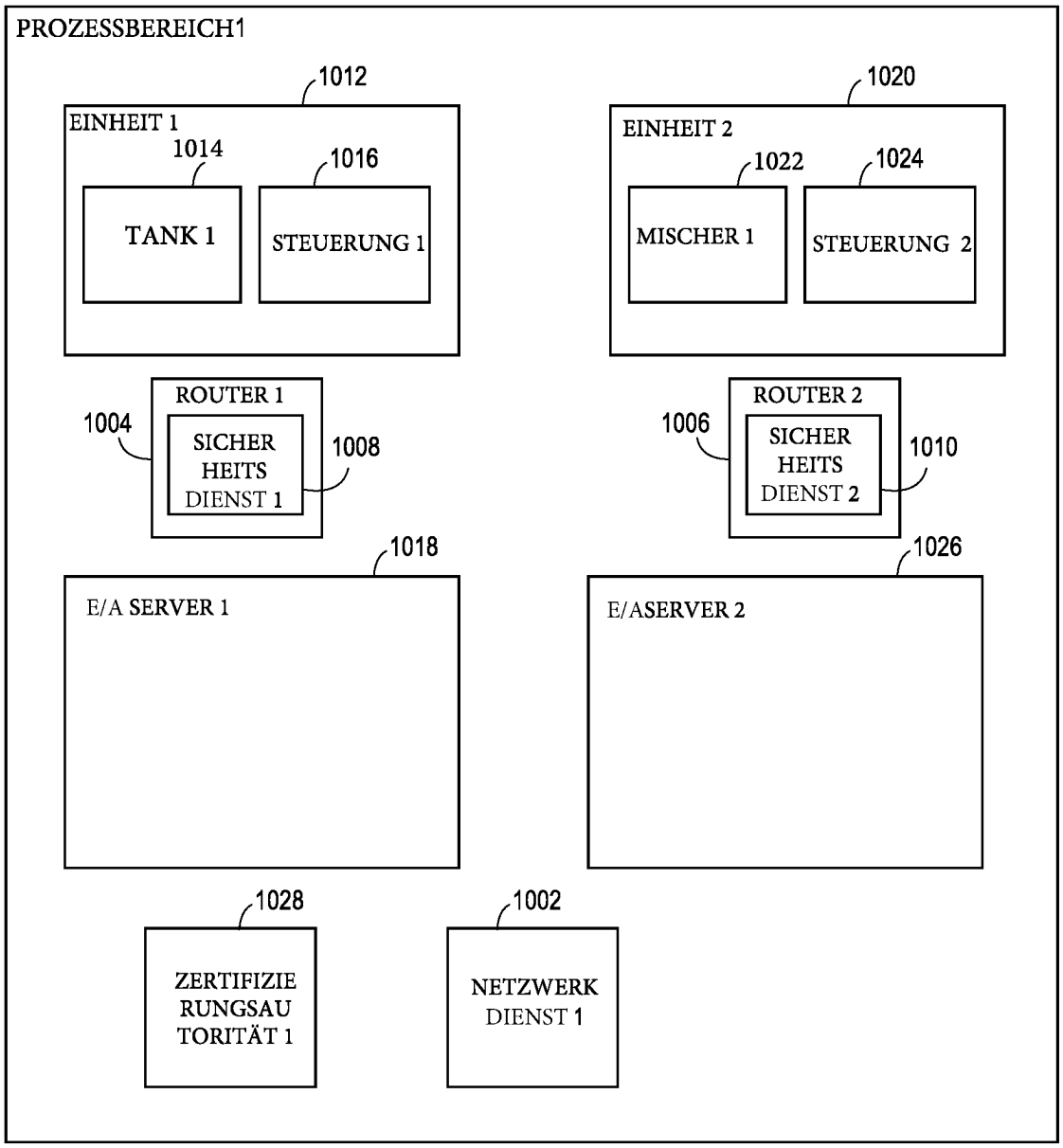

PROZESSBEREICH1
1012
EINHEIT 1
1014
TANK 1
1016
STEUERUNG 1
1020
EINHEIT 2
1022
MISCHER 1
1024
STEUERUNG 2
ROUTER 1
1004
SICHER HEITS DIENST 1
1008
ROUTER 2
1006
SICHER HEITS DIENST 2
1010
1018
E/A SERVER 1
1026
E/ASERVER 2
1028
ZERTIFIZIE RUNGSAU TORITÄT 1
1002
NETZWERK DIENST 1

FIG. 20

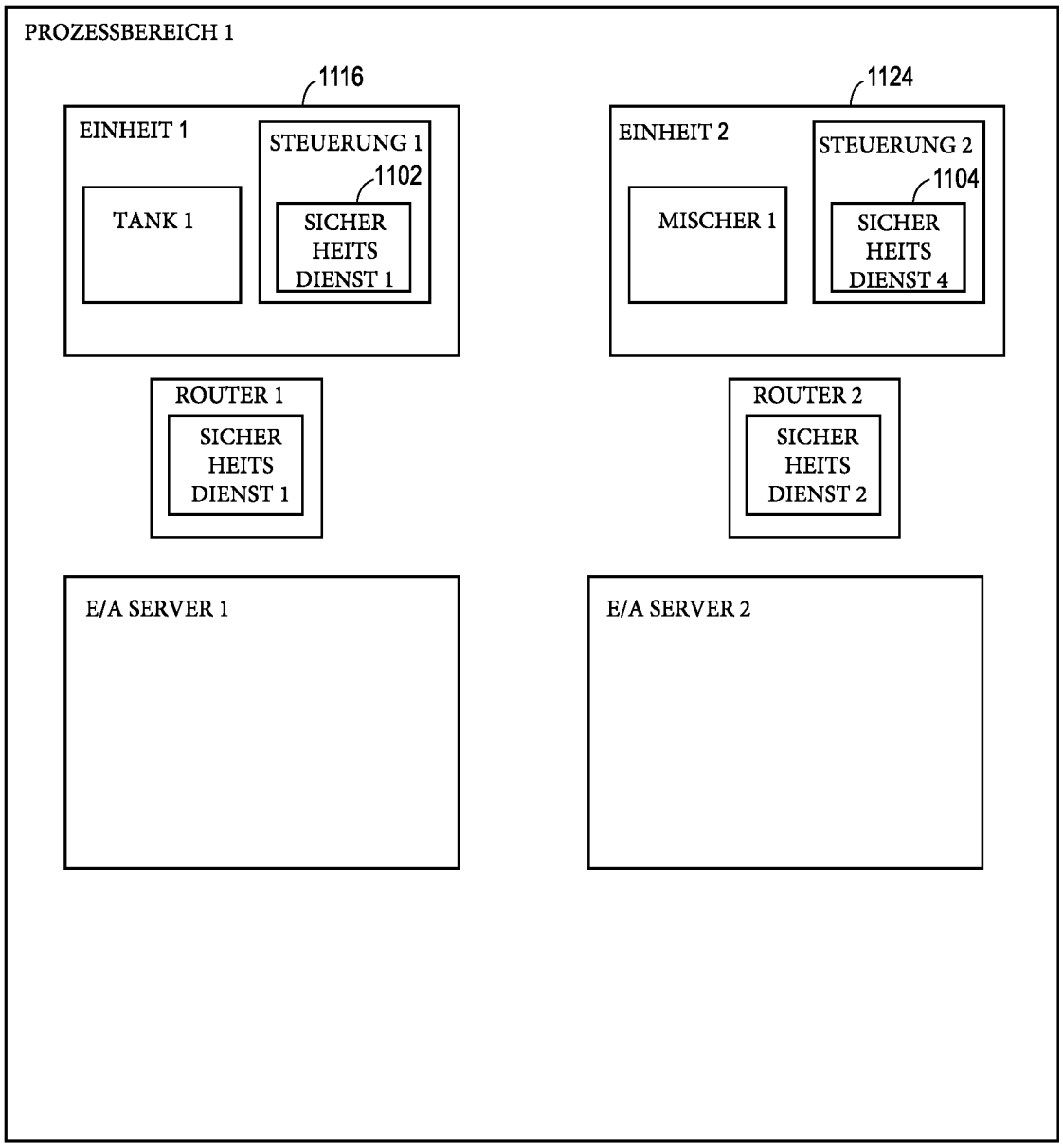

PROZESSBEREICH 1
1116
EINHEIT 1
STEUERUNG 1
1102
TANK 1
SICHER HEITS DIENST 1
1124
EINHEIT 2
STEUERUNG 2
1104
MISCHER 1
SICHER HEITS DIENST 4
ROUTER 1
SICHER HEITS DIENST 1
ROUTER 2
SICHER HEITS DIENST 2
E/A SERVER 1
E/A SERVER 2

FIG. 21

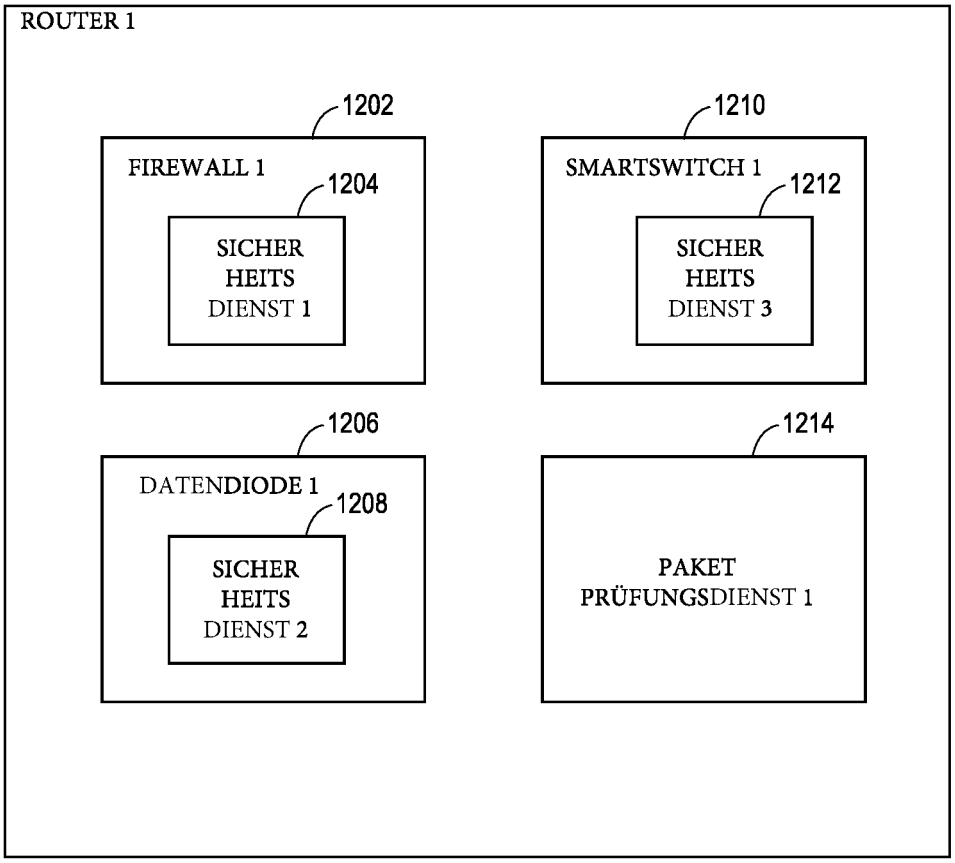

ROUTER 1
1202
FIREWALL 1
1204
SICHER HEITS DIENST 1
1210
SMARTSWITCH 1
1212
SICHER HEITS DIENST 3
1206
DATENDIODE 1
1208
SICHER HEITS DIENST 2
1214
PAKET PRÜFUNGSDIENST 1

FIG. 22

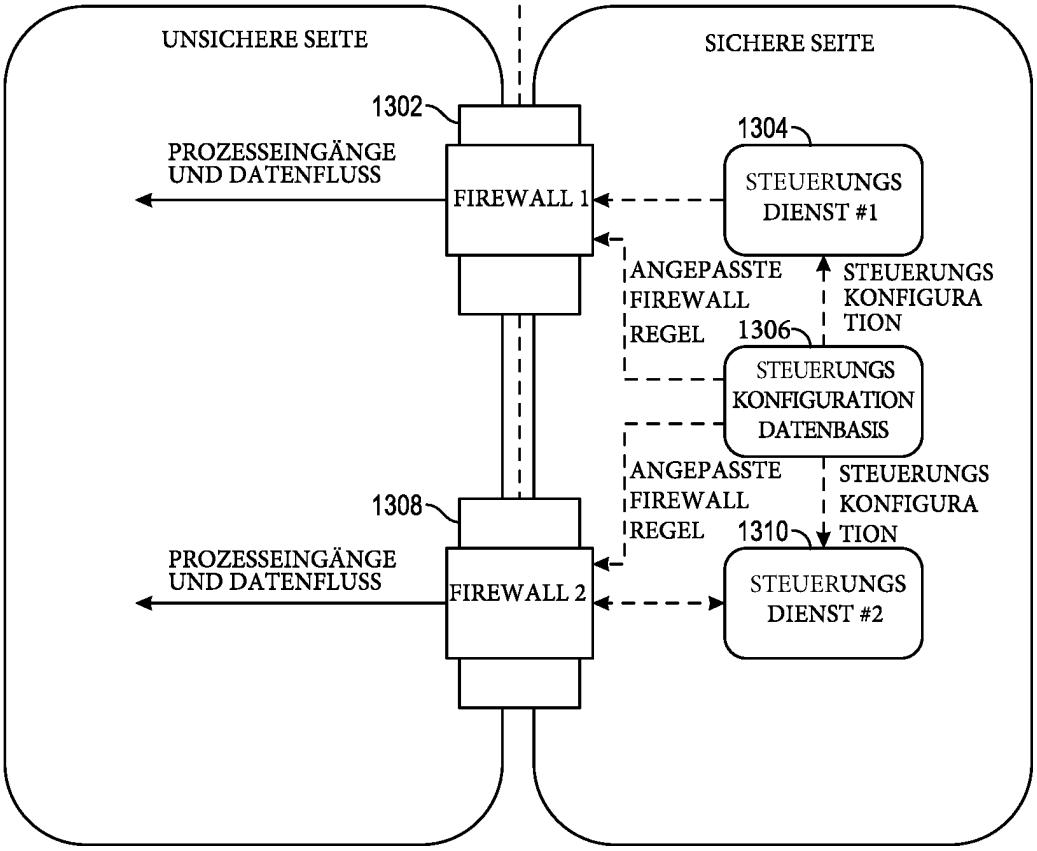

UNSICHERE SEITE
SICHERE SEITE
1302
1304
PROZESSEINGÄNGE UND DATENFLUSS
FIREWALL 1
STEUERUNGS DIENST #1
ANGEPASSTE FIREWALL REGEL
STEUERUNGS KONFIGURA TION
1306
STEUERUNGS KONFIGURATION DATENBASIS
1308
ANGEPASSTE FIREWALL REGEL
STEUERUNGS KONFIGURA TION
1310
PROZESSEINGÄNGE UND DATENFLUSS
FIREWALL 2
STEUERUNGS DIENST #2

FIG. 23

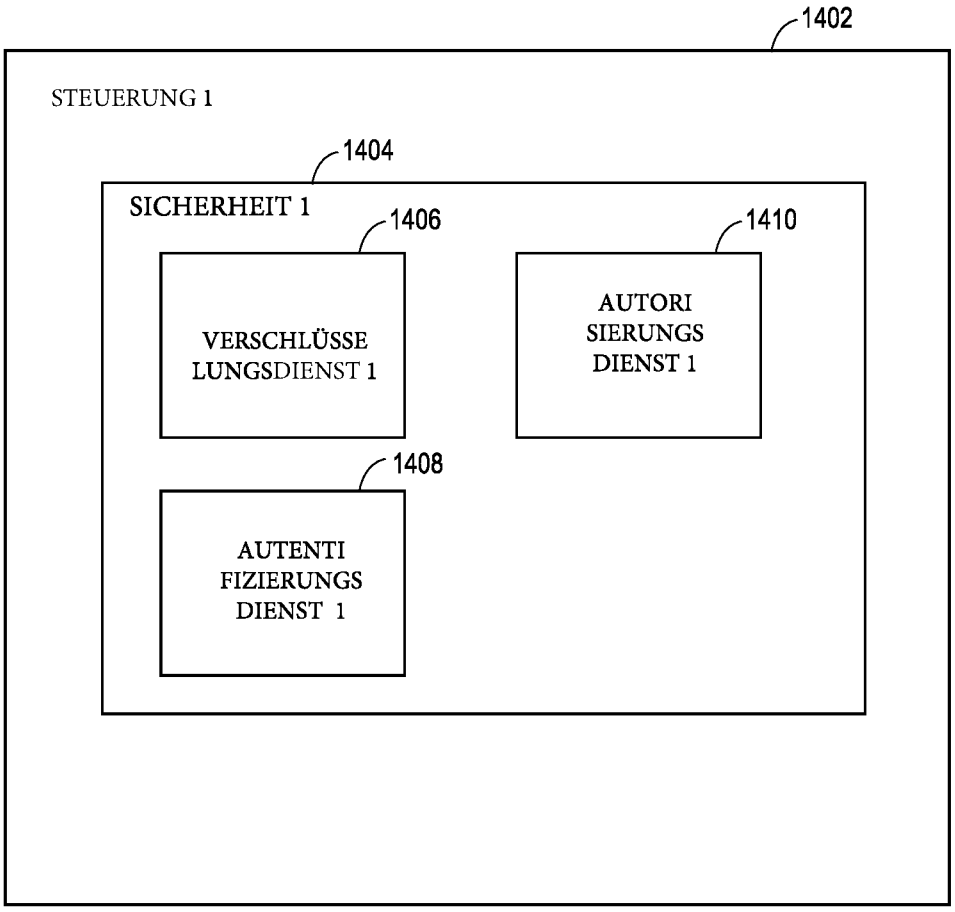

1402
STEUERUNG 1
1404
SICHERHEIT 1
1406
VERSCHLÜSSE LUNGSDIENST 1
1410
AUTORI SIERUNGS DIENST 1
1408
AUTENTI FIZIERUNGS DIENST 1

FIG. 24

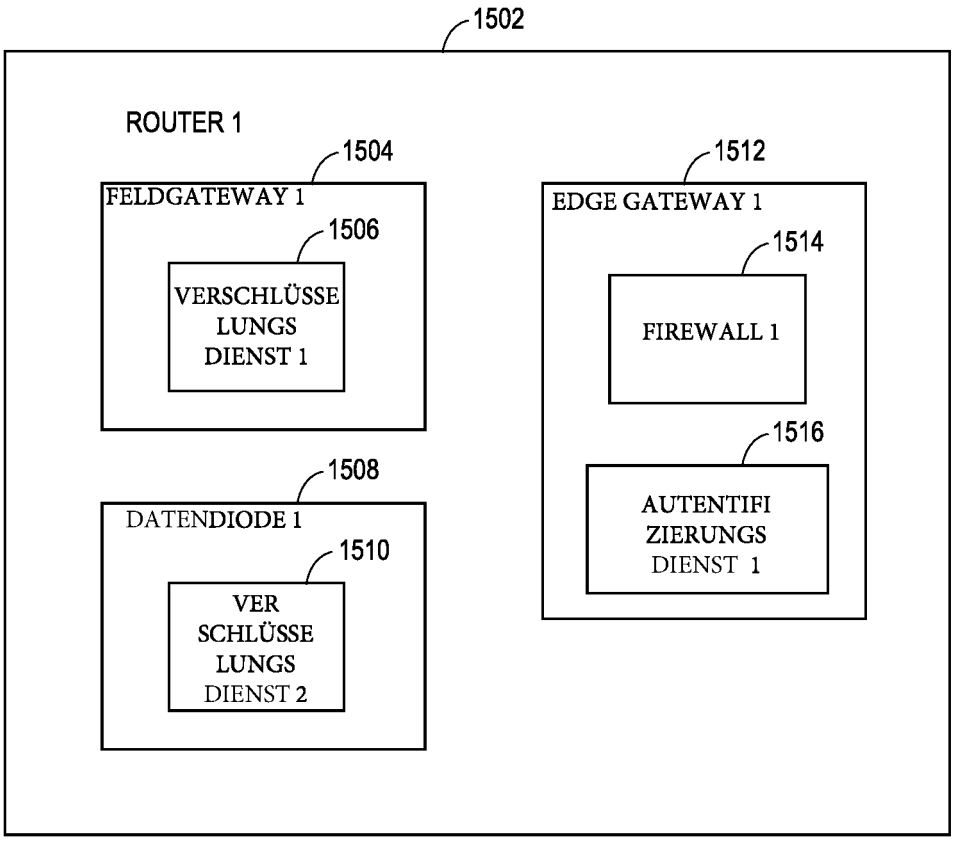

1502
ROUTER 1
1504
FELDGATEWAY 1
1506
VERSCHLÜSSE LUNGS DIENST 1
1508
DATENDIODE 1
1510
VER SCHLÜSSE LUNGS DIENST 2
1512
EDGE GATEWAY 1
1514
FIREWALL 1
1516
AUTENTIFI ZIERUNGS DIENST 1

FIG. 25

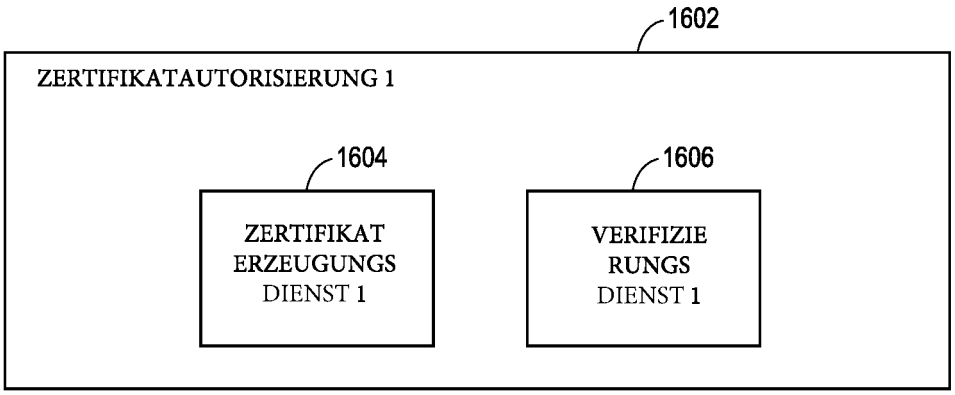

1602
ZERTIFIKATAUTORISIERUNG 1
1604
ZERTIFIKAT ERZEUGUNGS DIENST 1
1606
VERIFIZIE RUNGS DIENST 1

FIG. 26

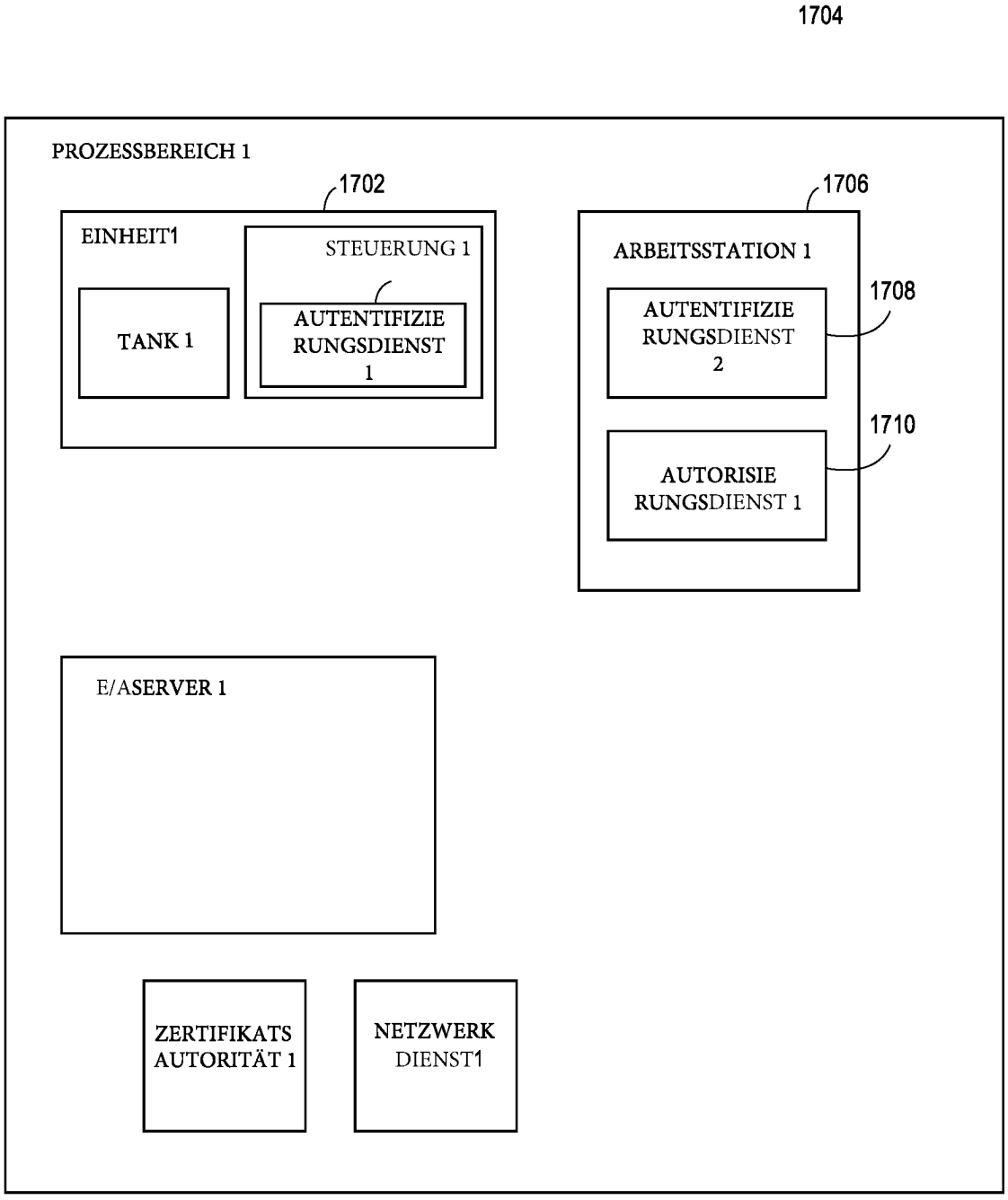

1704
PROZESSBEREICH 1
1702
EINHEIT1
STEUERUNG 1
TANK 1
AUTENTIFIZIE RUNGSDIENST 1
1706
ARBEITSSTATION 1
1708
AUTENTIFIZIE RUNGSDIENST 2
1710
AUTORISIE RUNGSDIENST 1
E/ASERVER 1
ZERTIFIKATS AUTORITÄT 1
NETZWERK DIENST1

FIG. 27

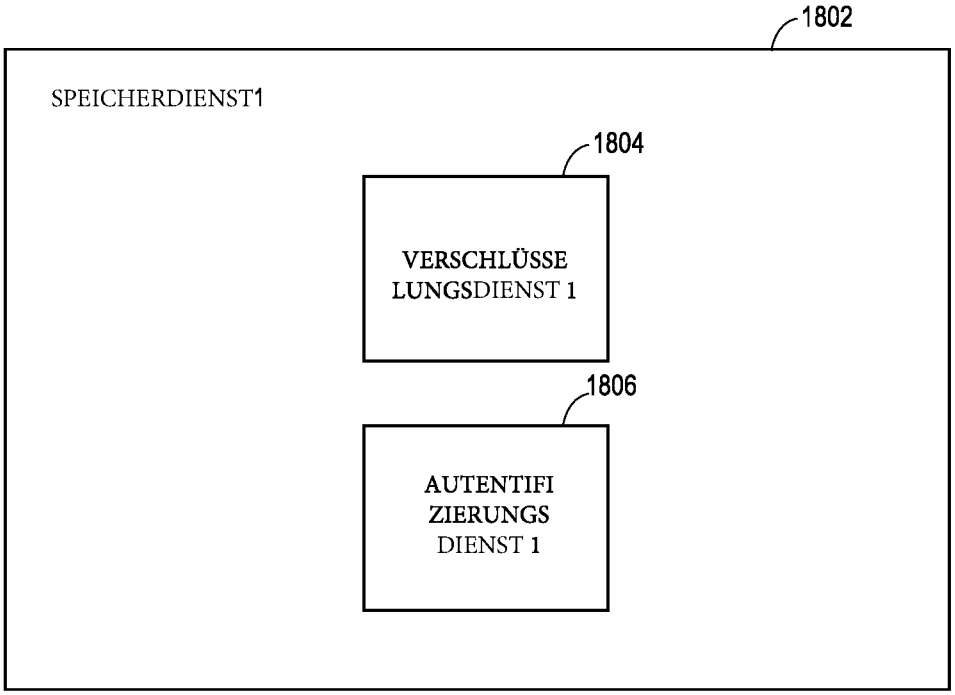

1802
SPEICHERDIENST1
1804
VERSCHLÜSSE LUNGSDIENST 1
1806
AUTENTIFI ZIERUNGS DIENST 1

FIG. 28

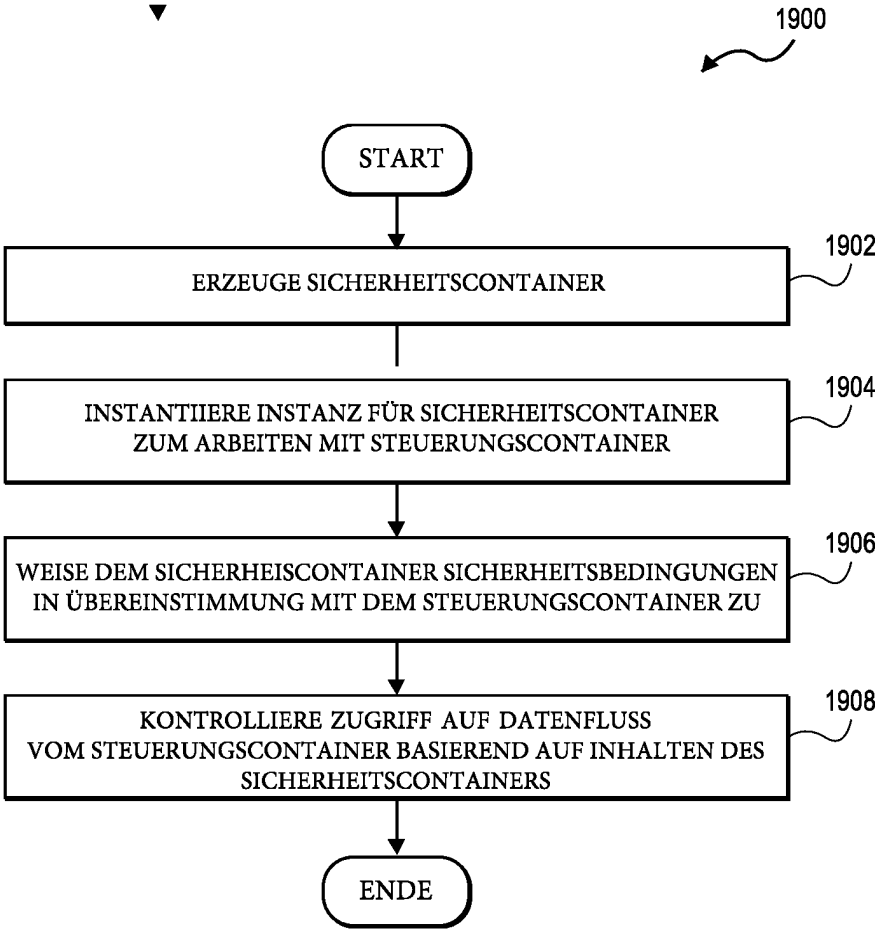

1900
START
ERZEUGE SICHERHEITSCONTAINER
1902
INSTANTIIERE INSTANZ FÜR SICHERHEITSCONTAINER ZUM ARBEITEN MIT STEUERUNGSCONTAINER
1904
WEISE DEM SICHERHEISCONTAINER SICHERHEITSBEDINGUNGEN IN ÜBEREINSTIMMUNG MIT DEM STEUERUNGSCONTAINER ZU
1906
KONTROLLIERE ZUGRIFF AUF DATENFLUSS VOM STEUERUNGSCONTAINER BASIEREND AUF INHALTEN DES SICHERHEITSCONTAINERS
1908
ENDE

FIG. 29

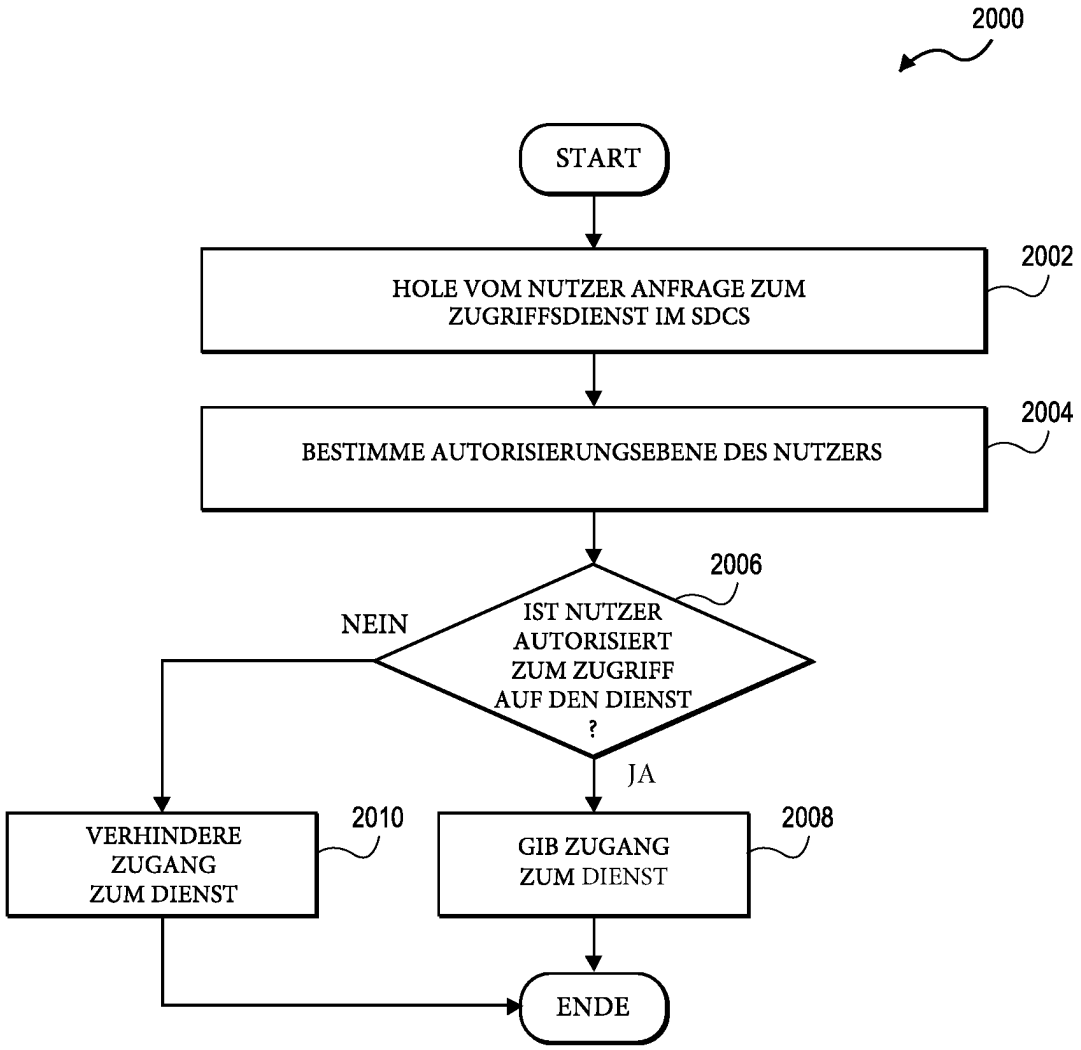

2000
START
HOLE VOM NUTZER ANFRAGE ZUM ZUGRIFFSDIENST IM SDCS
2002
BESTIMME AUTORISIERUNGSEBENE DES NUTZERS
2004
2006
IST NUTZER AUTORISIERT ZUM ZUGRIFF AUF DEN DIENST ?
NEIN
JA
VERHINDERE ZUGANG ZUM DIENST
2010
GIB ZUGANG ZUM DIENST
2008
ENDE

FIG. 30

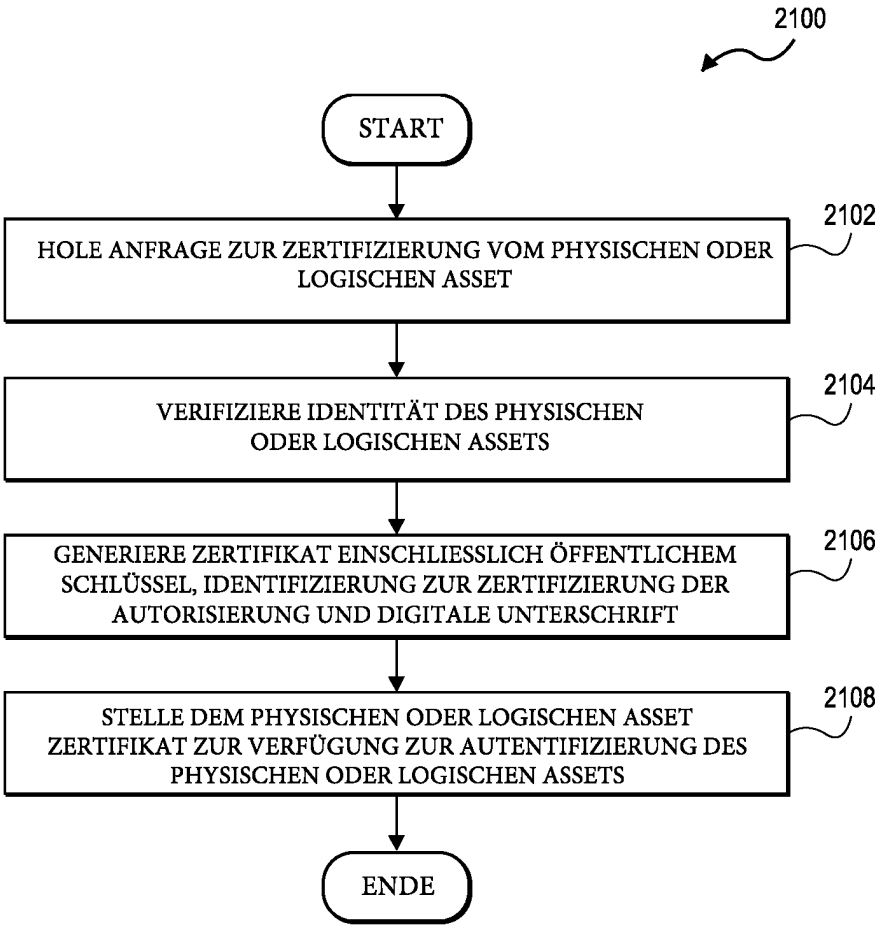

2100
START
HOLE ANFRAGE ZUR ZERTIFIZIERUNG VOM PHYSISCHEN ODER LOGISCHEN ASSET
2102
VERIFIZIERE IDENTITÄT DES PHYSISCHEN ODER LOGISCHEN ASSETS
2104
GENERIERE ZERTIFIKAT EINSCHLIESSLICH ÖFFENTLICHEM SCHLÜSSEL, IDENTIFIZIERUNG ZUR ZERTIFIZIERUNG DER AUTORISIERUNG UND DIGITALE UNTERSCHRIFT
2106
STELLE DEM PHYSISCHEN ODER LOGISCHEN ASSET ZERTIFIKAT ZUR VERFÜGUNG ZUR AUTENTIFIZIERUNG DES PHYSISCHEN ODER LOGISCHEN ASSETS
2108
ENDE

FIG. 31

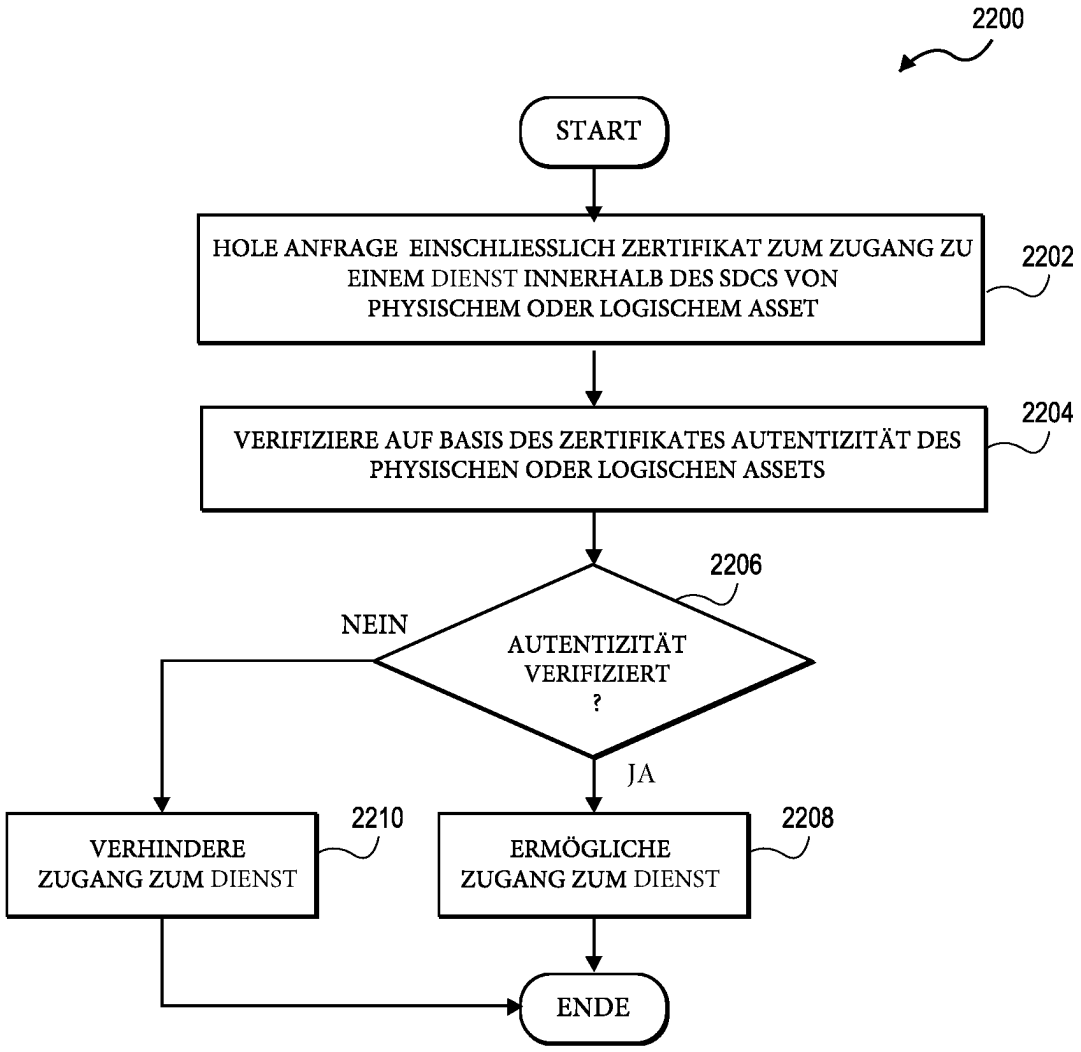

2200
START
HOLE ANFRAGE EINSCHLIESSLICH ZERTIFIKAT ZUM ZUGANG ZU EINEM DIENST INNERHALB DES SDCS VON PHYSISCHEM ODER LOGISCHEM ASSET
2202
VERIFIZIERE AUF BASIS DES ZERTIFIKATES AUTENTIZITÄT DES PHYSISCHEN ODER LOGISCHEN ASSETS
2204
2206
AUTENTIZITÄT VERIFIZIERT ?
NEIN
JA
VERHINDERE ZUGANG ZUM DIENST
2210
ERMÖGLICHE ZUGANG ZUM DIENST
2208
ENDE

FIG. 32

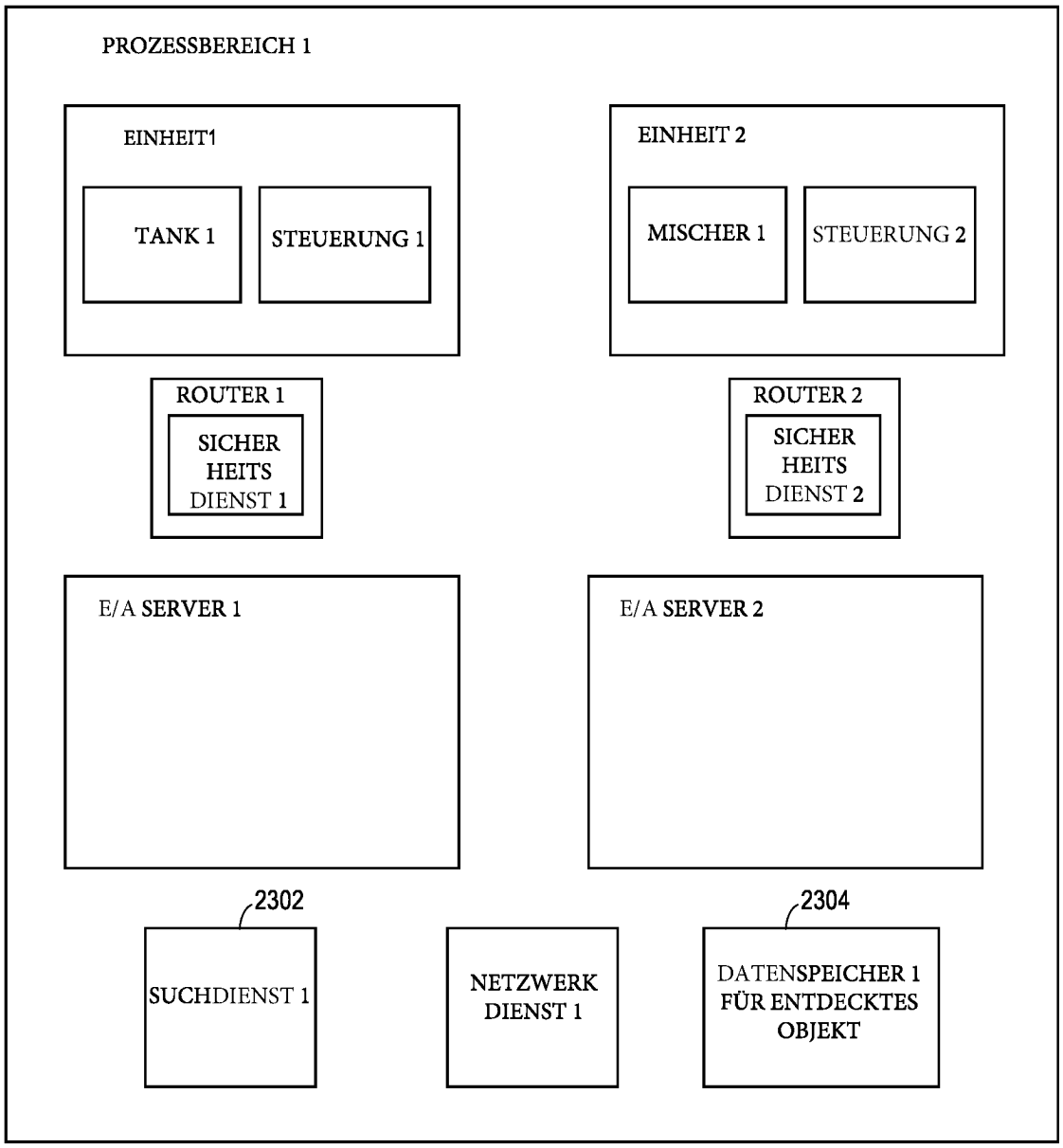

PROZESSBEREICH 1
EINHEIT1
TANK 1
STEUERUNG 1
EINHEIT 2
MISCHER 1
STEUERUNG 2
ROUTER 1
SICHER HEITS DIENST 1
ROUTER 2
SICHER HEITS DIENST 2
E/A SERVER 1
E/A SERVER 2
2302
SUCHDIENST 1
NETZWERK DIENST 1
2304
DATENSPEICHER 1 FÜR ENTDECKTES OBJEKT

FIG. 33

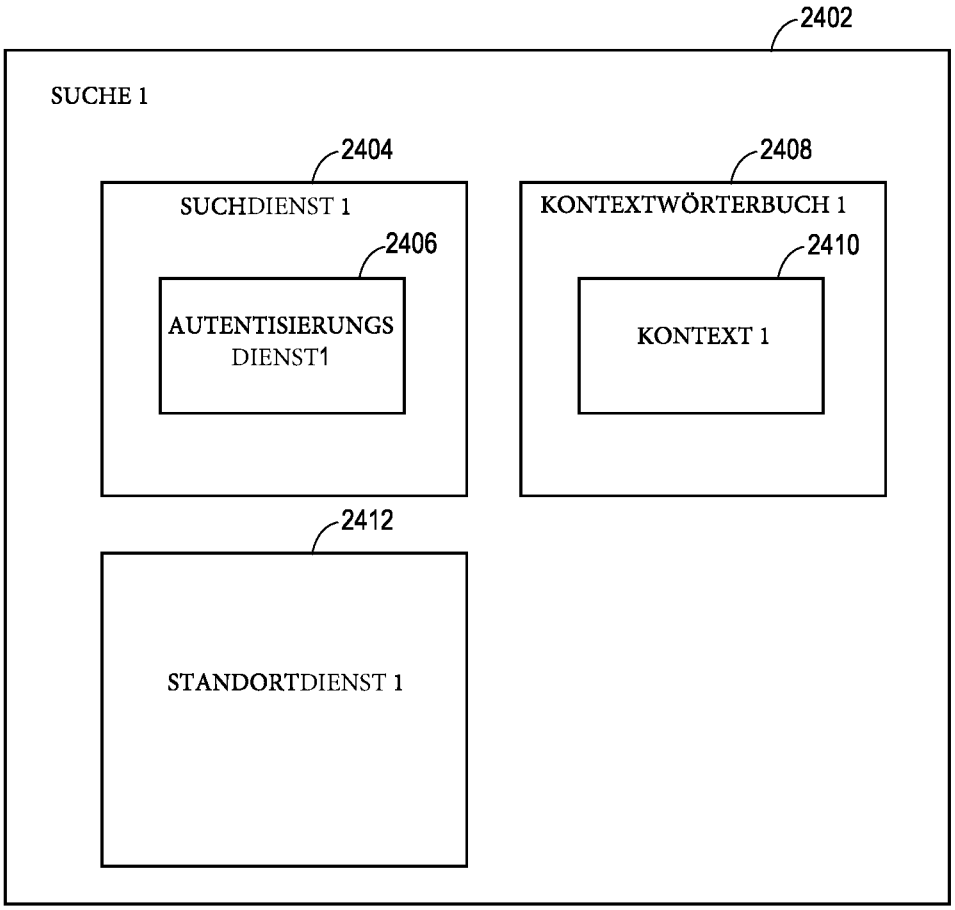

2402
SUCHE 1
2404
SUCHDIENST 1
2406
AUTENTISIERUNGS DIENST1
2408
KONTEXTWÖRTERBUCH 1
2410
KONTEXT 1
2412
STANDORTDIENST 1

FIG. 34

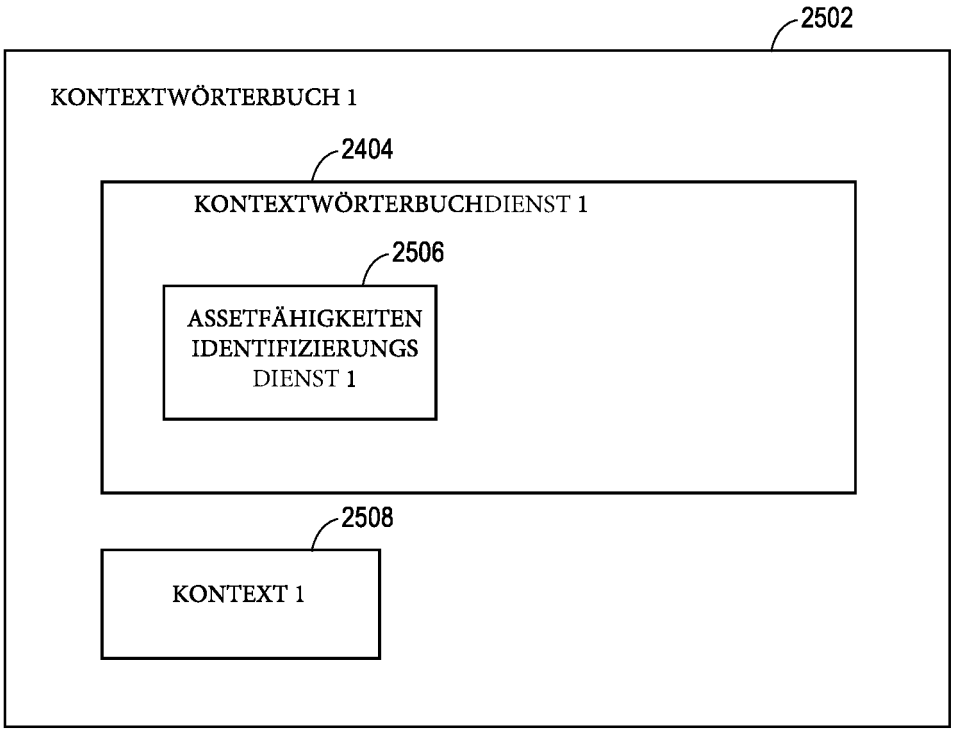

2502
KONTEXTWÖRTERBUCH 1
2404
KONTEXTWÖRTERBUCHDIENST 1
2506
ASSETFÄHIGKEITEN IDENTIFIZIERUNGS DIENST 1
2508
KONTEXT 1

FIG. 35

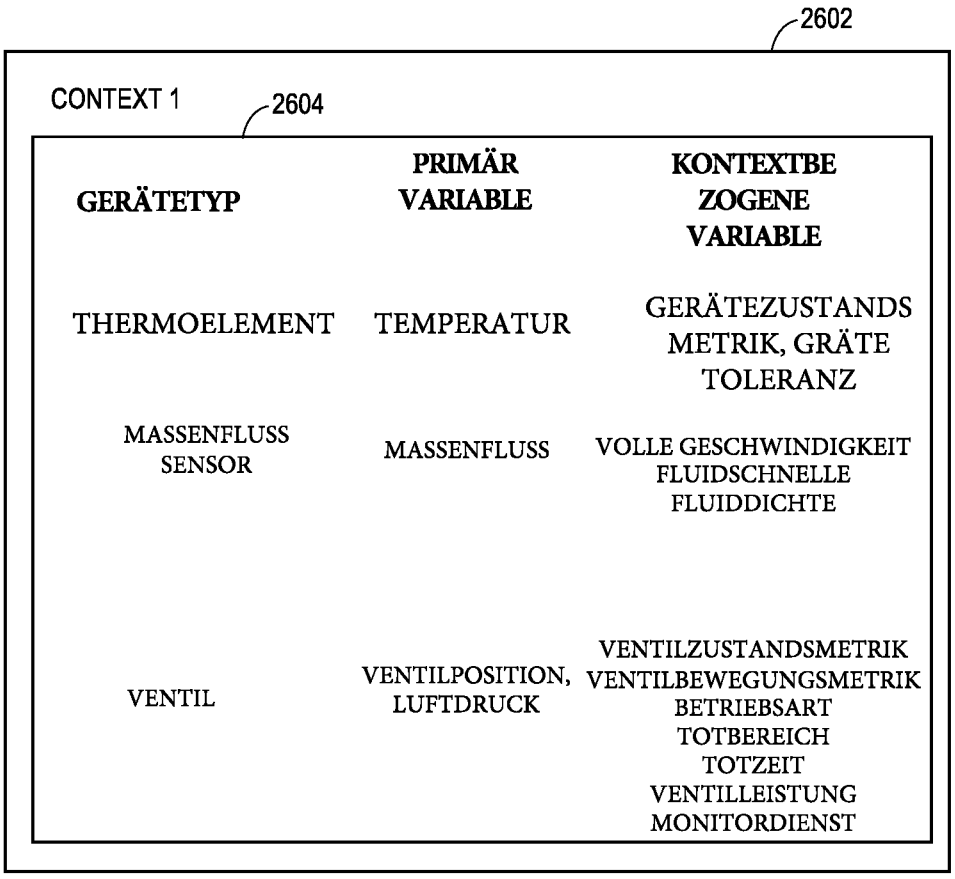

2602
CONTEXT 1
2604
GERÄTETYP
PRIMÄR VARIABLE
KONTEXTBEZOGENE VARIABLE
THERMOELEMENT
TEMPERATUR
GERÄTEZUSTANDSMETRIK, GRÄTE TOLERANZ
MASSENFLUSS SENSOR
MASSENFLUSS
VOLLE GESCHWINDIGKEIT
FLUIDSCHNELLE
FLUIDDICHTE
VENTIL
VENTILPOSITION, LUFTDRUCK
VENTILZUSTANDSMETRIK
VENTILBEWEGUNGSMETRIK
BETRIEBSART
TOTBEREICH
TOTZEIT
VENTILLEISTUNG
MONITORDIENST

FIG. 36

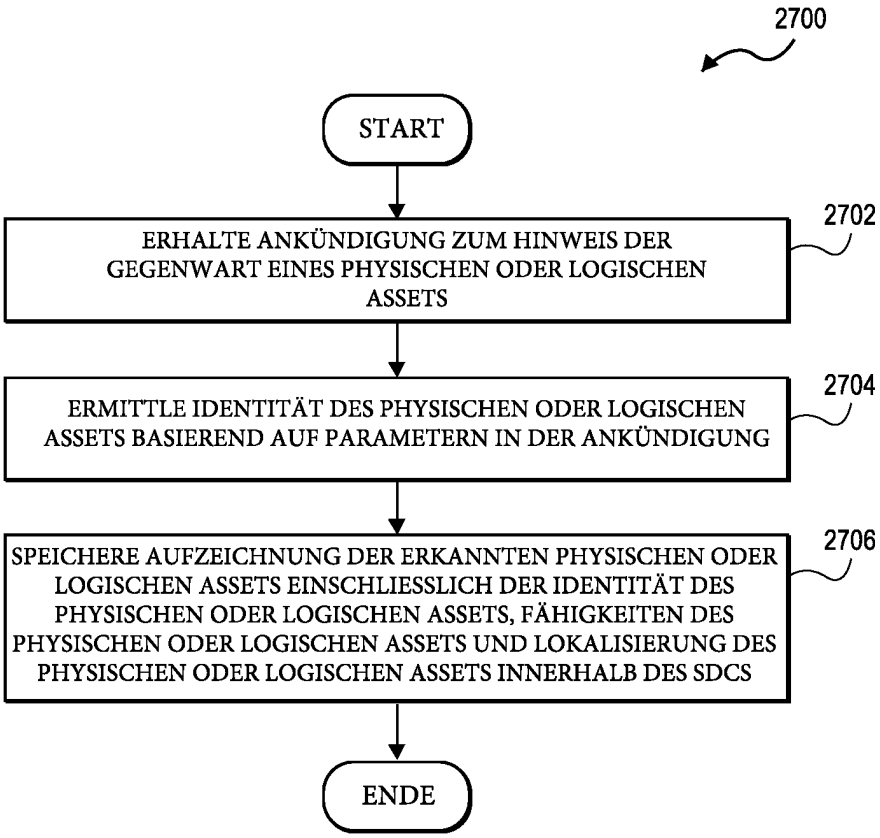

2700
START
ERHALTE ANKÜNDIGUNG ZUM HINWEIS DER GEGENWART EINES PHYSISCHEN ODER LOGISCHEN ASSETS
2702
ERMITTLE IDENTITÄT DES PHYSISCHEN ODER LOGISCHEN ASSETS BASIEREND AUF PARAMETERN IN DER ANKÜNDIGUNG
2704
SPEICHERE AUFZEICHNUNG DER ERKANNTEN PHYSISCHEN ODER LOGISCHEN ASSETS EINSCHLIESSLICH DER IDENTITÄT DES PHYSISCHEN ODER LOGISCHEN ASSETS, FÄHIGKEITEN DES PHYSISCHEN ODER LOGISCHEN ASSETS UND LOKALISIERUNG DES PHYSISCHEN ODER LOGISCHEN ASSETS INNERHALB DES SDCS
2706
ENDE

FIG. 37

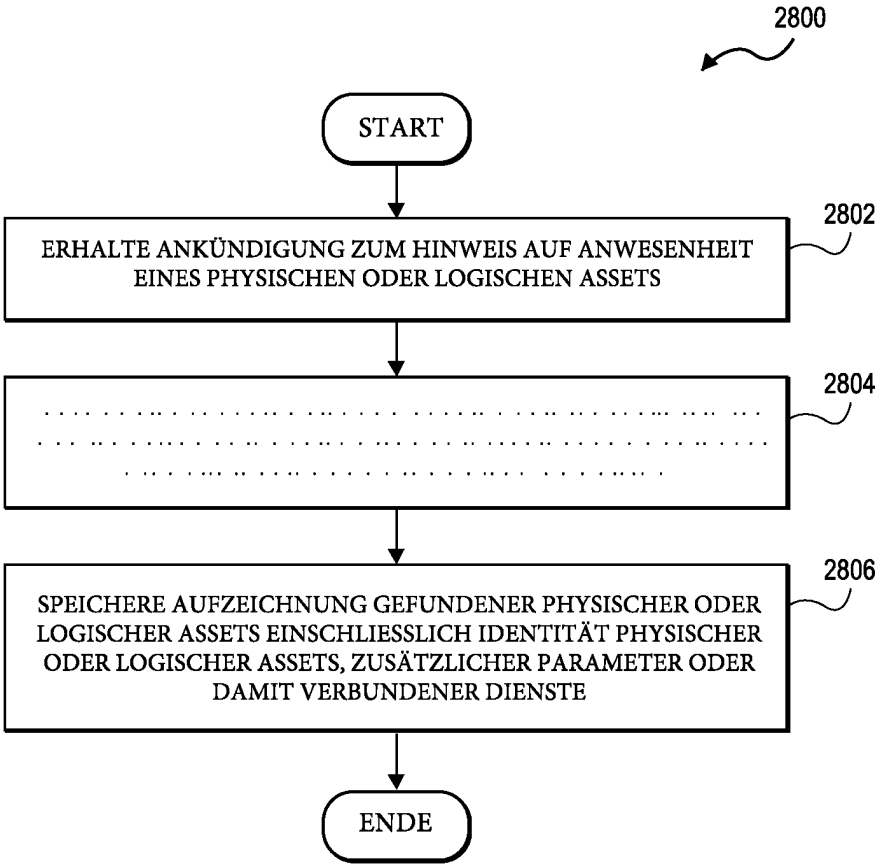

2800
START
ERHALTE ANKÜNDIGUNG ZUM HINWEIS AUF ANWESENHEIT EINES PHYSISCHEN ODER LOGISCHEN ASSETS
2802
2804
SPEICHERE AUFZEICHNUNG GEFUNDENER PHYSISCHER ODER LOGISCHER ASSETS EINSCHLIESSLICH IDENTITÄT PHYSISCHER ODER LOGISCHER ASSETS, ZUSÄTZLICHER PARAMETER ODER DAMIT VERBUNDENER DIENSTE
2806
ENDE

FIG. 38

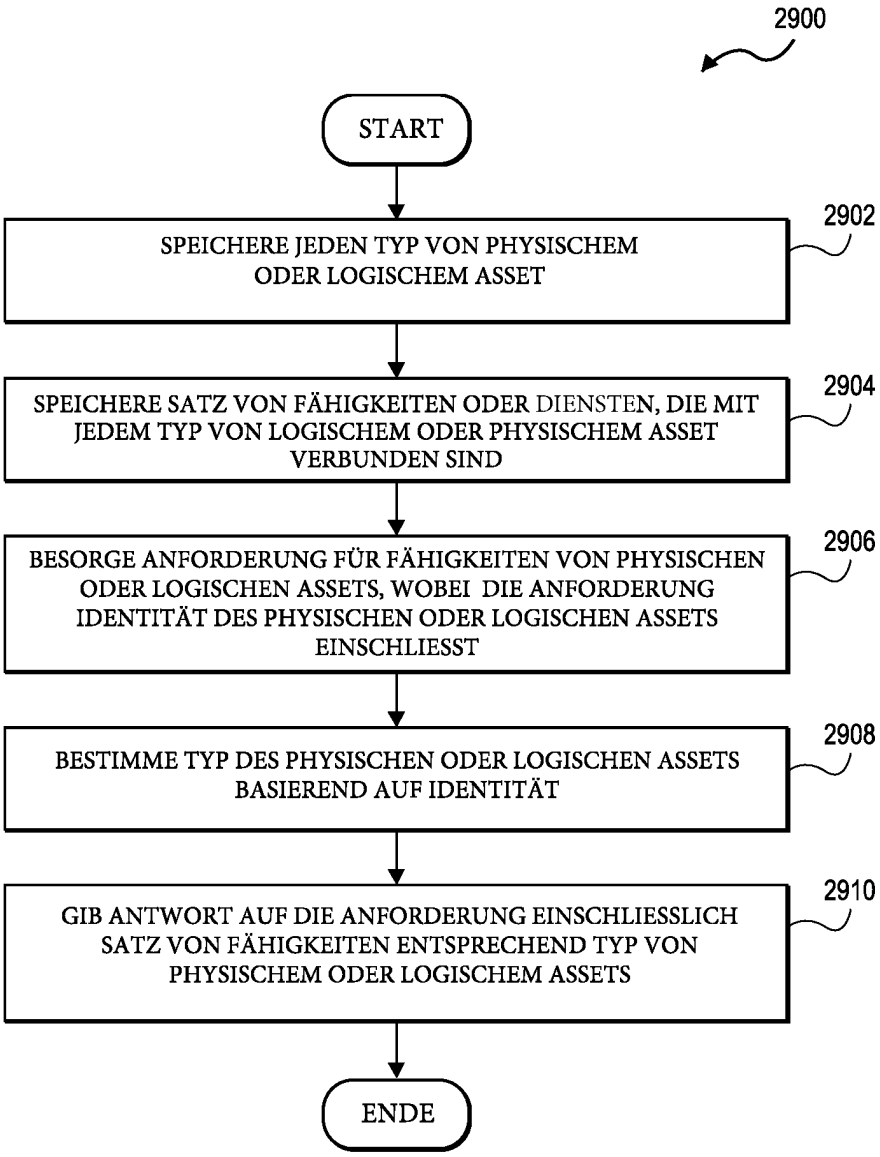

2900
START
SPEICHERE JEDEN TYP VON PHYSISCHEM ODER LOGISCHEM ASSET
2902
SPEICHERE SATZ VON FÄHIGKEITEN ODER DIENSTEN, DIE MIT JEDEM TYP VON LOGISCHEM ODER PHYSISCHEM ASSET VERBUNDEN SIND
2904
BESORGE ANFORDERUNG FÜR FÄHIGKEITEN VON PHYSISCHEN ODER LOGISCHEN ASSETS, WOBEI DIE ANFORDERUNG IDENTITÄT DES PHYSISCHEN ODER LOGISCHEN ASSETS EINSCHLIESST
2906
BESTIMME TYP DES PHYSISCHEN ODER LOGISCHEN ASSETS BASIEREND AUF IDENTITÄT
2908
GIB ANTWORT AUF DIE ANFORDERUNG EINSCHLIESSLICH SATZ VON FÄHIGKEITEN ENTSPRECHEND TYP VON PHYSISCHEM ODER LOGISCHEM ASSETS
2910
ENDE

FIG. 39

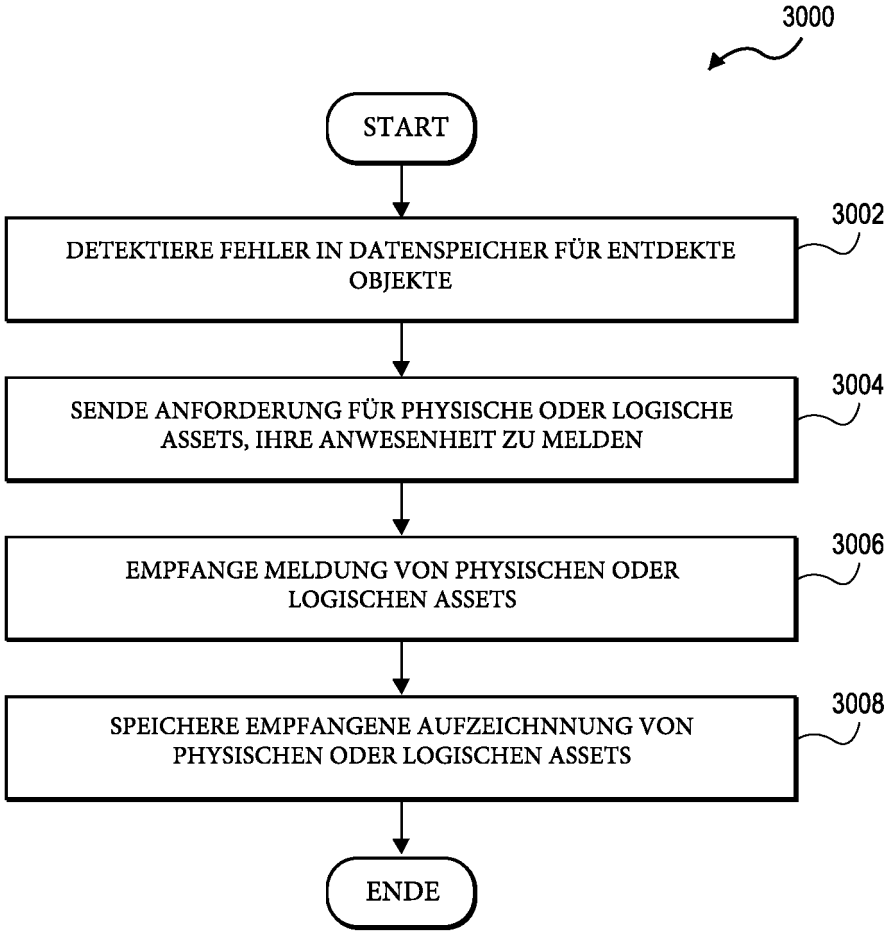

3000
START
DETEKTIERE FEHLER IN DATENSPEICHER FÜR ENTDEKTE OBJEKTE
3002
SENDE ANFORDERUNG FÜR PHYSISCHE ODER LOGISCHE ASSETS, IHRE ANWESENHEIT ZU MELDEN
3004
EMPFANGE MELDUNG VON PHYSISCHEN ODER LOGISCHEN ASSETS
3006
SPEICHERE EMPFANGENE AUFZEICHNNUNG VON PHYSISCHEN ODER LOGISCHEN ASSETS
3008
ENDE

FIG. 40

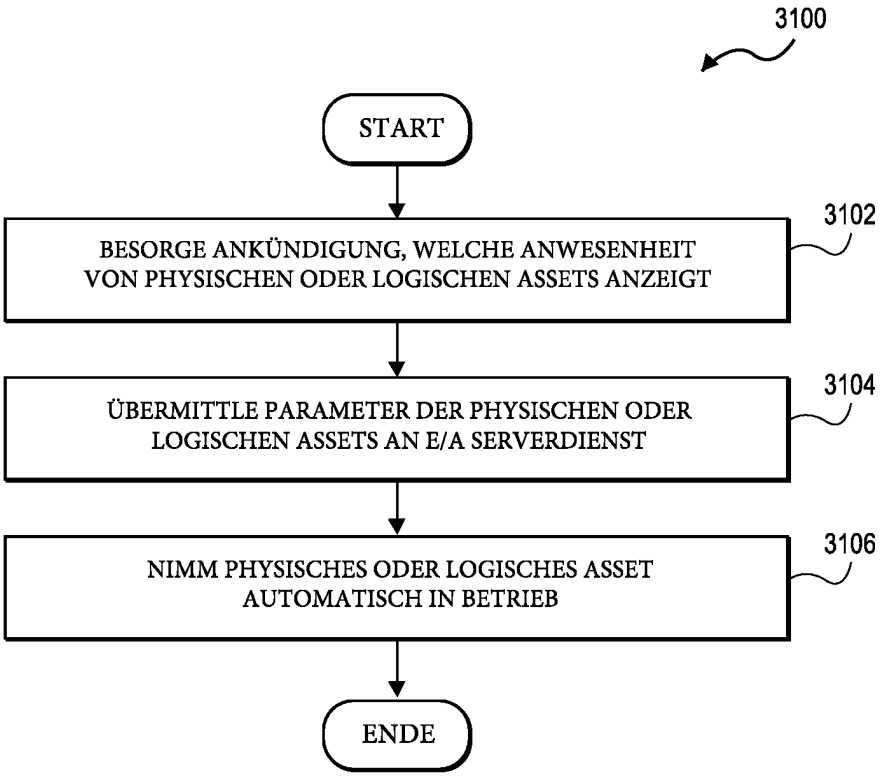

3100
START
BESORGE ANKÜNDIGUNG, WELCHE ANWESENHEIT VON PHYSISCHEN ODER LOGISCHEN ASSETS ANZEIGT
3102
ÜBERMITTLE PARAMETER DER PHYSISCHEN ODER LOGISCHEN ASSETS AN E/A SERVERDIENST
3104
NIMM PHYSISCHES ODER LOGISCHES ASSET AUTOMATISCH IN BETRIEB
3106
ENDE

FIG. 41

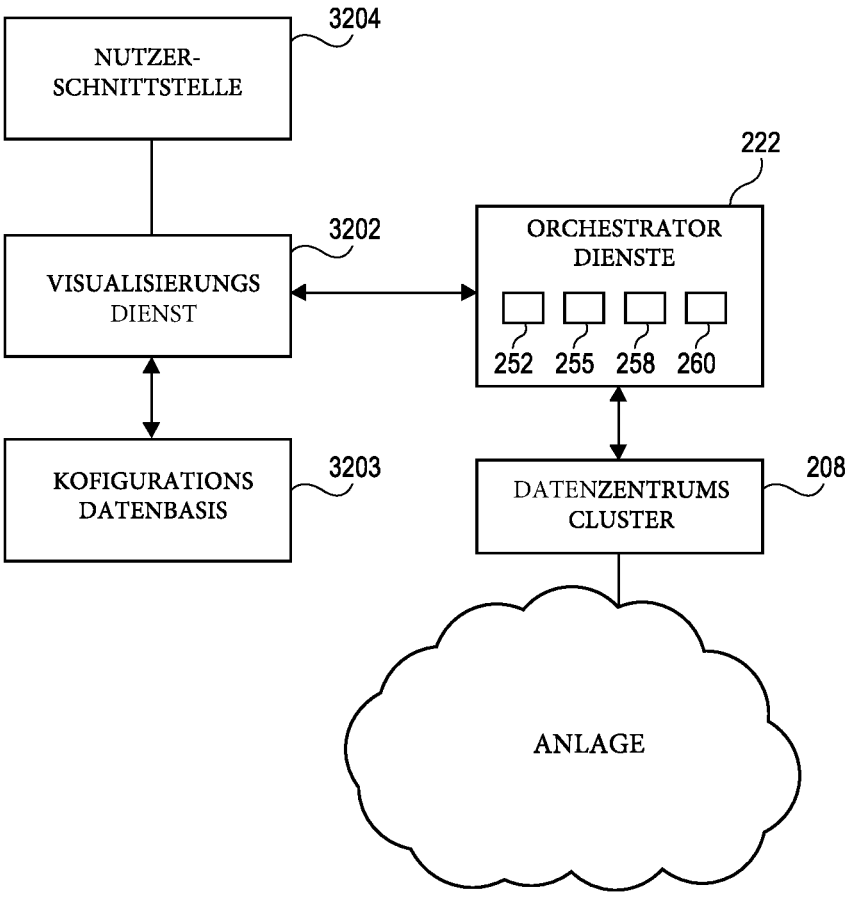

3204
NUTZER-
SCHNITTSTELLE
222
3202
VISUALISIERUNGS
DIENST
ORCHESTRATOR
DIENSTE
252
255
258
260
KOFIGURATIONS
DATENBASIS
3203
DATENZENTRUMS
CLUSTER
208
ANLAGE

FIG. 42

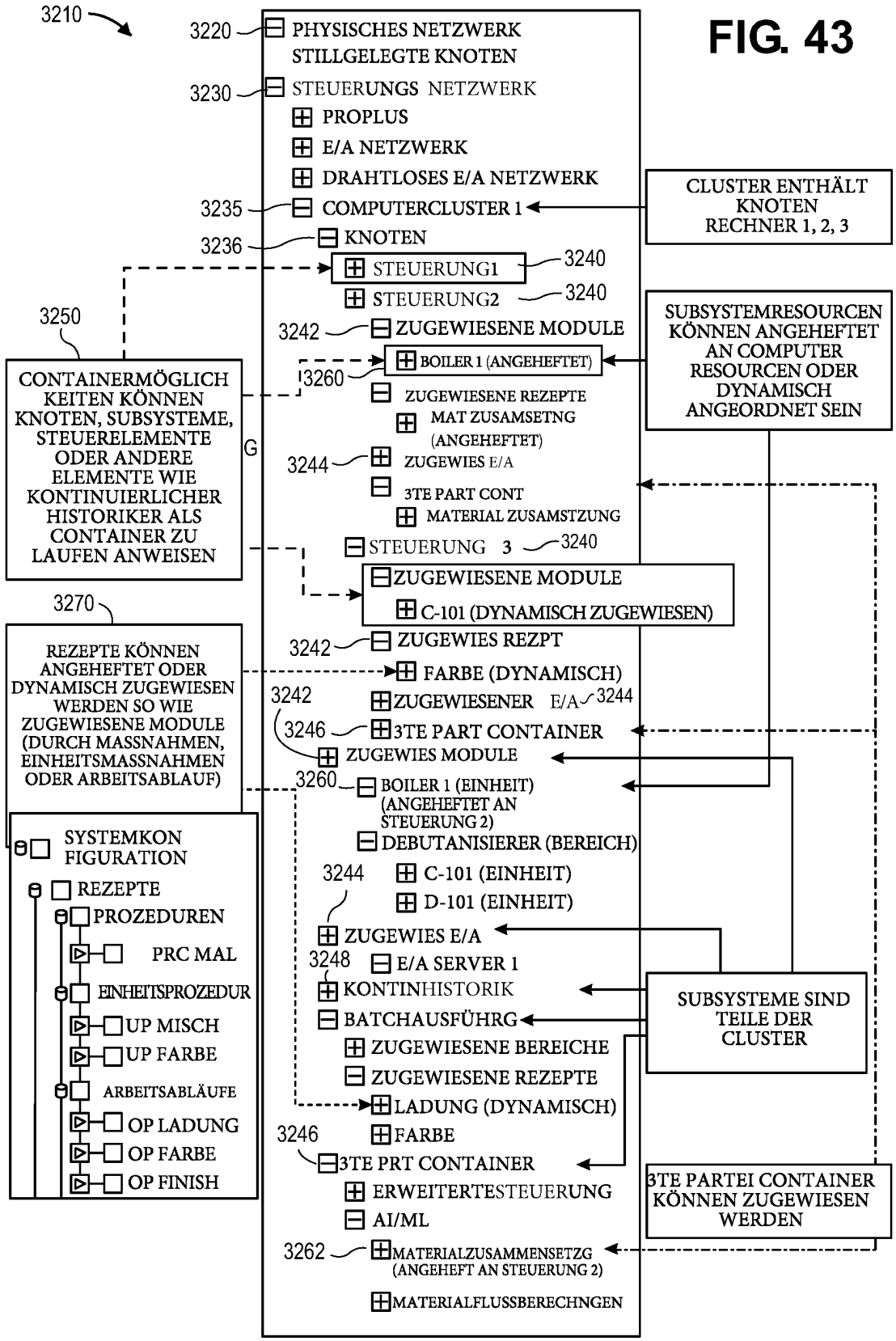

3210
3220
PHYSISCHES NETZWERK
STILLGELEGTE KNOTEN
3230
STEUERUNGS NETZWERK
PROPLUS
E/A NETZWERK
DRAHTLOSES E/A NETZWERK
3235
COMPUTERCLUSTER 1
CLUSTER ENTHÄLT KNOTEN RECHNER 1, 2, 3
3236
KNOTEN
STEUERUNG1
3240
STEUERUNG2
3240
3250
3242
ZUGEWIESENE MODULE
BOILER 1 (ANGEHEFTET)
SUBSYSTEMRESOURCEN KÖNNEN ANGEHEFTET AN COMPUTER RESOURCEN ODER DYNAMISCH ANGEORDNET SEIN
3260
ZUGEWIESENE REZEPTE
MAT ZUSAMSETNG (ANGEHEFTET)
CONTAINERMÖGLICHKEITEN KÖNNEN KNOTEN, SUBSYSTEME, STEUERELEMENTE ODER ANDERE ELEMENTE WIE KONTINUIERLICHER HISTORIKER ALS CONTAINER ZU LAUFEN ANWEISEN
3244
ZUGEWIES E/A
3TE PART CONT
MATERIAL ZUSAMSTZUNG
STEUERUNG 3
3240
ZUGEWIESENE MODULE
C-101 (DYNAMISCH ZUGEWIESEN)
3270
3242
ZUGEWIES REZPT
REZEPTE KÖNNEN ANGEHEFTET ODER DYNAMISCH ZUGEWIESEN WERDEN SO WIE ZUGEWIESENE MODULE (DURCH MASSNAHMEN, EINHEITSMASSNAHMEN ODER ARBEITSABLAUF)
FARBE (DYNAMISCH)
3242
ZUGEWIESENER E/A
3244
3246
3TE PART CONTAINER
ZUGEWIES MODULE
3260
BOILER 1 (EINHEIT) (ANGEHEFTET AN STEUERUNG 2)
DEBUTANISIERER (BEREICH)
3244
C-101 (EINHEIT)
D-101 (EINHEIT)
ZUGEWIES E/A
SYSTEMKONFIGURATION
REZEPTE
PROZEDUREN
PRC MAL
EINHEITSPROZEDUR
UP MISCH
UP FARBE
ARBEITSABLÄUFE
OP LADUNG
OP FARBE
OP FINISH
3248
E/A SERVER 1
KONTINHISTORIK
BATCHAUSFÜHRG
SUBSYSTEME SIND TEILE DER CLUSTER
ZUGEWIESENE BEREICHE
ZUGEWIESENE REZEPTE
LADUNG (DYNAMISCH)
3246
FARBE
3TE PRT CONTAINER
3TE PARTEI CONTAINER KÖNNEN ZUGEWIESEN WERDEN
ERWEITERTESTEUERUNG
AI/ML
3262
MATERIALZUSAMMENSETZG (ANGEHEFT AN STEUERUNG 2)
MATERIALFLUSSBERECHNGEN

FIG. 43

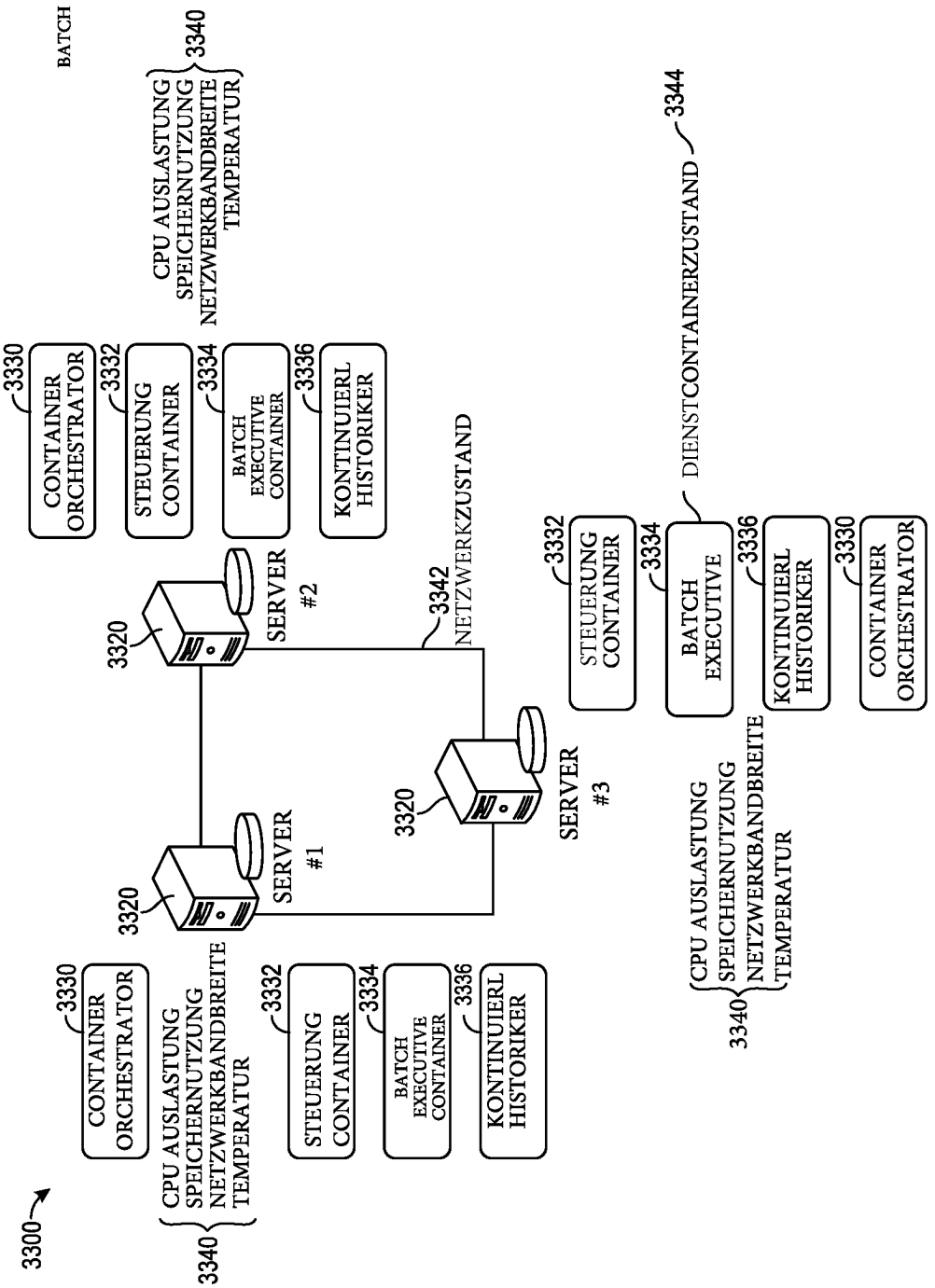

3300
BATCH
3340
CPU AUSLASTUNG
SPEICHERNUTZUNG
NETZWERKBANDBREITE
TEMPERATUR
3330
CONTAINER ORCHESTRATOR
3332
STEUERUNG CONTAINER
3334
BATCH EXECUTIVE CONTAINER
3336
KONTINUIERL HISTORIKER
3320
SERVER #1
SERVER #2
SERVER #3
3342
NETZWERKZUSTAND
DIENSTCONTAINERZUSTAND
3344

FIG. 44

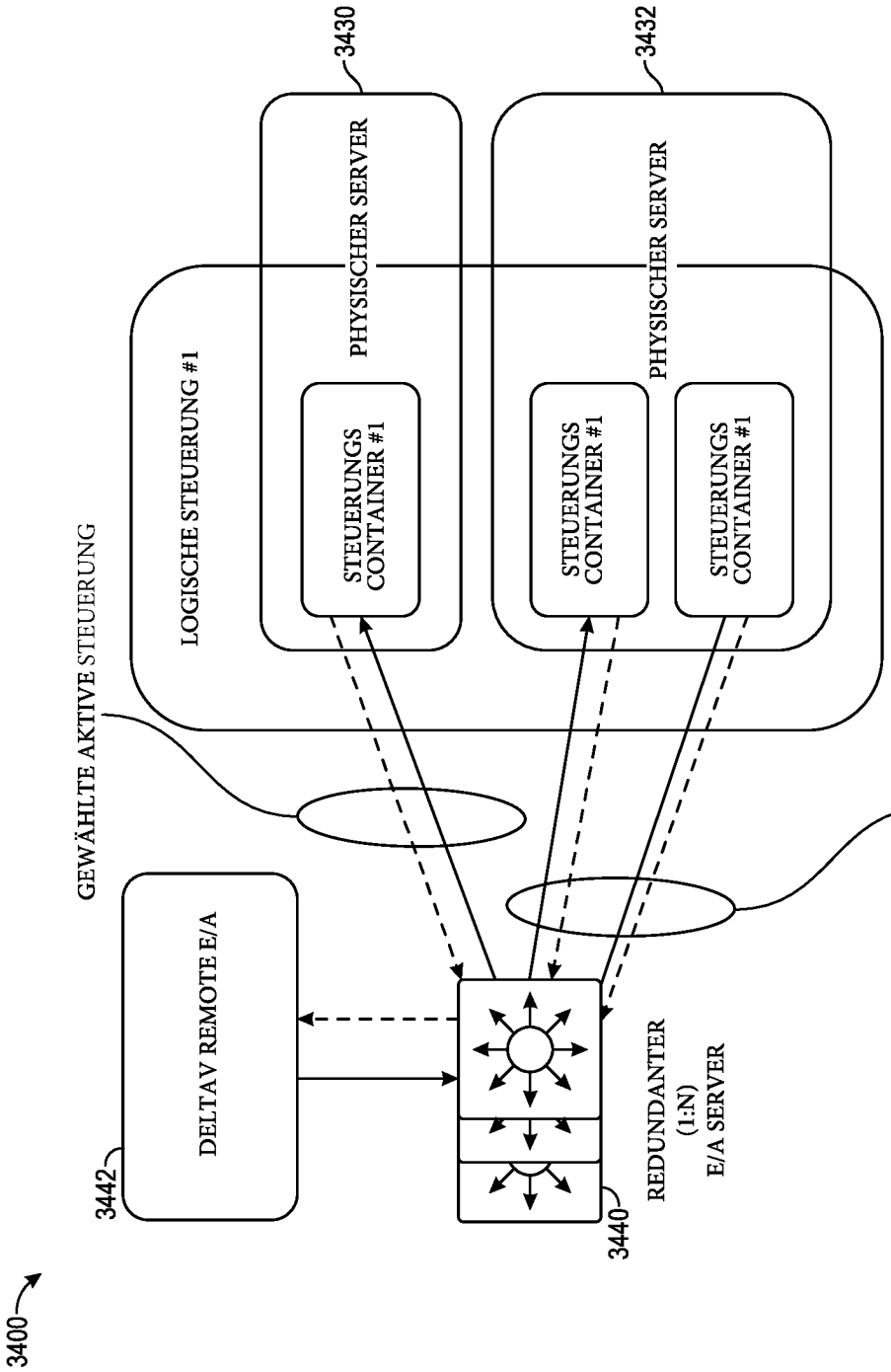

3400
3442
DELTAV REMOTE E/A
3440
REDUNDANTER (1:N) E/A SERVER
GEWÄHLTE AKTIVE STEUERUNG
EINGÄNGE AUFNEHMEN
LOGISCHE STEUERUNG #1
3430
PHYSISCHER SERVER
STEUERUNGS CONTAINER #1
3432
PHYSISCHER SERVER
STEUERUNGS CONTAINER #1
STEUERUNGS CONTAINER #1

FIG. 45

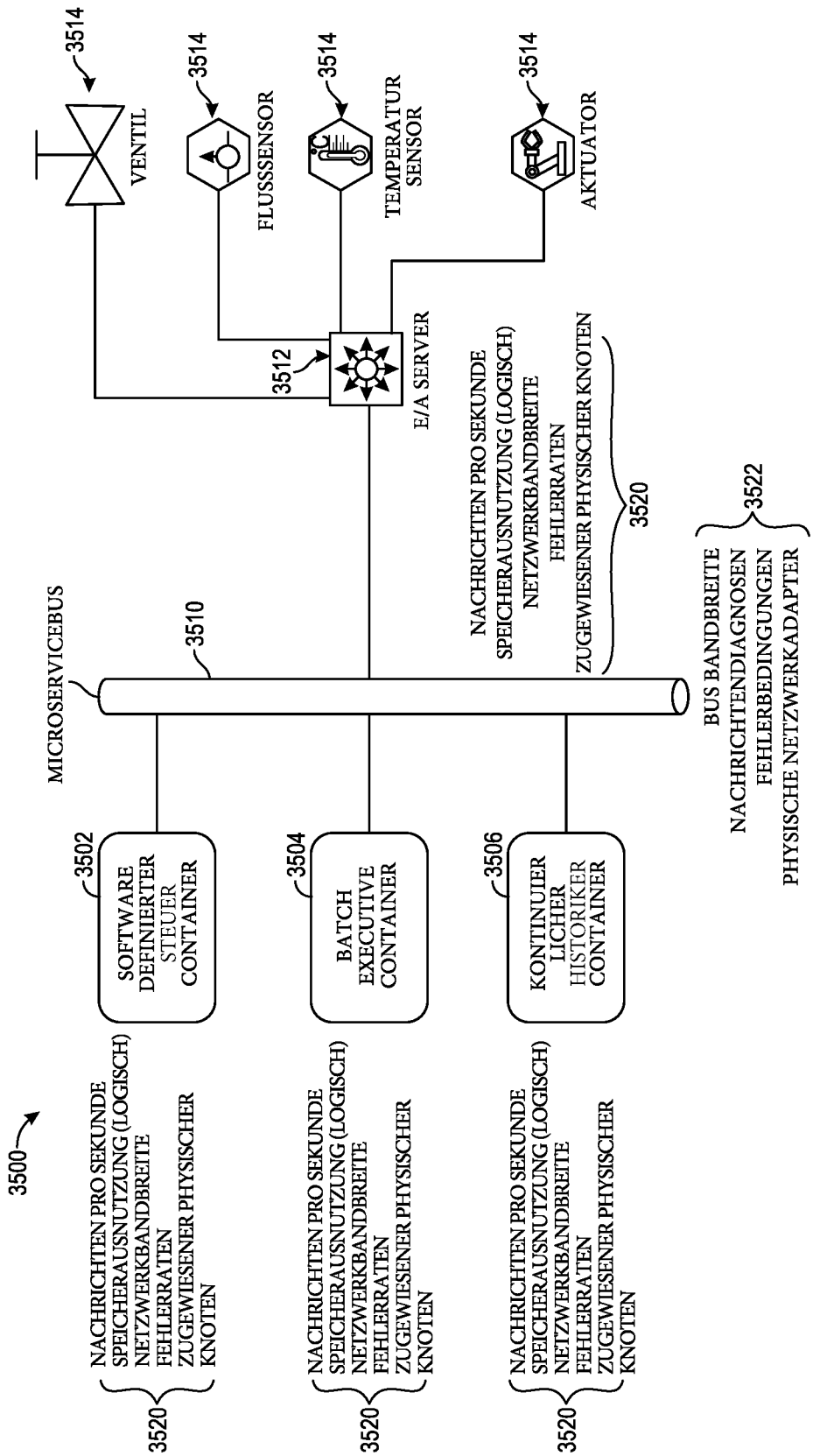

3500
MICROSERVICEBUS
3510
3502
SOFTWARE DEFINIERTER STEUER CONTAINER
3504
BATCH EXECUTIVE CONTAINER
3506
KONTINUIERLICHER HISTORIKER CONTAINER
NACHRICHTEN PRO SEKUNDE
SPEICHERAUSNUTZUNG (LOGISCH)
NETZWERKBANDBREITE
FEHLERRATEN
ZUGEWIESENER PHYSISCHER KNOTEN
3520
3512
E/A SERVER
3514
VENTIL
FLUSSSENSOR
TEMPERATUR SENSOR
AKTUATOR
NACHRICHTEN PRO SEKUNDE
SPEICHERAUSNUTZUNG (LOGISCH)
NETZWERKBANDBREITE
FEHLERRATEN
ZUGEWIESENER PHYSISCHER KNOTEN
3520
BUS BANDBREITE
NACHRICHTENDIAGNOSEN
FEHLERBEDINGUNGEN
PHYSISCHE NETZWERKADAPTER
3522

FIG. 46