(19) Deutsches Patent- und Markenamt

(10) **DE 11 2018 002 954 T5** 2020.04.02

(12) # Veröffentlichung

der internationalen Anmeldung mit der
(87) Veröffentlichungs-Nr.: **WO 2019/025921**
in der deutschen Übersetzung (Art. III § 8 Abs. 2 IntPatÜG)
(21) Deutsches Aktenzeichen: **11 2018 002 954.9**
(86) PCT-Aktenzeichen: **PCT/IB2018/055633**
(86) PCT-Anmeldetag: **27.07.2018**
(87) PCT-Veröffentlichungstag: **07.02.2019**
(43) Veröffentlichungstag der PCT Anmeldung in deutscher Übersetzung: **02.04.2020**

(51) Int Cl.: ***G06F 21/54*** (2013.01)

(30) Unionspriorität:
15/664,723 **31.07.2017** **US**

(71) Anmelder:
International Business Machines Corporation, Armonk, N.Y., US

(74) Vertreter:
Richardt Patentanwälte PartG mbB, 65185 Wiesbaden, DE

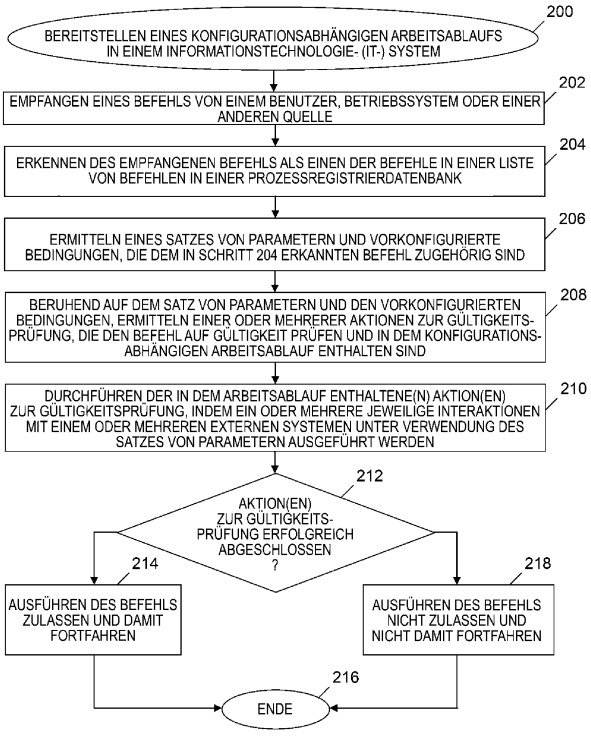
(72) Erfinder:
Gopinath, Arun, Bangalore, IN; Kumaramkandath, Sudheer, Bangalore, IN; Rao, Suryanarayana, Bangalore, IN; Pathak, Ramesh Chandra, Bangalore, IN

Prüfungsantrag gemäß § 44 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **BEREITSTELLEN EINES KONFIGURATIONSABHÄNGIGEN ARBEITSABLAUFS**

(57) Zusammenfassung: Ein Ansatz zum Bereitstellen eines konfigurationsabhängigen Arbeitsablaufs in einem IT-System wird bereitgestellt. Ein zum Ausführen eingeleiteter Befehl wird als in einer Liste von Befehlen enthalten erkannt. Ein Satz von Parametern und vorkonfigurierte Bedingungen, die dem erkannten Befehl zugehörig sind, werden ermittelt. Eine oder mehrere Aktionen zur Gültigkeitsprüfung, die den Befehl auf Gültigkeit prüfen und in dem konfigurationsabhängigen Arbeitsablauf enthalten sind, werden ermittelt. Die Aktion(en) zur Gültigkeitsprüfung wird/werden durch jeweils eine oder mehrere Interaktionen mit einem oder mehreren externen Systemen festgelegt. Eine oder mehrere Aktionen zur Gültigkeitsprüfung, die in dem konfigurationsabhängigen Arbeitsablauf enthalten sind, werden durchgeführt, indem die eine oder mehreren Interaktionen mit dem einen oder den mehreren externen Systemen unter Verwendung des Satzes von Parametern ausgeführt werden. Es wird ermittelt, ob die eine oder mehreren Aktionen zur Gültigkeitsprüfung erfolgreich abgeschlossen werden. Wenn die eine oder mehreren Aktionen zur Gültigkeitsprüfung erfolgreich abgeschlossen werden, wird das Ausführen des Befehls fortgesetzt. Wenn mindestens eine der einen oder mehreren Aktionen zur Gültigkeitsprüfung nicht erfolgreich abgeschlossen wird, wird das Ausführen des Befehls abgebrochen.



Beschreibung

HINTERGRUND

[0001] Die vorliegende Erfindung bezieht sich auf das Verwalten von Systemen der Informationstechnologie (IT) und insbesondere auf das Bereitstellen eines konfigurationsabhängigen Arbeitsablaufs in einem IT-System.

[0002] Als Reaktion darauf, dass ein Systemverwalter in einem IT-System in einer UNIX®-Umgebung einen Befehl zum Herunterfahren oder Neustarten ausgibt, leitet das IT-System ein entsprechendes Herunterfahren oder Neustarten des Systems ein. Wenn das IT-System aktive Anwendungen oder Datenbanken umfasst, beendet das System Prozesse, die den aktiven Anwendungen oder Datenbanken zugehörig sind. Wenn zum Zeitpunkt des Herunterfahrens oder Neustartens irgendwelche Datenbanktransaktionen stattfinden, kann eine Datenintegritätsverletzung in der Datenbank auftreten. Wenn also der Befehl zum Herunterfahren oder Neustarten aufgrund eines menschlichen Fehlverhaltens unwissentlich aufgerufen wurde, gehen wichtige Geschäftsfunktionalitäten verloren. In bekannten IT-Systemumgebungen gibt es keinen Mechanismus zum Steuern von Befehlen, die wissentlich oder unwissentlich von einem privilegierten (d.h. Root-) Benutzer ausgegeben werden und ein Herunterfahren eines Systems, ein Neustarten eines Systems oder eine andere kritische Systemaktivität durchführen. UNIX® ist eine eingetragene Marke von X/Open Company, Ltd., ansässig in Berkshire, Vereinigtes Königreich.

[0003] Rollenbasierte Zugriffssteuerung (RBAC, Role Based Access Control) ist ein bekanntes Modell, das den Zugriff auf Betriebssysteme und Software steuert. Innerhalb des RBAC-Modells wird Zugriff beruhend auf den Rollen gewährt, die einzelne Benutzer in der Organisation haben, in der das System verwendet wird. Zum Beispiel kann ein Benutzerverwalter mittels RBAC Benutzer hinzufügen, ändern oder löschen, ohne Zugriff auf leistungsfähigere Befehle zu haben, die ein Systemverwalter ausführen kann, und ohne Zugriff auf Dateien zu haben, auf die ein Systemverwalter zugreifen kann. RBAC löst das Problem, das UNIX®-Systeme haben können, bei denen „root“ verwendet wird, um einen vollständigen Zugriff zu erhalten, um die einfachsten Verwaltungsaufgaben zu erledigen, die keinen Superuser-Zugriff erfordern. Für RBAC gelten finanzielle Lizenzbedingungen, die kostspielig sind. Für die Unterstützung von RBAC sind zusätzliche Schulungen erforderlich. Auf dem UNIX®-Markt ist es schwierig, Ressourcen mit Kenntnissen über RBAC zu finden. Darüber hinaus kann ein RBAC-Root-Benutzer weiterhin ein Herunterfahren oder andere störende Befehle einleiten, ohne dass irgendeine andere stringente Steuerung auf die Befehle angewendet wird.

[0004] Ein weiteres bekanntes Zugriffssteuerungssystem für UNIX®-Systeme ist die eTrust®-Zugriffssteuerung, welche die Informationsbestände von Rechenzentren schützt, indem sie prüft, ob Benutzer, die Dienste von dem Host-Betriebssystem anfordern, berechtigt sind, auf diese Dienste zuzugreifen. Die eTrust®-Zugriffssteuerung kann so konfiguriert werden, dass sie das Aufrufen bestimmter Befehle verbietet, wobei aber ein Root-Benutzer den eTrust-Dienst anhalten und dann die zuvor verbotenen Befehle aufrufen kann. Des Weiteren können die Befehle von der Systemkonsole aus ausgeführt werden, selbst wenn der eTrust®-Zugriffssteuerungsdienst läuft.

KURZDARSTELLUNG

[0005] In einer Ausführungsform stellt die vorliegende Erfindung ein Verfahren zum Bereitstellen eines konfigurationsabhängigen Arbeitsablaufs in einem IT-System bereit. Das Verfahren umfasst das Erkennen durch einen Computer, dass ein Befehl in einer Liste von Befehlen enthalten ist. Der Befehl wird zum Ausführen eingeleitet. Als Reaktion auf den Schritt des Erkennens des Befehls ermittelt der Computer einen Satz von Parametern und vorkonfigurierte Bedingungen, die dem erkannten Befehl zugehörig sind. Beruhend auf dem Satz von Parametern und den vorkonfigurierten Bedingungen ermittelt der Computer eine oder mehrere Aktionen zur Gültigkeitsprüfung, die den Befehl auf Gültigkeit prüfen und in dem konfigurationsabhängigen Arbeitsablauf enthalten sind. Die eine oder mehreren Aktionen zur Gültigkeitsprüfung werden durch jeweilige eine oder mehrere Interaktionen mit einem oder mehreren externen Systemen festgelegt. Der Computer führt die eine oder mehreren Aktionen zur Gültigkeitsprüfung durch, die in dem konfigurationsabhängigen Arbeitsablauf enthalten sind, indem er die eine oder mehreren Interaktionen mit dem einen oder den mehreren externen Systemen unter Verwendung des Satzes von Parametern ausführt und ermittelt, ob die eine oder mehreren Aktionen zur Gültigkeitsprüfung erfolgreich abgeschlossen werden. Darüber hinaus fährt der Computer mit dem Ausführen des Befehls fort, wenn die eine oder mehreren Aktionen zur Gültigkeitsprüfung erfolgreich abgeschlossen werden, oder der Computer bricht das Ausführen des Befehls ab, wenn mindestens eine der einen oder mehreren Aktionen zur Gültigkeitsprüfung nicht erfolgreich abgeschlossen wird.

[0006] Vorteilhafterweise stellt die vorstehend genannte Ausführungsform eine Sicherheitsintegrationsschicht bereit, um Betriebssystembefehle auszuwerten und Befehle von einer beliebigen Quelle oder einem beliebigen Werkzeug abzufangen (z.B. von einer API-Verbindung (Schnittstelle zur Anwendungsprogrammierung), einem böswillig geschriebenen Cron-Job, einem Software-Agenten oder einem

Software-Werkzeug, das versucht, eine schädliche Aktion durchzuführen) und um die Befehle anhand von Konfigurationsregeln und -anwendungen von anpassbaren Unternehmenssicherheitsmodellen auszuwerten, bevor die Befehle den OS-Kernel erreichen, wodurch absichtliche und zufällige Fehler, die Systemverwaltern, Systembetreibern und anderen privilegierten Benutzern in komplexen IT-Umgebungen unterlaufen, verhindert oder reduziert werden, und dadurch wird sichergestellt, dass kritische Geschäftsfunktionalitäten eines IT-Systems nicht verloren gehen.

[0007] Vorzugsweise stellt die vorliegende Erfindung ein Verfahren bereit, welches das Durchführen einer oder mehrerer zusätzlicher Aktionen durch den Computer neben dem Abbrechen des Ausführens des Befehls aufweist, wenn eine Aktion zur Gültigkeitsprüfung, die in der einen oder den mehreren Aktionen zur Gültigkeitsprüfung enthalten ist, nicht erfolgreich abgeschlossen wird. Das Durchführen der einen [oder] mehreren zusätzlichen Aktionen umfasst das Senden einer Benachrichtigung, die angibt, dass die Aktion zur Gültigkeitsprüfung nicht erfolgreich abgeschlossen wurde. Vorteilhafterweise sorgt das Verfahren für das Senden einer Benachrichtigung, die einen Systemverwalter auf einen möglicherweise schädlichen Befehl aufmerksam macht, der bösartig ausgegeben wurde.

[0008] Vorzugsweise stellt die vorliegende Erfindung ein Verfahren bereit, welches das Durchführen einer oder mehrerer zusätzlicher Aktionen durch den Computer neben dem Schritt des Fortführens des Ausführens des Befehls aufweist, wenn eine Aktion zur Gültigkeitsprüfung, die in der einen oder den mehreren Aktionen zur Gültigkeitsprüfung enthalten ist, erfolgreich abgeschlossen wird. Vorteilhafterweise stellt das Verfahren das Durchführen einer oder mehrerer zusätzlicher Aktionen bereit, welche die Datenbankinstanzen vor einem Herunterfahren oder Neustarten des Systems herunterfahren kann, wodurch eine Datenintegritätsverletzung vermieden wird.

[0009] Vorzugsweise stellt die vorliegende Erfindung ein Verfahren bereit, das den Schritt des Ausführens der einen oder mehreren Interaktionen mit einem oder mehreren externen Systemen aufweist, was das Ausführen einer Interaktion mit einem externen System umfasst, das aus der Gruppe ausgewählt ist, die aus einem Konfigurationsverwaltungsdatenbank-System, einem Ticketsystem, einem Auftragsablauf-Steuerungssystem, einem Arbeitslast-Automatisierungssystem und einem Betriebsverwaltungssystem besteht. Vorteilhafterweise stellt das Verfahren das Ausführen der Interaktion mit einem externen System bereit, so dass durch das externe System bereitgestellte kritische Geschäftsfunktionalitäten nicht negativ beeinflusst werden.

[0010] Vorzugsweise stellt die vorliegende Erfindung ein Verfahren bereit, das den Schritt des Durchführens der einen oder mehreren Aktionen zur Gültigkeitsprüfung bereitstellt, was das Prüfen des Befehls auf Gültigkeit anhand von mehreren lokalen Sicherheitsrichtlinien und Richtlinien externer Systeme umfasst, bei denen es sich um an das IT-System angeschlossene Systeme handelt. Vorteilhafterweise stellt das Verfahren das Prüfen des Befehls auf Gültigkeit sowohl anhand von lokalen Sicherheitsrichtlinien als auch Richtlinien von angeschlossenen Systemen bereit, wodurch eine stringente Steuerung der Aktivitäten eines Systemverwalters ermöglicht wird, wodurch kritische Geschäftsfunktionalitäten, die von den angeschlossenen Systemen bereitgestellt werden, erhalten bleiben.

[0011] Vorzugsweise stellt die vorliegende Erfindung ein Verfahren bereit, das aufweist, dass vor dem Schritt des Erkennens des Befehls der Computer den Befehl (i) von einem Software-Werkzeug unter Verwendung einer API-Verbindung (Schnittstelle zur Anwendungsprogrammierung), (ii) als Teil eines in dem IT-System ausgeführten Auftrags, wobei der Auftrag von einem zeitabhängigen Auftragsablauf-Steuerprogramm geplant wird, oder (iii) von einem Software-Agenten empfängt. Vorteilhafterweise stellt das Verfahren eine stringente Steuerung über verschiedene mögliche Quellen eines Befehls bereit, der eine schädliche Aktion verursachen oder eine kritische Systemaktivität beeinträchtigen kann, wodurch kritische Geschäftsfunktionalitäten erhalten bleiben.

[0012] Vorzugsweise stellt die vorliegende Erfindung ein Verfahren bereit, das aufweist, dass vor dem Schritt des Erkennens des Befehls der Computer den Befehl von einem Betriebssystem oder Teilsystem des Betriebssystems empfängt. Vorteilhafterweise stellt das Verfahren eine stringente Steuerung über Teilsystem-Quellen eines Befehls bereit, der eine schädliche Aktion verursachen oder eine kritische Systemaktivität beeinträchtigen kann, wodurch kritische Geschäftsfunktionalitäten erhalten bleiben.

[0013] Vorzugsweise stellt die vorliegende Erfindung ein Verfahren bereit, welches das Erzeugen der Liste von Befehlen durch den Computer aufweist, die jeweilige kritische Aktivitäten des IT-Systems durchführen, wobei mindestens einer der Befehle eine Aktion durchführt, die schädlich für das IT-System ist. Vorteilhafterweise stellt das Verfahren das Erzeugen der Liste von Befehlen bereit, um wirksam eine vorkonfigurierte Liste von Befehlen bereitzustellen, mit der ein empfangener Befehl verglichen wird. Das Vorkonfigurieren der Befehle in der Liste gestattet eine effiziente Verarbeitung durch das vorstehend genannte Verfahren lediglich derjenigen Befehle, die eine kritische Systemaktivität beeinträchtigen können.

[0014] Die oben erörterten Vorteile gelten auch für die Ausführungsformen des Computersystems und des Computerprogrammprodukts, die im Folgenden zusammengefasst werden.

[0015] In einer anderen Ausführungsform stellt die vorliegende Erfindung ein Computerprogrammprodukt bereit, das ein durch einen Computer lesbares Speichermedium und durch einen Computer lesbaren Programmcode aufweist, der in dem durch einen Computer lesbaren Speichermedium gespeichert ist. Der durch einen Computer lesbare Programmcode umfasst Anweisungen, die von einer Zentraleinheit (CPU) eines Computersystems ausgeführt werden, um ein Verfahren zum Bereitstellen eines konfigurationsabhängigen Arbeitsablaufs in einem IT-System umzusetzen. Das Verfahren weist das Erkennen durch das Computersystem auf, dass ein Befehl in einer Liste von Befehlen enthalten ist. Der Befehl wird zum Ausführen eingeleitet. Als Reaktion auf den Schritt des Erkennens des Befehls ermittelt das Computersystem einen Satz von Parametern und vorkonfigurierte Bedingungen, die dem erkannten Befehl zugehörig sind, und das Computersystem ermittelt beruhend auf dem Satz von Parametern und den vorkonfigurierten Bedingungen eine oder mehrere Aktionen zur Gültigkeitsprüfung, die den Befehl auf Gültigkeit prüfen und in dem konfigurationsabhängigen Arbeitsablauf enthalten sind. Die eine oder mehreren Aktionen zur Gültigkeitsprüfung werden durch jeweilige eine oder mehrere Interaktionen mit einem oder mehreren externen Systemen festgelegt. Das Computersystem führt die eine oder mehreren Aktionen zur Gültigkeitsprüfung durch, die in dem konfigurationsabhängigen Arbeitsablauf enthalten sind, indem es die eine oder mehreren Interaktionen mit dem einen oder den mehreren externen Systemen unter Verwendung des Satzes von Parametern ausführt. Das Computersystem ermittelt dann, ob die eine oder mehreren Aktionen zur Gültigkeitsprüfung erfolgreich abgeschlossen werden. Wenn die eine oder mehreren Aktionen zur Gültigkeitsprüfung erfolgreich abgeschlossen werden, fährt das Computersystem mit dem Ausführen des Befehls fort, oder, wenn mindestens eine der einen oder mehreren Aktionen zur Gültigkeitsprüfung nicht erfolgreich abgeschlossen wird, bricht das Computersystem das Ausführen des Befehls ab.

[0016] Vorzugsweise stellt die vorliegende Erfindung ein Verfahren bereit, das darüber hinaus den Schritt des Durchführens einer oder mehrerer zusätzlicher Aktionen durch das Computersystem neben dem Schritt des Abbrechens des Ausführens des Befehls aufweist, wenn eine Aktion zur Gültigkeitsprüfung, die in der einen oder den mehreren Aktionen zur Gültigkeitsprüfung enthalten ist, nicht erfolgreich abgeschlossen wird, wobei der Schritt des Durchführens der einen oder mehreren zusätzlichen Aktionen das Senden einer Benachrichtigung umfasst, die angibt, dass die Aktion zur Gültigkeitsprüfung nicht erfolgreich abgeschlossen wurde.

[0017] Vorzugsweise stellt die vorliegende Erfindung ein Computerprogrammprodukt bereit, wobei das Verfahren darüber hinaus den Schritt des Durchführens einer oder mehrerer zusätzlicher Aktionen durch das Computersystem neben dem Schritt des Fortführens des Ausführens des Befehls aufweist, wenn eine Aktion zur Gültigkeitsprüfung, die in der einen oder den mehreren Aktionen zur Gültigkeitsprüfung enthalten ist, erfolgreich abgeschlossen wird.

[0018] Vorzugsweise stellt die vorliegende Erfindung ein Computerprogrammprodukt bereit, wobei der Schritt des Ausführens der einen oder mehreren Interaktionen mit einem oder mehreren externen Systemen das Ausführen der Interaktion mit einem externen System umfasst, das aus der Gruppe ausgewählt ist, die aus einem Konfigurationsverwaltungsdatenbank-System, einem Ticketsystem, einem Auftragsablauf-Steuerungssystem, einem Arbeitslast-Automatisierungssystem und einem Betriebsverwaltungssystem besteht.

[0019] Vorzugsweise stellt die vorliegende Erfindung ein Computerprogrammprodukt bereit, wobei der Schritt des Durchführens der einen oder mehreren Aktionen zur Gültigkeitsprüfung das Prüfen des Befehls auf Gültigkeit anhand von mehreren lokalen Sicherheitsrichtlinien und Richtlinien externer Systeme umfasst, bei denen es sich um an das IT-System angeschlossene Systeme handelt.

[0020] Vorzugsweise stellt die vorliegende Erfindung ein Computerprogrammprodukt bereit, wobei das Verfahren darüber hinaus den Schritt aufweist, dass vor dem Schritt des Erkennens des Befehls das Computersystem den Befehl (i) von einem Software-Werkzeug unter Verwendung einer API-Verbindung (Schnittstelle zur Anwendungsprogrammierung), (ii) als Teil eines in dem IT-System ausgeführten Auftrags, wobei der Auftrag von einem zeitabhängigen Auftragsablauf-Steuerprogramm geplant wird, oder (iii) von einem Software-Agenten empfängt.

[0021] Vorzugsweise stellt die vorliegende Erfindung ein Computerprogrammprodukt bereit, wobei das Verfahren darüber hinaus den Schritt aufweist, dass vor dem Schritt des Erkennens des Befehls das Computersystem den Befehl von einem Betriebssystem oder Teilsystem des Betriebssystems empfängt.

[0022] Vorzugsweise stellt die vorliegende Erfindung ein Computerprogrammprodukt bereit, wobei das Verfahren darüber hinaus das Erzeugen der Liste von Befehlen durch das Computersystem aufweist, wobei die Befehle jeweilige kritische Aktivitäten des IT-Systems durchführen, wobei mindestens einer der

Befehle eine Aktion durchführt, die schädlich für das IT-System ist.

[0023] In einer anderen Ausführungsform stellt die vorliegende Erfindung ein Computersystem bereit, das eine zentrale Verarbeitungseinheit (CPU), einen mit der CPU verbundenen Hauptspeicher und ein mit der CPU verbundenes, durch einen Computer lesbares Speichermedium umfasst. Das durch einen Computer lesbare Speichermedium umfasst Anweisungen, die von der CPU über den Hauptspeicher ausgeführt werden, um ein Verfahren zum Bereitstellen eines konfigurationsabhängigen Arbeitsablaufs in einem IT-System umzusetzen. Das Verfahren weist das Erkennen durch das Computersystem auf, dass ein Befehl in einer Liste von Befehlen enthalten ist. Der Befehl wird zum Ausführen eingeleitet. Als Reaktion auf den Schritt des Erkennens des Befehls ermittelt das Computersystem einen Satz von Parametern und vorkonfigurierte Bedingungen, die dem erkannten Befehl zugehörig sind. Beruhend auf dem Satz von Parametern und den vorkonfigurierten Bedingungen ermittelt das Computersystem eine oder mehrere Aktionen zur Gültigkeitsprüfung, die den Befehl auf Gültigkeit prüfen und in dem konfigurationsabhängigen Arbeitsablauf enthalten sind. Die eine oder mehreren Aktionen zur Gültigkeitsprüfung werden durch jeweilige eine oder mehrere Interaktionen mit einem oder mehreren externen Systemen festgelegt. Das Computersystem führt die eine oder mehreren Aktionen zur Gültigkeitsprüfung durch, die in dem konfigurationsabhängigen Arbeitsablauf enthalten sind, indem es die eine oder mehreren Interaktionen mit dem einen oder den mehreren externen Systemen unter Verwendung des Satzes von Parametern ausführt. Das Computersystem ermittelt, ob die eine oder mehreren Aktionen zur Gültigkeitsprüfung erfolgreich abgeschlossen werden. Wenn die eine oder mehreren Aktionen zur Gültigkeitsprüfung erfolgreich abgeschlossen werden, fährt das Computersystem mit dem Ausführen des Befehls fort, oder, wenn mindestens eine der einen oder mehreren Aktionen zur Gültigkeitsprüfung nicht erfolgreich abgeschlossen wird, bricht das Computersystem das Ausführen des Befehls ab.

[0024] Vorzugsweise stellt die vorliegende Erfindung ein Computersystem bereit, das den Schritt des Durchführens einer oder mehrerer zusätzlicher Aktionen durch das Computersystem neben dem Schritt des Fortführens des Ausführens des Befehls aufweist, wenn eine Aktion zur Gültigkeitsprüfung, die in der einen oder den mehreren Aktionen zur Gültigkeitsprüfung enthalten ist, erfolgreich abgeschlossen wird.

[0025] Vorzugsweise stellt die vorliegende Erfindung ein Computersystem bereit, wobei der Schritt des Ausführens der einen oder mehreren Interaktionen mit einem oder mehreren externen Systemen das Abschließen einer Interaktion mit einem externen System umfasst, das aus der Gruppe ausgewählt ist, die aus einem Konfigurationsverwaltungsdatenbank-System, einem Ticketsystem, einem Auftragsablauf-Steuerungssystem, einem Arbeitslast-Automatisierungssystem und einem Betriebsverwaltungssystem besteht.

[0026] Vorzugsweise stellt die vorliegende Erfindung ein Computersystem bereit, wobei der Schritt des Durchführens der einen oder mehreren Aktionen zur Gültigkeitsprüfung das Prüfen des Befehls auf Gültigkeit anhand von mehreren lokalen Sicherheitsrichtlinien und Richtlinien externer Systeme umfasst, bei denen es sich um an das IT-System angeschlossene Systeme handelt.

[0027] Vorzugsweise stellt die vorliegende Erfindung ein Computersystem bereit, wobei das Verfahren darüber hinaus den Schritt aufweist, dass vor dem Schritt des Erkennens des Befehls das Computersystem den Befehl (i) von einem Software-Werkzeug unter Verwendung einer API-Verbindung (Schnittstelle zur Anwendungsprogrammierung), (ii) als Teil eines in dem IT-System ausgeführten Auftrags, wobei der Auftrag von einem zeitabhängigen Auftragsablauf-Steuerprogramm geplant wird, oder (iii) von einem Software-Agenten empfängt.

[0028] In einer anderen Ausführungsform stellt die vorliegende Erfindung ein Verfahren zum Bereitstellen eines konfigurationsabhängigen Arbeitsablaufs in einem IT-System bereit. Das Verfahren weist das Abfangen eines Befehls, der eine für das IT-System schädliche Aktion einleitet, von einem Software-Werkzeug durch einen Computer auf. Der Computer erkennt, dass der abgefangene Befehl in einer vorkonfigurierten Liste von Befehlen enthalten ist. Der erkannte Befehl wird dann zum Ausführen eingeleitet. Als Reaktion auf den Schritt des Erkennens des Befehls ermittelt der Computer einen Satz von Parametern und vorkonfigurierte Bedingungen, die dem erkannten Befehl zugehörig sind. Beruhend auf dem Satz von Parametern und den vorkonfigurierten Bedingungen erzeugt der Computer XML-Daten (Extensible Markup Language). Der Computer tauscht mit externen Systemen Daten über eine generische externe Systemsteuerungsroutine aus, indem er die XML-Daten über SOAP über eine HTTPS-Schicht (Hypertext Transfer Protocol over Transport Security Layer) verwendet. Die externen Systeme weisen ein Ticketsystem für das IT-System und ein Auftragsablauf-Steuerungssystem für das IT-System auf. Als Reaktion auf den Schritt des Austauschens von Daten nimmt der Computer mit dem Ticketsystem in dem konfigurationsabhängigen Arbeitsablauf Verbindung auf, wodurch ermittelt wird, ob für den erkannten Befehl eine genehmigte Änderungssteuerung vorhanden ist. Als Reaktion auf den Schritt des Austauschens von Daten nimmt der Computer mit

dem Auftragsablauf-Steuerungssystem in dem konfigurationsabhängigen Arbeitsablauf Verbindung auf, wodurch ermittelt wird, ob Sicherungskopien innerhalb eines vorher festgelegten Zeitraums vor dem Abfangen des erkannten Befehls als gültig eingestuft werden. Wenn die genehmigte Änderungssteuerung vorhanden ist und die Sicherungskopien als gültig eingestuft werden, fährt der Computer mit dem Ausführen des erkannten Befehls fort, bzw. wenn die genehmigte Änderungssteuerung nicht vorhanden ist, beendet der Computer das Ausführen des erkannten Befehls, so dass das IT-System durch die schädliche Aktion nicht beeinträchtigt wird, oder, wenn die Sicherungskopien als nicht gültig eingestuft werden, beendet der Computer das Ausführen des erkannten Befehls, so dass das IT-System durch die schädliche Aktion beeinträchtigt wird.

[0029] In einer anderen Ausführungsform stellt die vorliegende Erfindung ein Computerprogrammprodukt bereit, das ein durch einen Computer lesbares Speichermedium und durch einen Computer lesbaren Programmcode aufweist, der in dem durch einen Computer lesbaren Speichermedium gespeichert ist. Der durch einen Computer lesbare Programmcode umfasst Anweisungen, die von einer Zentraleinheit (CPU) eines Computersystems ausgeführt werden, um ein Verfahren zum Bereitstellen eines konfigurationsabhängigen Arbeitsablaufs in einem IT-System umzusetzen. Das Verfahren weist das Abfangen eines Befehls, der eine für das IT-System schädliche Aktion einleitet, von einem Software-Werkzeug durch das Computersystem auf. Das Verfahren weist das Erkennen durch das Computersystem auf, dass der abgefangene Befehl in einer vorkonfigurierten Liste von Befehlen enthalten ist. Der erkannte Befehl wird zum Ausführen eingeleitet. Als Reaktion auf den Schritt des Erkennens des Befehls ermittelt das Computersystem einen Satz von Parametern und vorkonfigurierte Bedingungen, die dem erkannten Befehl zugehörig sind. Beruhend auf dem Satz von Parametern und den vorkonfigurierten Bedingungen erzeugt das Computersystem XML-Daten (Extensible Markup Language). Das Computersystem tauscht mit externen Systemen Daten über eine generische externe Systemsteuerungsroutine aus, indem es die XML-Daten über SOAP über eine HTTPS-Schicht (Hypertext Transfer Protocol over Transport Security Layer) verwendet. Die externen Systeme weisen ein Ticketsystem für das IT-System und ein Auftragsablauf-Steuerungssystem für das IT-System auf. Als Reaktion auf den Schritt des Austauschens von Daten nimmt das Computersystem mit dem Ticketsystem in dem konfigurationsabhängigen Arbeitsablauf Verbindung auf, wodurch ermittelt wird, ob für den erkannten Befehl eine genehmigte Änderungssteuerung vorhanden ist. Als Reaktion auf den Schritt des Austauschens von Daten nimmt das Computersystem mit dem Auftragsablauf-Steuerungssystem in dem konfigurationsabhängigen Arbeitsablauf Verbindung auf, wodurch ermittelt wird, ob Sicherungskopien innerhalb eines vorher festgelegten Zeitraums vor dem Abfangen des erkannten Befehls als gültig eingestuft werden. Wenn die genehmigte Änderungssteuerung vorhanden ist und die Sicherungskopien als gültig eingestuft werden, fährt das Computersystem mit dem Ausführen des erkannten Befehls fort, bzw. wenn die genehmigte Änderungssteuerung nicht vorhanden ist, beendet das Computersystem das Ausführen des erkannten Befehls, so dass das IT-System durch die schädliche Aktion nicht beeinträchtigt wird, oder, wenn die Sicherungskopien als nicht gültig eingestuft werden, beendet das Computersystem das Ausführen des erkannten Befehls, so dass das IT-System durch die schädliche Aktion beeinträchtigt wird.

Figurenliste

Fig. 1 ist ein Blockschaubild eines Systems zum Bereitstellen eines konfigurationsabhängigen Arbeitsablaufs in einem IT-System, in das eine Regel-Steuerungsroutine integriert ist, gemäß Ausführungsformen der vorliegenden Erfindung.

Fig. 2 ist ein Ablaufplan eines Prozesses des Bereitstellens eines konfigurationsabhängigen Arbeitsablaufs in einem IT-System, in das eine Regel-Steuerungsroutine integriert ist, gemäß Ausführungsformen der vorliegenden Erfindung.

Fig. 3A stellt ein Beispiel von in dem Prozess aus **Fig. 2** verwendeten Registrierdatenbanken und APIs gemäß Ausführungsformen der vorliegenden Erfindung dar.

Die **Fig. 3B** bis **Fig. 3C** stellen ein Beispiel des Prozesses aus **Fig. 2** unter Verwendung der Registrierdatenbanken und APIs in **Fig. 3A** gemäß Ausführungsformen der vorliegenden Erfindung dar.

Fig. 4 ist ein Blockschaubild eines Computers, der in dem System aus **Fig. 1** enthalten ist und den Prozess aus **Fig. 2** umsetzt, gemäß Ausführungsformen der vorliegenden Erfindung.

AUSFÜHRLICHE BESCHREIBUNG

ÜBERBLICK

[0030] Ausführungsformen der vorliegenden Erfindung stellen eine Sicherheitsintegrationsschicht zwischen dem Benutzer und dem Betriebssystem (**OS**) in einem IT-System bereit. Die Sicherheitsintegrationsschicht tauscht mit dem **OS** über einen Prozessdämon im Kernelkontext Daten aus. Die Sicherheitsintegrationsschicht agiert oberhalb des **OS**, um Befehle von Benutzern, Anwendungen bzw. dem **OS** auszuwerten, die kritische Systemaktivitäten durchführen (z.B. Herunterfahren des Systems, Neustar-

ten des Systems, Erstellen eines Dateisystems, Formatieren einer neu zugewiesenen Nummer einer logischen Speichereinheit (LUN, logical unit number), usw.), und um Befehle von einer beliebigen Quelle oder einem beliebigen Werkzeug abzufangen, wie zum Beispiel von einer API-Verbindung, einem böswillig geschriebenen Cron-Job oder einem Software-Werkzeug oder - Agenten, die versuchen, eine für das IT-System schädliche Aktion durchzuführen, und um eine fundierte Entscheidung über die abgefangenen Befehle beruhend auf einer vorkonfigurierten Logik (z.B. Konfigurationsregeln) zu treffen. Das Auswerten und Abfangen von Befehlen durch die Sicherheitsintegrationsschicht verhindert oder verringert Bedienfehler, darunter vorsätzliche Fehler und zufällige Fehler. Bestandteile der Sicherheitsintegrationsschicht umfassen (1) eine Prozessregistrierdatenbank, (2) eine Konfigurationsregistrierdatenbank, (3) eine Aktionsregistrierdatenbank und (4) APIs zu externen Systemen, die in der Erörterung der nachfolgend beschriebenen **Fig. 1** ausführlicher beschrieben werden.

[0031] Eine einzigartige Herausforderung in einer UNIX®-Umgebung besteht in dem Mangel an definierten Wegen zum Steuern von Aktivitäten eines privilegierten Benutzers (d.h. Root-Benutzers). Nachdem sich ein Benutzer als Root-Benutzer in dem UNIX®-System angemeldet hat, erhält dieser Benutzer als privilegierter Benutzer Zugriff auf alle Befehle. Ein nachfolgender menschlicher Fehler durch den privilegierten Benutzer kann einen Befehl zum Herunterfahren oder Neustarten auslösen, der aktive Anwendungs- und Datenbankprozesse beenden kann. Wenn zum Zeitpunkt des Ablaufens des Herunterfahrens oder Neustartens Datenbanktransaktionen stattfinden, kann die Integrität von Daten verletzt werden. Folglich kann ein unwissentlich aufgerufener Befehl dazu führen, dass kritische Geschäftsfunktionalitäten verloren gehen. Hierin offenbarte Ausführungsformen vermeiden die vorstehend genannten Probleme durch menschliche Fehler, indem sie den Befehl mittels eines Satzes von Vorbedingungen auswerten. Als ein Beispiel in Bezug auf einen Befehl zum Herunterfahren kann der Satz von Vorbedingungen umfassen, dass eine Änderungssteuerung durch Austauschen von Daten mit einem Ticketsystem auf Gültigkeit geprüft wird, dass aktuelle Sicherungskopien durch Austauschen von Daten mit einem Auftragsablauf-Steuerungssystem auf Gültigkeit geprüft werden, und dass Datenbankinstanzen erkannt und heruntergefahren werden.

[0032] In einer Ausführungsform werden, bevor die Befehle eines Bedieners den OS-Kernel erreichen, die Befehle einem Analysieren (parsing) unterzogen und automatisch anhand von Konfigurationsregeln und einem Anwenden von anpassbaren Unternehmenssicherheitsmodellen ausgewertet.

[0033] In einer Ausführungsform ist die Sicherheitsintegrationsschicht mit APIs externer Systeme (z.B. Ticketsysteme, Änderungsverwaltungsdatenbank- (CMDB-) Systeme, Wartungs-/Ausfallzeit-Repositories, Unternehmenschargenverwaltungs-Werkzeuge (enterprise batch management tools) und Systemüberwachungsagenten) integriert, um fundierte und automatisierte Entscheidungen darüber zu treffen, ob Befehle eines Bedieners erlaubt und ausgeführt werden sollen, um (eine) Aktion(en) durchzuführen, oder ob sie verboten und beendet werden sollen, so dass die Aktion(en) nicht durchgeführt wird/werden. Wenn ein Befehl eines Bedieners verboten und beendet wird, so dass eine dem Befehl zugehörige Aktion nicht durchgeführt wird, kann die Sicherheitsintegrationsschicht eine fundierte und automatisierte Entscheidung treffen, um zu ermitteln, ob eine oder mehrere andere Aktionen ausgeführt werden.

[0034] Ausführungsformen der vorliegenden Erfindung können als Teil eines Standardsystemangebots oder mit einem Cloud-Angebot gebündelt werden.

SYSTEM ZUM BEREITSTELLEN EINES KONFIGURATIONSABHÄNGIGEN ARBEITSABLAUFS

[0035] **Fig. 1** ist ein Blockschaubild eines Systems **100** zum Bereitstellen eines konfigurationsabhängigen Arbeitsablaufs in einem IT-System gemäß Ausführungsformen der vorliegenden Erfindung. Das System **100** umfasst einen Computer **102**, der eine Sicherheitsintegrationsschicht **104** ausführt (d.h. ein auf Software beruhendes Sicherheitsintegrationssystem). Die Sicherheitsintegrationsschicht **104** umfasst eine zentrale Verwaltungskonsole **106**, einen Zwischenspeicherkanal **108**, eine Prozessregistrierdatenbank **110**, eine Konfigurationsregistrierdatenbank **112**, eine Aktionsregistrierdatenbank **114**, eine generische externe Systemsteuerungsroutine **116** und ein systemspezifisches Übersetzungsmodul **118**.

[0036] Die Sicherheitsintegrationsschicht **104** empfängt Befehle **120-1**, ..., **120-N** und wertet diese aus, wozu Benutzer- und/oder Anwendungsbefehle gehören, und wobei N eine ganze Zahl größer oder gleich eins ist. Die Sicherheitsintegrationsschicht **104** tauscht mit einem Betriebssystem (**OS**) (nicht gezeigt) des Computers **102** über einen Prozessdämon im Kernelkontext Daten aus. Die Sicherheitsintegrationsschicht **104** agiert oberhalb des **OS**, um jeden der Befehle **120-1**, ..., **120-N** auszuwerten, und trifft beruhend auf vorkonfigurierten Regeln fundierte Entscheidungen bezüglich des Prüfens der Gültigkeit jedes der Befehle **120-1**, ..., **120-N** sowie darüber, ob das Ausführen jedes der Befehle **120-1**, ..., **120-N** fortzuführen ist.

[0037] Die Prozessregistrierdatenbank **110** umfasst eine Liste von Prozessen und Befehlen, die als durch die Sicherheitsintegrationsschicht **104** verwaltet und gesteuert gekennzeichnet sind. Wenn der Befehl oder Prozess in der Prozessregistrierdatenbank **110** aufgeführt ist, übergibt die Sicherheitsintegrationsschicht **104** die Steuerung an die Konfigurationsregistrierdatenbank **112**.

[0038] Die Konfigurationsregistrierdatenbank **112** umfasst einen Satz von konfigurierbaren Parametern und vorkonfigurierten Bedingungen, anhand derer jeder der Befehle **120-1**, ..., **120-N** geprüft wird, um die Befehle **120-1**, ..., **120-N** auf Gültigkeit zu prüfen. Zum Beispiel kann die Konfigurationsregistrierdatenbank **112** eine vorkonfigurierte Bedingung umfassen, die angibt, dass eine Gültigkeitsprüfung eines Befehls eine Anbindung an ein externes Ticketsystem umfassen muss, das in einem externen System **122-1**, ..., externen System **122-M** umfasst ist, wobei M eine ganze Zahl größer oder gleich eins ist. Durch die Anbindung an das externe Ticketsystem wird sichergestellt, dass für den Befehl eine gültige Änderungsverwaltung vorhanden ist. Als Reaktion darauf, dass die Konfigurationsregistrierdatenbank **112** den Befehl anhand des Satzes von Parametern und der vorkonfigurierten Bedingungen als gültig einstuft, übergibt die Sicherheitsintegrationsschicht **104** die Steuerung an die Aktionsregistrierdatenbank **114**.

[0039] Die Aktionsregistrierdatenbank **114** umfasst (eine) konfigurierbare Aktion(en), die als Reaktion auf die erfolgreiche Gültigkeitsprüfung eines in den Befehlen **120-1**, ..., **120-N** enthaltenen Befehls durch die Konfigurationsregistrierdatenbank **112** durchgeführt werden. Die Aktionsregistrierdatenbank **114** kann auf mehrere Arten konfiguriert sein: (1) Ausführen des Befehls; (2) Abbrechen des Befehls; oder (3) Einleiten zusätzlicher Aktionen.

[0040] Die Prozessregistrierdatenbank **110**, die Konfigurationsregistrierdatenbank **112** und die Aktionsregistrierdatenbank **114** werden zentral durch die zentrale Verwaltungskonsole **106** verwaltet, aber lokal durch den Zwischenspeicherkanal **108** zwischengespeichert.

[0041] Die generische externe Systemsteuerungsroutine **116** umfasst APIs, die für das Austauschen von Daten mit dem externen System **122-1**, ..., externen System **122-M** verwendet werden, wobei M eine ganze Zahl größer oder gleich eins ist. Der vorstehend erwähnte Datenaustausch mit den externen Systemen **122-1**, ..., **122-M** führt dazu, dass zusätzliche Anfragen empfangen und zusätzliche Antworten übermittelt werden, um endgültige Entscheidungen darüber zu treffen, ob jeder der Befehle **120-1**, ..., **120-N** erfolgreich auf Gültigkeit geprüft wird.

[0042] Die Sicherheitsintegrationsschicht **104** läuft lokal in Bezug auf das IT-System. Die Sicherheitsintegrationsschicht **104** nutzt den Zwischenspeicherkanal **108** zum Vermeiden oder Verringern von Übertragungsverzögerungen (d.h. Latenzen beim Auswerten der Befehle **120-1**, ..., **120-N** oder von Konfigurationsänderungen). Die zentrale Verwaltungskonsole **106** stellt zentralisierte Systemverwaltungsfunktionen bereit, die ein Steuern von anderen Systemen (nicht gezeigt) ermöglichen, zu denen jeweilige Sicherheitsintegrationsschichten (nicht gezeigt) gehören, welche die Funktionalitäten der Sicherheitsintegrationsschicht **104** bereitstellen.

[0043] Die Sicherheitsintegrationsschicht **104** fängt schädliche Befehle, die in den Befehlen **120-1**, ..., **120-N** enthalten sind, von einer beliebigen Quelle oder einem beliebigen Software-Werkzeug ab (z.B. von einer API-Verbindung, einem böswillig geschriebenen Cron-Job oder einem Software-Agenten oder -Werkzeug, die versuchen, eine für das System **100** schädliche Aktion durchzuführen).

[0044] In einer Ausführungsform ist die Sicherheitsintegrationsschicht **104** auf der OS-Schicht des Systems **100** mit den externen Systemen **122-1**, ..., **122-M** integriert. In einer Ausführungsform umfassen die externen Systeme **122-1**, ..., **122-M** Ticketsysteme oder andere berechtigungsgesteuerte Systeme zum Austauschen von Daten über Sockel oder andere Mittel unter Verwendung von XML-Daten (Extensible Markup Language) über SOAP (ursprünglich Simple Object Access Protocol) über HTTPS (Hypertext Transfer Protocol over Transport Layer Security). In einer Ausführungsform kann die Sicherheitsintegrationsschicht **104** die XML-Daten zum Durchführen von konfigurierten zusätzlichen Prüfungen mit den externen Systemen **122-1**, ..., **122-M** verwenden.

[0045] In einer Ausführungsform umfassen die externen Systeme **122-1**, ..., **122-M** ein Ticketsystem, ein Konfigurationsverwaltungsdatenbank-System, ein Überwachungssystem, das eine Betriebs- und Netzwerkverwaltung bereitstellt, und/oder ein Auftragsablauf-Steuerungssystem, das sicherstellt, dass während der Gültigkeitsprüfung eines der Befehle **120-1**, ..., **120-N** kein Auftrag läuft, und das genehmigte Ausfallzeiten prüft, Wartungsfenster prüft, usw.

[0046] In einer Ausführungsform ist der Datenaustausch, den die Sicherheitsintegrationsschicht **104** mit den externen Systemen **122-1**, ..., **122-M** durchführt, in die generische externe Systemsteuerungsroutine **116** eingebettet, um zusätzliche Anfragen und Antworten zu empfangen und zu senden, um eine endgültige Entscheidung über die Gültigkeitsprüfung und das Ausführen jedes der Befehle **120-1**, ..., **120-N** zu treffen.

[0047] In einer alternativen Ausführungsform fängt die Sicherheitsintegrationsschicht **104** OS-Befehle und Teilsystem-Befehle (z.B. aus einem Datenbanksystem, Middleware usw.) über ein beliebiges Eingangsprotokoll wie zum Beispiel Open Database Connectivity (ODBC) ab.

[0048] Die Funktionalität der in **Fig. 1** gezeigten Bestandteile wird in der Erörterung der nachfolgend dargestellten **Fig. 2** und **Fig. 4** näher beschrieben.

PROZESS ZUM BEREITSTELLEN VON KONFIGURATIONSABHÄNGIGEN ARBEITSABLÄUFEN

[0049] **Fig. 2** ist ein Ablaufplan eines Prozesses des Bereitstellens eines konfigurationsabhängigen Arbeitsablaufs in einem IT-System, in das eine Regel-Steuerungsroutine integriert ist, gemäß Ausführungsformen der vorliegenden Erfindung. Der Prozess aus **Fig. 2** beginnt bei Schritt **200**. In Schritt **202** empfängt die Sicherheitsintegrationsschicht **104** (siehe **Fig. 1**) einen Befehl **120-1** (siehe **Fig. 1**) von einem Benutzer, einem Betriebssystem oder einer anderen Quelle.

[0050] In Schritt **204** erkennt die Sicherheitsintegrationsschicht **104** (siehe **Fig. 1**) den in Schritt **202** empfangenen Befehl als einen der Befehle in einer Liste von Befehlen, die in der Prozessregistrierdatenbank **110** (siehe **Fig. 1**) enthalten sind.

[0051] In Schritt **206** ermittelt die Sicherheitsintegrationsschicht **104** (siehe **Fig. 1**) einen Satz von Parametern und vorkonfigurierte Bedingungen, die dem in Schritt **204** erkannten Befehl zugehörig sind.

[0052] In Schritt **208** ermittelt die Sicherheitsintegrationsschicht **104** (siehe **Fig. 1**) beruhend auf dem Satz von Parametern und den vorkonfigurierten Bedingungen, die in Schritt **206** ermittelt wurden, (eine) Aktion(en) zur Gültigkeitsprüfung, die den Befehl **120-1** (siehe **Fig. 1**) auf Gültigkeit prüft/prüfen und in dem konfigurationsabhängigen Arbeitsablauf enthalten ist/sind.

[0053] In Schritt **210** führt die Sicherheitsintegrationsschicht **104** (siehe **Fig. 1**) die Aktion(en) zur Gültigkeitsprüfung durch, die in Schritt **208** ermittelt wurde(n), indem eine oder mehrere jeweilige Interaktionen mit einem oder mehreren externen Systemen ausgeführt werden, die in den externen Systemen **122-1**, ..., **122-M** (siehe **Fig. 1**) enthalten sind, wobei der/die Interaktion(en) den Satz von Parametern nutzt/nutzen, der in Schritt **206** ermittelt wurde.

[0054] In Schritt **212** ermittelt die Sicherheitsintegrationsschicht **104** (siehe **Fig. 1**), ob die in Schritt **210** durchgeführte(n) Aktion(en) zur Gültigkeitsprüfung erfolgreich abgeschlossen wurde(n). Wenn in Schritt **212** festgestellt wurde, dass die durchgeführte (n) Aktion(en) zur Gültigkeitsprüfung erfolgreich abgeschlossen wurde(n), wird die Ja-Verzweigung von Schritt **212** genommen, und Schritt **214** wird durchgeführt.

[0055] In Schritt **214** lässt die Sicherheitsintegrationsschicht **104** (siehe **Fig. 1**) das Ausführen des Befehls **120-1** (siehe **Fig. 1**) zu und fährt mit dessen Ausführen fort. Nach Schritt **214** endet der Prozess aus **Fig. 2** bei Schritt **216**.

[0056] Zurück zu Schritt **212**, wenn die Sicherheitsintegrationsschicht **104** (siehe **Fig. 1**) feststellt, dass mindestens eine der Aktion(en) zur Gültigkeitsprüfung nicht erfolgreich abgeschlossen wurde, wird die Nein-Verzweigung von Schritt **212** genommen, und Schritt **218** wird durchgeführt.

[0057] In Schritt **218** lässt die Sicherheitsintegrationsschicht **104** (siehe **Fig. 1**) das Ausführen des Befehls **120-1** (siehe **Fig. 1**) nicht zu und fährt nicht mit dessen Ausführen fort. Nach Schritt **218** endet der Prozess aus **Fig. 2** bei Schritt **216**.

BEISPIELE

[0058] **Fig. 3A** stellt ein Beispiel 300 von in dem Prozess aus **Fig. 2** verwendeten Registrierdatenbanken und APIs gemäß Ausführungsformen der vorliegenden Erfindung dar. Das Beispiel 300 umfasst die Prozessregistrierdatenbank **110**, die Konfigurationsregistrierdatenbank **112**, externe System-APIs **302** und die Aktionsregistrierdatenbank **114**. Die Prozessregistrierdatenbank **110** umfasst einen Befehl **304** zum Herunterfahren, um einen Prozess S1P auszuführen, und einen Befehl **306** zum Neustarten, um einen Prozess S2P auszuführen.

[0059] Die Konfigurationsregistrierdatenbank **112** umfasst Abläufe S1C1, **S1C2** bzw. **S1C3** für die folgenden Aktionen zur Gültigkeitsprüfung: Gültigkeitsprüfung der Änderungssteuerung **308**, Gültigkeitsprüfung für aktuelle Sicherungskopien **310** und Gültigkeitsprüfung für Datenbankinstanzen **312**.

[0060] Externe System-APIs umfassen APIs zum Austauschen von Daten mit einem Ticketsystem **314**, einem Ablaufsteuerungssystem **316** und einem Datenbankverwaltungssystem **318**. Die APIs zum Austauschen von Daten mit dem Datenbankverwaltungssystem **318** können JDBC oder ODBC umfassen.

[0061] Die Aktionsregistrierdatenbank **114** legt Abläufe **S1A1** (d.h. Abbrechen des Befehls und Benachrichtigen der Verwaltung über das Abbrechen des Befehls) und **S1A2** (d.h. Fortführen des Ausführens des Befehls) fest, die Ergebnissen aus dem Durchführen der Gültigkeitsprüfung der Änderungssteuerung **308** (d.h. Ablauf S1C1) durch die Konfigurationsre-

gistrierdatenbank **112** durch Austauschen von Daten mit dem Ticketsystem **314** über in den externen System-APIs **302** enthaltene APIs zugehörig sind.

[0062] Darüber hinaus legt die Aktionsregistrierdatenbank **114** Abläufe **S1A3** (d.h. Abbrechen des Befehls) und **S1A4** (d.h. Fortführen des Ausführens des Befehls) fest, die Ergebnissen aus dem Durchführen der Gültigkeitsprüfung für aktuelle Sicherungskopien **310** (d.h. Ablauf **S1C2**) durch die Konfigurationsregistrierdatenbank **112** durch Austauschen von Daten mit einem Ablaufsteuerungssystem **316** über in den externen System-APIs **302** enthaltene APIs zugehörig sind.

[0063] Weiterhin legt die Aktionsregistrierdatenbank **114** Abläufe **S1A5** (d.h. Herunterfahren der Datenbank) und **S1A6** (d.h. Fortführen des Ausführens des Befehls) fest, die Ergebnissen aus dem Durchführen der Gültigkeitsprüfung für Datenbankinstanzen **312** (d.h. Ablauf **S1C3**) durch die Konfigurationsregistrierdatenbank **112** durch Austauschen von Daten mit einem Datenbankverwaltungssystem **318** über in den externen System-APIs **302** enthaltene APIs (z.B. JDBC oder ODBC) zugehörig sind.

[0064] Die Verwendung der Registrierdatenbanken **110**, **112** und **114** sowie der externen System-APIs **302** zum Erkennen und Prüfen eines Befehls auf Gültigkeit und zum Durchführen von (einer) Aktion(en) beruhend auf den Ergebnissen der Gültigkeitsprüfung des Befehls unter Verwendung des Prozesses aus **Fig. 2** ist nachstehend in Bezug auf das in den **Fig. 3B** bis **Fig. 3C** abgebildete Beispiel beschrieben.

[0065] Die **Fig. 3B** bis **Fig. 3C** stellen ein Beispiel **330** des Prozesses aus **Fig. 2** unter Verwendung der Registrierdatenbanken und APIs in **Fig. 3A** gemäß Ausführungsformen der vorliegenden Erfindung dar. Das Beispiel **330** umfasst Aktionen **332**, die durch die Aktionsregistrierdatenbank **114** (siehe **Fig. 3A)** durchgeführt werden, Aktionen **334**, die durch die APIs **302** (siehe **Fig. 3A)** durchgeführt werden, die in der generischen externen Systemsteuerungsroutine **116** (siehe **Fig. 1**) enthalten sind, und Aktionen **336**, die durch die Konfigurationsregistrierdatenbank **112** (siehe **Fig. 3A)** durchgeführt werden. Der Prozess in dem Beispiel **330** beginnt bei Schritt **350** mit dem Ausgeben eines Befehls zum Herunterfahren des Systems durch einen Systemverwalter oder einen anderen Benutzer eines IT-Systems (d.h. das Einleiten eines Herunterfahrens des IT-Systems). Nachstehend wird in der Erörterung der **Fig. 3B** bis **Fig. 3C** der in Schritt **350** ausgegebene Befehl zum Herunterfahren des Systems einfach als „der Befehl" bezeichnet. Die Sicherheitsintegrationsschicht **104** (siehe **Fig. 1**) empfängt den Befehl in Schritt **202** (siehe **Fig. 2**).

[0066] In Schritt **351** (d.h. Abfolge **S1**) wertet die Sicherheitsintegrationsschicht **104** (siehe **Fig. 1**) den Befehl aus und prüft den Befehl anhand der Prozessregistrierdatenbank **110** (siehe **Fig. 3A)** auf Gültigkeit.

[0067] In Schritt **352** (d.h. Prozess S1P) ermittelt die Sicherheitsintegrationsschicht **104** (siehe **Fig. 1**), ob die Gültigkeitsprüfung in Schritt **351** erfolgreich ist (d.h. eine erfolgreiche Gültigkeitsprüfung gibt an, dass der Befehl in einer vorkonfigurierten Liste von Befehlen gefunden wurde, die in der Prozessregistrierdatenbank **110** (siehe **Fig. 3A)** enthalten sind). Die Schritte **351** und **352** sind in Schritt **204** (siehe **Fig. 2**) enthalten.

[0068] Wenn die Sicherheitsintegrationsschicht **104** (siehe **Fig. 1**) in Schritt **352** feststellt, dass die Gültigkeitsprüfung in Schritt **351** erfolgreich ist, wird der Ja-Verzweigung von Schritt **352** gefolgt, und Schritt **353** wird durchgeführt.

[0069] Schritt **206** (siehe **Fig. 2**) geht Schritt **353** voraus. In Schritt **353** (d.h. Abfolge S1C) behält die Sicherheitsintegrationsschicht **104** (siehe **Fig. 1**) die Steuerung über das Verarbeiten des Befehls bei und leitet Gültigkeitsprüfungen für den Befehl anhand von in der Konfigurationsregistrierdatenbank **112** (siehe **Fig. 1**) vorkonfigurierten Bedingungen ein. Die Vorbedingungen bestehen aus dem Prüfen der Gültigkeit (i) der Änderungssteuerung, (ii) der letzten Sicherungskopien und (iii) der Datenbankinstanzen.

[0070] In Schritt **354** (d.h. Abfolge S1C1) leitet die Sicherheitsintegrationsschicht **104** (siehe **Fig. 1**) eine Gültigkeitsprüfung der Änderungssteuerung für den Befehl ein, wodurch versucht wird, zu bestätigen, dass ein genehmigter Änderungsdatensatz vorhanden ist. In Schritt **355** tauscht die Sicherheitsintegrationsschicht **104** (siehe **Fig. 1**) mit dem Ticketsystem **314** (siehe **Fig. 3A)** über eine API in den externen System-APIs **302** (siehe **Fig. 3A)** Daten aus. Die Schritte **354** und **355** sind in Schritt **210** (siehe **Fig. 2**) enthalten.

[0071] In Schritt **356** (d.h. Abfolge **S1A1** oder **S1A2**) ermittelt die Sicherheitsintegrationsschicht **104** (siehe **Fig. 1**), ob der genehmigte Änderungsdatensatz vorhanden ist. Wenn die Sicherheitsintegrationsschicht **104** (siehe **Fig. 1**) in Schritt **356** feststellt, dass der genehmigte Änderungsdatensatz nicht vorhanden ist, wird der Nein-Verzweigung von Schritt **356** gefolgt, und die Schritte **357** und **358** werden durchgeführt, um weitere in der Aktionsregistrierdatenbank **114** (siehe **Fig. 3A)** konfigurierte Aktionen auszuführen. Schritt **356** ist in Schritt **212** (siehe **Fig. 2**) enthalten.

[0072] Als Reaktion darauf, dass die genehmigte Änderungssteuerung in Schritt **356** nicht gefunden wird,

sendet die Sicherheitsintegrationsschicht **104** (siehe **Fig. 1**) in Schritt **357** (d.h. Teil der Abfolge **S1A1**) eine Benachrichtigung an die Verwaltung, die angibt, dass keine genehmigte Änderungssteuerung gefunden wurde. Als Reaktion darauf, dass die genehmigte Änderungssteuerung in Schritt **356** nicht gefunden wird, bricht die Sicherheitsintegrationsschicht **104** (siehe **Fig. 1**) in Schritt **358** das Ausführen des Befehls ab. Schritt **358** ist in Schritt **218** (siehe **Fig. 2**) enthalten.

[0073] Zurück zu Schritt **356**, wenn die Sicherheitsintegrationsschicht **104** (siehe **Fig. 1**) feststellt, dass der genehmigte Änderungsdatensatz vorhanden ist, wird der Ja-Verzweigung von Schritt **356** gefolgt, und Schritt **359** wird durchgeführt.

[0074] Als Reaktion darauf, dass eine genehmigte Änderungssteuerung in Schritt **356** gefunden wird, fährt die Sicherheitsintegrationsschicht **104** (siehe **Fig. 1**) in Schritt **359** (d.h. Abfolge **S1A2**) mit dem Ausführen des Befehls fort, indem sie die Gültigkeitsprüfung des Befehls unter Verwendung der verbleibenden, in Schritt **353** genannten Vorbedingungen fortführt. Schritt **359** ist in Schritt **214** (siehe **Fig. 2**) enthalten.

[0075] In Schritt **360** (d.h. Abfolge **S1C2**) leitet die Sicherheitsintegrationsschicht **104** (siehe **Fig. 1**) anschließend an ein erfolgreiches Abschließen der Gültigkeitsprüfung in Abfolge S1C1 die Gültigkeitsprüfung für die letzten Sicherungskopien ein (d.h. Sicherungskopien, die innerhalb eines vordefinierten Zeitraums unmittelbar vor dem aktuellen Zeitpunkt angefertigt wurden), wobei es sich um die nächste vorkonfigurierte Bedingung in der Konfigurationsregistrierdatenbank **112** (siehe **Fig. 3A)** handelt.

[0076] In Schritt **361** tauscht die Sicherheitsintegrationsschicht **104** (siehe **Fig. 1**) mit dem Ablaufsteuerungssystem **316** (siehe **Fig. 3A)** über eine API in den externen System-APIs **302** (siehe **Fig. 3A)** Daten aus. In Schritt **362** (d.h. Abfolge **S1A3** oder **S1A4**) ermittelt die Sicherheitsintegrationsschicht **104** (siehe **Fig. 1**), ob die letzten Sicherungskopien als gültig eingestuft werden. Die Schritte **360** und **361** sind in Schritt **210** (siehe **Fig. 2**) enthalten.

[0077] Wenn die Sicherheitsintegrationsschicht **104** (siehe **Fig. 1**) in Schritt **362** feststellt, dass die letzten Sicherungskopien nicht als gültig eingestuft werden, wird der Nein-Verzweigung von Schritt **362** gefolgt, und Schritt **358** wird in der Abfolge **S1A3** durchgeführt, wodurch das Ausführen des Befehls abgebrochen wird. Wenn die Sicherheitsintegrationsschicht **104** (siehe **Fig. 1**) in Schritt **362** feststellt, dass die letzten Sicherungskopien als gültig eingestuft werden, wird der Ja-Verzweigung von Schritt **362** gefolgt, und Schritt **359** wird in der Abfolge **S1A4** durchgeführt, wodurch das Ausführen des Befehls fortgesetzt wird, indem die Gültigkeitsprüfung des Befehls unter Verwendung der verbleibenden, in der Konfigurationsregistrierdatenbank **112** (siehe **Fig. 3A)** enthaltenen Vorbedingungen fortgeführt wird. Schritt **362** ist in Schritt **212** (siehe **Fig. 2**) enthalten.

[0078] In Schritt **363** (d.h. Abfolge **S1C3**) leitet die Sicherheitsintegrationsschicht **104** (siehe **Fig. 1**) anschließend an ein erfolgreiches Abschließen der Gültigkeitsprüfung in Abfolge **S1C2** die Gültigkeitsprüfung für die Datenbankinstanzen ein, wobei es sich um die nächste vorkonfigurierte Bedingung in der Konfigurationsregistrierdatenbank **112** (siehe **Fig. 3A)** handelt.

[0079] Nach Schritt **363** fährt der Prozess mit Schritt **364** in **Fig. 3C** fort. **Fig. 3C** umfasst Aktionen **332**, die durch die Aktionsregistrierdatenbank **114** (siehe **Fig. 3A)** durchgeführt werden, und eine Aktion **334**, die durch die APIs **302** (siehe **Fig. 3A)** durchgeführt wird, die in der generischen externen Systemsteuerungsroutine **116** (siehe **Fig. 1**) enthalten sind. In Schritt **364** in **Fig. 3C** tauscht die Sicherheitsintegrationsschicht **104** (siehe **Fig. 1**) mit dem Datenbankverwaltungssystem **318** (siehe **Fig. 3A)** über eine API in den externen System-APIs **302** (siehe **Fig. 3A)** Daten aus. Schritt **363** (siehe **Fig. 3B)** und Schritt **364** sind in Schritt **210** (siehe **Fig. 2**) enthalten.

[0080] In Schritt **365** (d.h. Abfolge **S1A5** oder **S1A6**) ermittelt die Sicherheitsintegrationsschicht **104** (siehe **Fig. 1**) beruhend auf der Interaktion mit dem Datenbankverwaltungssystem **318** (siehe **Fig. 3A)**, ob Datenbankinstanzen gestartet wurden und laufen. Wenn die Sicherheitsintegrationsschicht **104** (siehe **Fig. 1**) in Schritt **365** feststellt, dass eine oder mehrere Datenbankinstanzen gestartet wurden und laufen, wird der Ja-Verzweigung von Schritt **365** gefolgt, und Schritt **366** wird durchgeführt. Schritt **365** ist in Schritt **212** (siehe **Fig. 2**) enthalten.

[0081] Als Reaktion auf das Feststellen in Schritt **365**, dass die Datenbankinstanz(en) gestartet wurde(n) und läuft/laufen, leitet die Sicherheitsintegrationsschicht **104** (siehe **Fig. 1**) in Schritt **366** die Abfolge **S1A5** ein und fährt die Datenbankinstanz(en) herunter. Als Reaktion auf das Feststellen in Schritt **365**, dass die Datenbankinstanz(en) gestartet wurde (n) und läuft/laufen, leitet die Sicherheitsintegrationsschicht **104** (siehe **Fig. 1**) in Schritt **367** die Abfolge **S1A6** ein und lässt das Abschließen des Ausführens des Befehls zu, was dazu führt, dass das IT-System heruntergefahren wird. Schritt **367** ist in Schritt **214** (siehe **Fig. 2**) enthalten.

[0082] Zurück zu Schritt **365**, wenn die Sicherheitsintegrationsschicht **104** (siehe **Fig. 1**) feststellt, dass keine Datenbankinstanz gestartet wurde und läuft, wird der Nein-Verzweigung von Schritt **365** gefolgt, und Schritt **367** wird durchgeführt, wodurch das Ab-

schließen des Ausführens des Befehls zugelassen wird, was dazu führt, dass das IT-System heruntergefahren wird.

[0083] Zurück zu Schritt **352** in **Fig. 3B**, wenn die Sicherheitsintegrationsschicht **104** (siehe **Fig. 1**) feststellt, dass der Befehl in der vorkonfigurierten Liste von Befehlen nicht gefunden wurde, die in der Prozessregistrierdatenbank **110** (siehe **Fig. 3A)** enthalten sind, wird Schritt **368** in **Fig. 3B** durchgeführt. In Schritt **368** überträgt die Sicherheitsintegrationsschicht **104** (siehe **Fig. 1**) die Steuerung über den Befehl an das Betriebssystem des IT-Systems, und in Schritt **367** lässt die Sicherheitsintegrationsschicht **104** (siehe **Fig. 1**) das Abschließen des Ausführens des Befehls zu.

[0084] Obwohl der Prozess in den **Fig. 3B** bis **Fig. 3C** als Beispiel dargestellt ist, stellen die Logik und die Schritte in dem Prozess in den **Fig. 3B** bis **Fig. 3C** eine Ausführungsform der vorliegenden Erfindung dar.

COMPUTERSYSTEM

[0085] Fig. 4 ist ein Blockschaubild eines Computers, der in dem System aus **Fig. 1** enthalten ist und den Prozess aus **Fig. 2** umsetzt, gemäß Ausführungsformen der vorliegenden Erfindung. Bei dem Computer **102** handelt es sich um ein Computersystem, das im Allgemeinen eine zentrale Verarbeitungseinheit (CPU) **402**, einen Hauptspeicher **404**, eine Eingabe/Ausgabe-(E/A-) Schnittstelle **406** und einen Bus **408** umfasst. Darüber hinaus ist der Computer **102** mit E/A-Einheiten **410** und einer Computer-Datenspeichereinheit **412** verbunden. Die CPU **402** führt Berechnungs- und Steuerfunktionen des Computers **102** durch, darunter das Ausführen von in dem Programmcode **414** enthaltenen Anweisungen für die Sicherheitsintegrationsschicht **104** (siehe **Fig. 1**) zum Durchführen eines Verfahrens zum Bereitstellen eines konfigurationsabhängigen Arbeitsablaufs in einem IT-System, wobei die Anweisungen von der CPU **402** über den Hauptspeicher **404** ausgeführt werden. Die CPU **402** kann eine einzelne Verarbeitungseinheit umfassen oder auf eine oder mehrere Verarbeitungseinheiten an einem oder mehreren Orten verteilt sein (z.B. auf einem Client und einem Server).

[0086] Der Hauptspeicher **404** umfasst ein bekanntes durch einen Computer lesbares Speichermedium, das nachfolgend beschrieben ist. In einer Ausführungsform stellen Cachespeicherelemente des Hauptspeichers **404** eine vorübergehende Speicherung von zumindest etwas Programmcode (z.B. des Programmcodes **414**) bereit, um die Häufigkeit zu verringern, mit der Code von dem Massenspeicher abgerufen werden muss, während Anweisungen des Programmcodes ausgeführt werden. Außerdem kann sich der Hauptspeicher **404** ähnlich wie die CPU **402** an einem einzigen physikalischen Ort befinden, darunter eine oder mehrere Typen von Datenspeicher, oder er kann auf eine Vielzahl von physikalischen Systemen in verschiedenen Formen verteilt sein. Darüber hinaus kann der Hauptspeicher **404** Daten umfassen, die zum Beispiel über ein lokales Netzwerk (LAN) oder ein Weitverkehrsnetz (WAN) verteilt sind.

[0087] Die E/A-Schnittstelle **406** umfasst ein beliebiges System zum Austauschen von Informationen zu oder von einer externen Quelle. Die E/A-Einheiten **410** enthalten einen beliebigen Typ externer Einheit, darunter eine Anzeige, eine Tastatur, usw. Der Bus **408** stellt eine Datenübertragungsverbindung zwischen jeder der Komponenten in dem Computer **102** bereit und kann jeden Typ von Übertragungsverbindung umfassen, darunter elektrisch, optisch, drahtlos usw.

[0088] Die E/A-Schnittstelle **406** ermöglicht es dem Computer **102** auch, Informationen (z.B. Daten oder Programmanweisungen wie zum Beispiel den Programmcode **414**) auf der Computer-Datenspeichereinheit **412** oder einer anderen Computer-Datenspeichereinheit (nicht gezeigt) zu speichern oder davon abzurufen. Die Computer-Datenspeichereinheit **412** umfasst ein bekanntes durch einen Computer lesbares Speichermedium, das nachfolgend beschrieben ist. In einer Ausführungsform handelt es sich bei der Computer-Datenspeichereinheit **412** um eine nichtflüchtige Datenspeichereinheit, wie zum Beispiel ein Magnetplattenlaufwerk (d.h. ein Festplattenlaufwerk) oder ein optisches Plattenlaufwerk (z.B. ein CD-ROM-Laufwerk, das eine CD-ROM-Scheibe aufnimmt).

[0089] Der Hauptspeicher **404** und/oder die Speichereinheit **412** können Computerprogrammcode **414** speichern, der Anweisungen umfasst, die von der CPU **402** über den Hauptspeicher **404** ausgeführt werden, um einen konfigurationsabhängigen Arbeitsablauf in einem IT-System bereitzustellen. Auch wenn **Fig. 4** den Hauptspeicher **404** als Programmcode umfassend darstellt, sieht die vorliegende Erfindung Ausführungsformen vor, bei denen der Hauptspeicher **404** nicht den gesamten Code **414** gleichzeitig umfasst, sondern stattdessen jeweils nur einen Teil des Codes **414**.

[0090] Darüber hinaus kann der Hauptspeicher **404** ein Betriebssystem (nicht gezeigt) und andere Systeme umfassen, die nicht in **Fig. 4** gezeigt sind.

[0091] Die Speichereinheit **412** und/oder eine oder mehrere andere Computer-Datenspeichereinheiten (nicht gezeigt), die mit dem Computer **102** verbunden sind, können Parameter und vorkonfigurierte Bedingungen umfassen, welche die Grundlagen von Aktio-

nen zur Gültigkeitsprüfung mit dem Befehl **120-1**, ..., Befehl **120-N** (siehe **Fig. 1**) bilden.

[0092] Der Fachmann wird verstehen, dass es sich bei der vorliegenden Erfindung in einer ersten Ausführungsform um ein Verfahren handeln kann, es sich in einer zweiten Ausführungsform bei der vorliegenden Erfindung um ein System handeln kann, und es sich in einer dritten Ausführungsform bei der vorliegenden Erfindung um ein Computerprogrammprodukt handeln kann.

[0093] Jede beliebige der Komponenten einer Ausführungsform der vorliegenden Erfindung kann durch einen Dienstanbieter eingesetzt, verwaltet, betreut usw. werden, der anbietet, eine Datenverarbeitungsinfrastruktur im Hinblick auf das Bereitstellen eines konfigurationsabhängigen Arbeitsablaufs in einem IT-System einzusetzen oder zu integrieren. Folglich offenbart eine Ausführungsform der vorliegenden Erfindung einen Prozess zum Unterstützen einer Computerinfrastruktur, wobei der Prozess das Bereitstellen von mindestens einem unterstützenden Dienst entweder für das Integrieren, das Bereitstellen per Hosting und/oder das Pflegen und Einsetzen von durch einen Computer lesbarem Code (z.B. Programmcode **414**) in einem Computersystem (z.B. dem Computer **102**) aufweist, das einen oder mehrere Prozessoren (z.B. die CPU **402**) umfasst, wobei der/die Prozessor(en) Anweisungen ausführt bzw. ausführen, die in dem Code enthalten sind und das Computersystem dazu veranlassen, einen konfigurationsabhängigen Arbeitsablauf in einem IT-System bereitzustellen. Eine andere Ausführungsform offenbart einen Prozess zum Unterstützen einer Computerinfrastruktur, wobei der Prozess das Integrieren von durch einen Computer lesbarem Programmcode in ein einen Prozessor enthaltenden Computersystem umfasst. Der Schritt des Integrierens umfasst das Speichern des Programmcodes in einer durch einen Computer lesbaren Speichereinheit des Computersystems durch Verwendung des Prozessors. Der Programmcode setzt ein Verfahren zum Bereitstellen eines konfigurationsabhängigen Arbeitsablaufs in einem IT-System bereit, wenn er durch den Prozessor ausgeführt wird.

[0094] Es versteht sich zwar, dass der Programmcode **414** zum Bereitstellen eines konfigurationsabhängigen Arbeitsablaufs in einem IT-System durch manuelles Laden direkt in die Client-, Server- und Proxy-Computer (nicht gezeigt) über das Laden eines durch einen Computer lesbaren Speichermediums (z.B. die Computer-Datenspeichereinheit **412**) bereitgestellt werden kann, der Programmcode **414** jedoch auch automatisch oder halbautomatisch in den Computer **102** durch Senden des Programmcodes **414** an einen zentralen Server oder eine Gruppe von zentralen Servern bereitgestellt werden kann. Der Programmcode **414** wird dann auf Client-Computer (z.B. den Computer **102**) heruntergeladen, welche den Programmcode **414** ausführen. Alternativ wird der Programmcode **414** direkt per eMail an den Client-Computer gesendet. Der Programmcode **414** wird dann entweder in ein Verzeichnis auf dem Client-Computer abgetrennt oder direkt in ein Verzeichnis auf dem Client-Computer geladen, und zwar durch eine Schaltfläche in der eMail, die ein Programm ausführt, das den Programmcode **414** in ein Verzeichnis abtrennt. Eine andere Alternative besteht darin, den Programmcode **414** direkt an ein Verzeichnis auf der Festplatte des Client-Computers zu senden. Wenn es Proxy-Server gibt, wählt der Prozess den Proxy-Server-Code aus, bestimmt, auf welchen Computern der Code der Proxy-Server platziert werden soll, überträgt den Proxy-Server-Code und installiert dann den Proxy-Server-Code auf dem Proxy-Computer. Der Programmcode **414** wird an den Proxy-Server übertragen und dann auf dem Proxy-Server gespeichert.

[0095] Eine andere Ausführungsform der Erfindung stellt ein Verfahren bereit, das die Prozessschritte auf der Grundlage eines Abonnements, einer Werbung und/oder einer Gebühr durchführt. Das heißt, ein Dienstanbieter, wie zum Beispiel ein Lösungsintegrator, kann anbieten, einen Prozess zum Bereitstellen eines konfigurationsabhängigen Arbeitsablaufs in einem IT-System zu erstellen, zu warten, zu unterstützen, usw. In diesem Fall kann der Dienstanbieter eine Computerinfrastruktur erzeugen, pflegen, unterstützen usw., welche die Prozessschritte für einen oder mehrere Kunden durchführt. Im Gegenzug kann der Dienstanbieter im Rahmen eines Abonnements und/oder einer Gebührenvereinbarung eine Zahlung von dem/den Kunden erhalten, und/oder der Dienstanbieter kann eine Zahlung aus dem Verkauf von Werumfassen an einen oder mehrere Dritte erhalten.

[0096] Bei der vorliegenden Erfindung kann es sich um ein System, ein Verfahren und/oder ein Computerprogrammprodukt auf jedem möglichen technischen Detaillierungsgrad der Integration handeln. Das Computerprogrammprodukt kann (ein) durch einen Computer lesbare(s) Speichermedium (oder -medien) (d.h. den Hauptspeicher **404** und die Computer-Datenspeichereinheit **412**) umfassen, auf dem/denen durch einen Computer lesbare Programmanweisungen **414** gespeichert ist/sind, um einen Prozessor (z.B. die CPU **402**) dazu zu veranlassen, Aspekte der vorliegenden Erfindung auszuführen.

[0097] Bei dem durch einen Computer lesbaren Speichermedium kann es sich um eine physische Einheit handeln, die Anweisungen (z.B. den Programmcode **414**) zur Verwendung durch eine Einheit zur Ausführung von Anweisungen (z.B. den Computer **102**) behalten und speichern kann. Bei dem durch einen Computer lesbaren Speichermedium kann es sich zum Beispiel um eine elektronische Speicher-

einheit, eine magnetische Speichereinheit, eine optische Speichereinheit, eine elektromagnetische Speichereinheit, eine Halbleiterspeichereinheit oder jede geeignete Kombination daraus handeln, ohne auf diese beschränkt zu sein. Zu einer nicht erschöpfenden Liste spezifischerer Beispiele des durch einen Computer lesbaren Speichermediums gehören die Folgenden: eine tragbare Computerdiskette, eine Festplatte, ein Direktzugriffsspeicher (RAM), ein Nur-Lese-Speicher (ROM), ein löschbarer programmierbarer Nur-Lese-Speicher (EPROM bzw. Flash-Speicher), ein statischer Direktzugriffsspeicher (SRAM), ein tragbarer Kompaktspeicherplatte-Nur-Lese-Speicher (CD-ROM), eine DVD (digital versatile disc), ein Speicher-Stick, eine Diskette, eine mechanisch kodierte Einheit wie zum Beispiel Lochkarten oder gehobene Strukturen in einer Rille, auf denen Anweisungen gespeichert sind, und jede geeignete Kombination daraus. Ein durch einen Computer lesbares Speichermedium soll in der Verwendung hierin nicht als flüchtige Signale an sich aufgefasst werden, wie zum Beispiel Funkwellen oder andere sich frei ausbreitende elektromagnetische Wellen, elektromagnetische Wellen, die sich durch einen Wellenleiter oder ein anderes Übertragungsmedium ausbreiten (z.B. durch ein Glasfaserkabel geleitete Lichtimpulse) oder durch einen Draht übertragene elektrische Signale.

[0098] Hierin beschriebene, durch einen Computer lesbare Programmanweisungen (z.B. der Programmcode **414**) können von einem durch einen Computer lesbaren Speichermedium auf jeweilige Datenverarbeitungs-/Verarbeitungseinheiten (z.B. den Computer **102**) oder über ein Netzwerk (nicht gezeigt) wie zum Beispiel das Internet, ein lokales Netzwerk, ein Weitverkehrsnetz und/oder ein drahtloses Netzwerk auf einen externen Computer oder eine externe Speichereinheit (z.B. die Computer-Datenspeichereinheit **412**) heruntergeladen werden. Das Netzwerk kann Kupferübertragungskabel, Lichtwellenübertragungsleiter, drahtlose Übertragung, Leitwegrechner, Firewalls, Vermittlungseinheiten, Gateway-Computer und/oder Edge-Server aufweisen. Eine Netzwerkadapterkarte (nicht gezeigt) oder Netzwerkschnittstelle (nicht gezeigt) in jeder Datenverarbeitungs-/Verarbeitungseinheit empfängt durch einen Computer lesbare Programmanweisungen aus dem Netzwerk und leitet die durch einen Computer lesbaren Programmanweisungen zur Speicherung in einem durch einen Computer lesbaren Speichermedium innerhalb der entsprechenden Datenverarbeitungs-/Verarbeitungseinheit weiter.

[0099] Bei durch einen Computer lesbaren Programmanweisungen (z.B. dem Programmcode **414**) zum Ausführen von Arbeitsschritten der vorliegenden Erfindung kann es sich um Assembler-Anweisungen, ISA-Anweisungen (Instruction-Set-Architecture), Maschinenanweisungen, maschinenabhängige Anweisungen, Mikrocode, Firmware-Anweisungen, zustandssetzende Daten, Konfigurationsdaten für integrierte Schaltungen oder entweder Quellcode oder Objektcode handeln, die in einer beliebigen Kombination aus einer oder mehreren Programmiersprachen geschrieben werden, darunter objektorientierte Programmiersprachen wie Smalltalk, C++ o.ä. sowie herkömmliche prozedurale Programmiersprachen wie die Programmiersprache „C“ oder ähnliche Programmiersprachen. Die durch einen Computer lesbaren Programmanweisungen können vollständig auf dem Computer des Benutzers, teilweise auf dem Computer des Benutzers, als eigenständiges Software-Paket, teilweise auf dem Computer des Benutzers und teilweise auf einem fernen Computer oder vollständig auf dem fernen Computer oder Server ausgeführt werden. In letzterem Fall kann der entfernt angeordnete Computer mit dem Computer des Benutzers durch eine beliebige Art Netzwerk verbunden sein, darunter ein lokales Netzwerk (LAN) oder ein Weitverkehrsnetz (WAN), oder die Verbindung kann mit einem externen Computer hergestellt werden (zum Beispiel über das Internet unter Verwendung eines Internet-Dienstanbieters). In einigen Ausführungsformen können elektronische Schaltungen, darunter zum Beispiel programmierbare Logikschaltungen, im Feld programmierbare Gatter-Anordnungen (FPGA, field programmable gate arrays) oder programmierbare Logikanordnungen (PLA, programmable logic arrays) die durch einen Computer lesbaren Programmanweisungen ausführen, indem sie Zustandsinformationen der durch einen Computer lesbaren Programmanweisungen nutzen, um die elektronischen Schaltungen zu personalisieren, um Aspekte der vorliegenden Erfindung durchzuführen.

[0100] Aspekte der vorliegenden Erfindung sind hierin unter Bezugnahme auf Ablaufpläne (z.B. **Fig. 2**) und/oder Blockschaltbilder bzw. Schaubilder (z.B. **Fig. 1** und **Fig. 4**) von Verfahren, Vorrichtungen (Systemen) und Computerprogrammprodukten gemäß Ausführungsformen der Erfindung beschrieben. Es wird darauf hingewiesen, dass jeder Block der Ablaufpläne und/oder der Blockschaltbilder bzw. Schaubilder sowie Kombinationen von Blöcken in den Ablaufplänen und/oder den Blockschaltbildern bzw. Schaubildern mittels durch einen Computer lesbare Programmanweisungen (z.B. den Programmcode **414**) ausgeführt werden können.

[0101] Diese durch einen Computer lesbaren Programmanweisungen können einem Prozessor (z.B. der CPU **402**) eines Universalcomputers, eines Spezialcomputers oder einer anderen programmierbaren Datenverarbeitungsvorrichtung (z.B. des Computers **102**) bereitgestellt werden, um eine Maschine zu erzeugen, so dass die über den Prozessor des Computers bzw. der anderen programmierbaren Datenverarbeitungsvorrichtung ausgeführten Anweisungen ein Mittel zur Umsetzung der in dem Block bzw. den Blöcken der Ablaufpläne und/oder

der Blockschaltbilder bzw. Schaubilder festgelegten Funktionen/Schritte erzeugen. Diese durch einen Computer lesbaren Programmanweisungen können auch auf einem durch einen Computer lesbaren Speichermedium (z.B. auf der Computer-Datenspeichereinheit **412**) gespeichert sein, das einen Computer, eine programmierbare Datenverarbeitungsvorrichtung und/oder andere Einheiten so steuern kann, dass sie auf eine bestimmte Art funktionieren, so dass das durch einen Computer lesbare Speichermedium, auf dem Anweisungen gespeichert sind, ein Herstellungsprodukt aufweist, darunter Anweisungen, welche Aspekte der/des in dem Block bzw. den Blöcken des Ablaufplans und/oder der Blockschaltbilder bzw. Schaubilder angegebenen Funktion/Schritts umsetzen.

[0102] Die durch einen Computer lesbaren Programmanweisungen (z.B. der Programmcode **414**) können auch auf einen Computer (z.B. den Computer **102**), eine andere programmierbare Datenverarbeitungsvorrichtung oder eine andere Einheit geladen werden, um das Ausführen einer Reihe von Prozessschritten auf dem Computer bzw. der anderen programmierbaren Vorrichtung oder anderen Einheit zu verursachen, um einen auf einem Computer ausgeführten Prozess zu erzeugen, so dass die auf dem Computer, einer anderen programmierbaren Vorrichtung oder einer anderen Einheit ausgeführten Anweisungen die in dem Block bzw. den Blöcken der Ablaufpläne und/oder der Blockschaltbilder bzw. Schaubilder festgelegten Funktionen/Schritte umsetzen.

[0103] Die Ablaufpläne und die Blockschaltbilder bzw. Schaubilder in den Figuren veranschaulichen die Architektur, die Funktionalität und den Betrieb möglicher Ausführungen von Systemen, Verfahren und Computerprogrammprodukten gemäß verschiedenen Ausführungsformen der vorliegenden Erfindung. In diesem Zusammenhang kann jeder Block in den Ablaufplänen oder Blockschaltbildern bzw. Schaubildern ein Modul, ein Segment oder einen Teil von Anweisungen darstellen, die eine oder mehrere ausführbare Anweisungen zur Ausführung der bestimmten logischen Funktion(en) aufweisen. In einigen alternativen Ausführungen können die in dem Block angegebenen Funktionen in einer anderen Reihenfolge als in den Figuren gezeigt stattfinden. Zwei nacheinander gezeigte Blöcke können zum Beispiel in Wirklichkeit im Wesentlichen gleichzeitig ausgeführt werden, oder die Blöcke können manchmal je nach entsprechender Funktionalität in umgekehrter Reihenfolge ausgeführt werden. Es ist ferner anzumerken, dass jeder Block der Blockschaltbilder bzw. Schaubilder und/oder der Ablaufpläne sowie Kombinationen aus Blöcken in den Blockschaltbildern bzw. Schaubildern und/oder den Ablaufplänen durch spezielle auf Hardware beruhende Systeme umgesetzt werden können, welche die festgelegten Funktionen oder Schritte durchführen, oder Kombinationen aus Spezial-Hardware und Computeranweisungen ausführen.

[0104] Obwohl Ausführungsformen der vorliegenden Erfindung hierin der Veranschaulichung halber beschrieben wurden, werden für den Fachmann viele Abänderungen und Änderungen ersichtlich sein. Dementsprechend sollen die beigefügten Ansprüche alle derartigen Abänderungen und Änderungen umfassen, die in den wahren Sinngehalt und Umfang dieser Erfindung fallen.

Patentansprüche

1. Verfahren zum Bereitstellen eines konfigurationsabhängigen Arbeitsablaufs in einem IT-System, wobei das Verfahren die folgenden Schritte aufweist:
Erkennen durch einen Computer, dass ein Befehl in einer Liste von Befehlen enthalten ist, wobei der Befehl zum Ausführen eingeleitet wird;
als Reaktion auf den Schritt des Erkennens des Befehls, Ermitteln eines Satzes von Parametern und von vorkonfigurierten Bedingungen, die dem erkannten Befehl zugehörig sind, durch den Computer;
beruhend auf dem Satz von Parametern und den vorkonfigurierten Bedingungen, Ermitteln einer oder mehrerer Aktionen zur Gültigkeitsprüfung, die den Befehl auf Gültigkeit prüfen und in dem konfigurationsabhängigen Arbeitsablauf enthalten sind, durch den Computer, wobei die eine oder mehreren Aktionen zur Gültigkeitsprüfung jeweils durch eine oder mehrere Interaktionen mit einem oder mehreren externen Systemen festgelegt werden;
Durchführen der einen oder mehreren Aktionen zur Gültigkeitsprüfung, die in dem konfigurationsabhängigen Arbeitsablauf enthalten sind, durch den Computer, indem die eine oder mehreren Interaktionen mit dem einen oder den mehreren externen Systemen unter Verwendung des Satzes von Parametern ausgeführt werden;
Ermitteln durch den Computer, ob die eine oder mehreren Aktionen zur Gültigkeitsprüfung erfolgreich abgeschlossen werden; und
wenn die eine oder mehreren Aktionen zur Gültigkeitsprüfung erfolgreich abgeschlossen werden, Fortfahren mit dem Ausführen des Befehls durch den Computer, oder, wenn mindestens eine der einen oder mehreren Aktionen zur Gültigkeitsprüfung nicht erfolgreich abgeschlossen wird, Abbrechen des Ausführens des Befehls durch den Computer.

2. Verfahren nach Anspruch 1, darüber hinaus aufweisend den Schritt des Durchführens einer oder mehrerer zusätzlicher Aktionen durch den Computer neben dem Schritt des Abbrechens des Ausführens des Befehls, wenn eine Aktion zur Gültigkeitsprüfung, die in der einen oder den mehreren Aktionen zur Gültigkeitsprüfung enthalten ist, nicht erfolgreich abgeschlossen wird, wobei der Schritt des Durchführens der einen oder mehreren zusätzlichen Aktionen das

Senden einer Benachrichtigung umfasst, die angibt, dass die Aktion zur Gültigkeitsprüfung nicht erfolgreich abgeschlossen wurde.

3. Verfahren nach Anspruch 1, darüber hinaus aufweisend den Schritt des Durchführens einer oder mehrerer zusätzlicher Aktionen durch den Computer neben dem Schritt des Fortführens des Ausführens des Befehls, wenn eine Aktion zur Gültigkeitsprüfung, die in der einen oder den mehreren Aktionen zur Gültigkeitsprüfung enthalten ist, erfolgreich abgeschlossen wird.

4. Verfahren nach Anspruch 1, wobei der Schritt des Ausführens der einen oder mehreren Interaktionen mit einem oder mehreren externen Systemen das Ausführen einer Interaktion mit einem externen System umfasst, das aus der Gruppe ausgewählt ist, die aus einem Konfigurationsverwaltungsdatenbank-System, einem Ticketsystem, einem Auftragsablauf-Steuerungssystem, einem Arbeitslast-Automatisierungssystem und einem Betriebsverwaltungssystem besteht.

5. Verfahren nach Anspruch 1, wobei der Schritt des Durchführens der einen oder mehreren Aktionen zur Gültigkeitsprüfung das Prüfen des Befehls auf Gültigkeit anhand von mehreren lokalen Sicherheitsrichtlinien und Richtlinien externer Systeme umfasst, bei denen es sich um an das IT-System angeschlossene Systeme handelt.

6. Verfahren nach Anspruch 1, darüber hinaus aufweisend den Schritt des Empfangens des Befehls durch den Computer (i) von einem Software-Werkzeug unter Verwendung einer API-Verbindung (Schnittstelle zur Anwendungsprogrammierung), (ii) als Teil eines in dem IT-System ausgeführten Auftrags, wobei der Auftrag von einem zeitabhängigen Auftragsablauf-Steuerprogramm geplant wird, oder (iii) von einem Software-Agenten vor dem Schritt des Erkennens des Befehls.

7. Verfahren nach Anspruch 1, darüber hinaus aufweisend den Schritt des Empfangens des Befehls durch den Computer von einem Betriebssystem oder Teilsystem des Betriebssystems vor dem Schritt des Erkennens des Befehls.

8. Verfahren nach Anspruch 1, darüber hinaus aufweisend das Erzeugen der Liste von Befehlen durch den Computer, wobei die Befehle jeweilige kritische Aktivitäten des IT-Systems durchführen, wobei mindestens einer der Befehle eine Aktion durchführt, die schädlich für das IT-System ist.

9. Verfahren nach Anspruch 1, darüber hinaus aufweisend den Schritt des:
Bereitstellens von zumindest einem Unterstützungsdienst für zumindest entweder das Erstellen, das Integrieren, das Bereitstellen per Hosting, das Pflegen und/oder das Einsetzen von durch einen Computer lesbarem Programmcode in dem Computer, wobei der Programmcode von einem Prozessor des Computers ausgeführt wird, um die Schritte des Erkennens des Befehls, des Ermittelns des Satzes von Parametern und der vorkonfigurierten Bedingungen, des Ermittelns der einen oder mehreren Aktionen zur Gültigkeitsprüfung, des Durchführens der einen oder mehreren Aktionen zur Gültigkeitsprüfung, des Ausführens der einen oder mehreren Interaktionen mit dem einen oder den mehreren externen Systemen unter Verwendung des Satzes von Parametern, des Ermittelns, ob die eine oder mehreren Aktionen zur Gültigkeitsprüfung erfolgreich abgeschlossen werden, und des Fortführens des Ausführens des Befehls, wenn die eine oder mehreren Aktionen zur Gültigkeitsprüfung erfolgreich abgeschlossen werden, oder des Abbrechens des Befehls, wenn eine der einen oder mehreren Aktionen zur Gültigkeitsprüfung nicht erfolgreich abgeschlossen werden, umzusetzen.

10. Computerprogrammprodukt, aufweisend:
ein durch einen Computer lesbares Speichermedium und einen durch einen Computer lesbaren Programmcode, der in dem durch einen Computer lesbaren Speichermedium gespeichert ist, wobei der durch einen Computer lesbare Programmcode Anweisungen umfasst, die von einer zentralen Verarbeitungseinheit (CPU) eines Computersystems ausgeführt werden, um ein Verfahren zum Bereitstellen eines konfigurationsabhängigen Arbeitsablaufs in einem IT-System umzusetzen, wobei das Verfahren die folgenden Schritte aufweist:
Erkennen durch das Computersystem, dass ein Befehl in einer Liste von Befehlen enthalten ist, wobei der Befehl zum Ausführen eingeleitet wird;
als Reaktion auf den Schritt des Erkennens des Befehls, Ermitteln eines Satzes von Parametern und von vorkonfigurierten Bedingungen, die dem erkannten Befehl zugehörig sind, durch das Computersystem;
beruhend auf dem Satz von Parametern und den vorkonfigurierten Bedingungen, Ermitteln einer oder mehrerer Aktionen zur Gültigkeitsprüfung, die den Befehl auf Gültigkeit prüfen und in dem konfigurationsabhängigen Arbeitsablauf enthalten sind, durch das Computersystem, wobei die eine oder mehreren Aktionen zur Gültigkeitsprüfung jeweils durch eine oder mehrere Interaktionen mit einem oder mehreren externen Systemen festgelegt werden;
Durchführen der einen oder mehreren Aktionen zur Gültigkeitsprüfung, die in dem konfigurationsabhängigen Arbeitsablauf enthalten sind, durch das Computersystem, indem die eine oder mehreren Interaktionen mit dem einen oder den mehreren externen Systemen unter Verwendung des Satzes von Parametern ausgeführt werden;

Ermitteln durch das Computersystem, ob die eine oder mehreren Aktionen zur Gültigkeitsprüfung erfolgreich abgeschlossen werden; und
wenn die eine oder mehreren Aktionen zur Gültigkeitsprüfung erfolgreich abgeschlossen werden, Fortfahren mit dem Ausführen des Befehls durch das Computersystem, oder, wenn mindestens eine der einen oder mehreren Aktionen zur Gültigkeitsprüfung nicht erfolgreich abgeschlossen wird, Abbrechen des Ausführens des Befehls durch das Computersystem.

11. Computerprogrammprodukt nach Anspruch 10, wobei das Verfahren darüber hinaus den Schritt des Durchführens einer oder mehrerer zusätzlicher Aktionen durch das Computersystem neben dem Schritt des Abbrechens des Ausführens des Befehls aufweist, wenn eine Aktion zur Gültigkeitsprüfung, die in der einen oder den mehreren Aktionen zur Gültigkeitsprüfung enthalten ist, nicht erfolgreich abgeschlossen wird, wobei der Schritt des Durchführens der einen oder mehreren zusätzlichen Aktionen das Senden einer Benachrichtigung umfasst, die angibt, dass die Aktion zur Gültigkeitsprüfung nicht erfolgreich abgeschlossen wurde.

12. Computerprogrammprodukt nach Anspruch 10, wobei das Verfahren darüber hinaus den Schritt des Durchführens einer oder mehrerer zusätzlicher Aktionen durch das Computersystem neben dem Schritt des Fortführens des Ausführens des Befehls aufweist, wenn eine Aktion zur Gültigkeitsprüfung, die in der einen oder den mehreren Aktionen zur Gültigkeitsprüfung enthalten ist, erfolgreich abgeschlossen wird.

13. Computerprogrammprodukt nach Anspruch 10, wobei der Schritt des Ausführens der einen oder mehreren Interaktionen mit einem oder mehreren externen Systemen das Ausführen einer Interaktion mit einem externen System umfasst, das aus der Gruppe ausgewählt ist, die aus einem Konfigurationsverwaltungsdatenbank-System, einem Ticketsystem, einem Auftragsablauf-Steuerungssystem, einem Arbeitslast-Automatisierungssystem und einem Betriebsverwaltungssystem besteht.

14. Computerprogrammprodukt nach Anspruch 10, wobei der Schritt des Durchführens der einen oder mehreren Aktionen zur Gültigkeitsprüfung das Prüfen des Befehls auf Gültigkeit anhand von mehreren lokalen Sicherheitsrichtlinien und Richtlinien externer Systeme umfasst, bei denen es sich um an das IT-System angeschlossene Systeme handelt.

15. Computerprogrammprodukt nach Anspruch 10, wobei das Verfahren darüber hinaus vor dem Schritt des Erkennens des Befehls den Schritt des Empfangens des Befehls durch das Computersystem (i) von einem Software-Werkzeug unter Verwendung einer API-Verbindung (Schnittstelle zur Anwendungsprogrammierung), (ii) als Teil eines in dem IT-System ausgeführten Auftrags, wobei der Auftrag von einem zeitabhängigen Auftragsablauf-Steuerprogramm geplant wird, oder (iii) von einem Software-Agenten aufweist.

16. Computerprogrammprodukt nach Anspruch 10, wobei das Verfahren darüber hinaus vor dem Schritt des Erkennens des Befehls den Schritt des Empfangens des Befehls durch den Computer von einem Betriebssystem oder Teilsystem des Betriebssystems aufweist.

17. Computerprogrammprodukt nach Anspruch 10, wobei das Verfahren darüber hinaus das Erzeugen der Liste von Befehlen durch das Computersystem aufweist, wobei die Befehle jeweilige kritische Aktivitäten des IT-Systems durchführen, wobei mindestens einer der Befehle eine Aktion durchführt, die schädlich für das IT-System ist.

18. Computersystem, aufweisend:
eine zentrale Verarbeitungseinheit (CPU);
einen mit der CPU verbundenen Hauptspeicher; und ein durch einen Computer lesbares Speichermedium, das mit der CPU verbunden ist, wobei das durch einen Computer lesbare Speichermedium Anweisungen umfasst, die von der CPU über den Hauptspeicher ausgeführt werden, um ein Verfahren zum Bereitstellen eines konfigurationsabhängigen Arbeitsablaufs in einem IT-System umzusetzen, wobei das Verfahren die folgenden Schritte aufweist:
Erkennen durch das Computersystem, dass ein Befehl in einer Liste von Befehlen enthalten ist, wobei der Befehl zum Ausführen eingeleitet wird;
als Reaktion auf den Schritt des Erkennens des Befehls, Ermitteln eines Satzes von Parametern und von vorkonfigurierten Bedingungen, die dem erkannten Befehl zugehörig sind, durch das Computersystem;
beruhend auf dem Satz von Parametern und den vorkonfigurierten Bedingungen, Ermitteln einer oder mehrerer Aktionen zur Gültigkeitsprüfung, die den Befehl auf Gültigkeit prüfen und in dem konfigurationsabhängigen Arbeitsablauf enthalten sind, durch das Computersystem, wobei die eine oder mehreren Aktionen zur Gültigkeitsprüfung jeweils durch eine oder mehrere Interaktionen mit einem oder mehreren externen Systemen festgelegt werden;
Durchführen der einen oder mehreren Aktionen zur Gültigkeitsprüfung, die in dem konfigurationsabhängigen Arbeitsablauf enthalten sind, durch das Computersystem, indem die eine oder mehreren Interaktionen mit dem einen oder den mehreren externen Systemen unter Verwendung des Satzes von Parametern ausgeführt werden;
Ermitteln durch das Computersystem, ob die eine oder mehreren Aktionen zur Gültigkeitsprüfung erfolgreich abgeschlossen werden; und
wenn die eine oder mehreren Aktionen zur Gültigkeitsprüfung erfolgreich abgeschlossen werden, Fort-

fahren mit dem Ausführen des Befehls durch das Computersystem, oder, wenn mindestens eine der einen oder mehreren Aktionen zur Gültigkeitsprüfung nicht erfolgreich abgeschlossen wird, Abbrechen des Ausführens des Befehls durch das Computersystem.

19. Computersystemnach Anspruch 18, wobei das Verfahren darüber hinaus den Schritt des Durchführens einer oder mehrerer zusätzlicher Aktionen durch das Computersystem neben dem Schritt des Abbrechens des Ausführens des Befehls aufweist, wenn eine Aktion zur Gültigkeitsprüfung, die in der einen oder den mehreren Aktionen zur Gültigkeitsprüfung enthalten ist, nicht erfolgreich abgeschlossen wird, wobei der Schritt des Durchführens der einen oder mehreren zusätzlichen Aktionen das Senden einer Benachrichtigung umfasst, die angibt, dass die Aktion zur Gültigkeitsprüfung nicht erfolgreich abgeschlossen wurde.

20. Computersystem nach Anspruch 18, wobei das Verfahren darüber hinaus den Schritt des Durchführens einer oder mehrerer zusätzlicher Aktionen durch das Computersystem neben dem Schritt des Fortführens des Ausführens des Befehls aufweist, wenn eine Aktion zur Gültigkeitsprüfung, die in der einen oder den mehreren Aktionen zur Gültigkeitsprüfung enthalten ist, erfolgreich abgeschlossen wird.

21. Computersystem nach Anspruch 18, wobei der Schritt des Ausführens der einen oder mehreren Interaktionen mit einem oder mehreren externen Systemen das Ausführen einer Interaktion mit einem externen System umfasst, das aus der Gruppe ausgewählt ist, die aus einem Konfigurationsverwaltungsdatenbank-System, einem Ticketsystem, einem Auftragsablauf-Steuerungssystem, einem Arbeitslast-Automatisierungssystem und einem Betriebsverwaltungssystem besteht.

22. Computersystem nach Anspruch 18, wobei der Schritt des Durchführens der einen oder mehreren Aktionen zur Gültigkeitsprüfung das Prüfen des Befehls auf Gültigkeit anhand von mehreren lokalen Sicherheitsrichtlinien und Richtlinien externer Systeme umfasst, bei denen es sich um an das IT-System angeschlossene Systeme handelt.

23. Computersystem nach Anspruch 18, wobei das Verfahren darüber hinaus vor dem Schritt des Erkennens des Befehls den Schritt des Empfangens des Befehls durch das Computersystem (i) von einem Software-Werkzeug unter Verwendung einer API-Verbindung (Schnittstelle zur Anwendungsprogrammierung), (ii) als Teil eines in dem IT-System ausgeführten Auftrags, wobei der Auftrag von einem zeitabhängigen Auftragsablauf-Steuerprogramm geplant wird, oder (iii) von einem Software-Agenten aufweist.

24. Verfahren zum Bereitstellen eines konfigurationsabhängigen Arbeitsablaufs in einem IT-System, wobei das Verfahren die folgenden Schritte aufweist:
Abfangen eines Befehls, der eine für das IT-System schädliche Aktion einleitet, von einem Software-Werkzeug durch einen Computer;
Erkennen durch den Computer, dass der abgefangene Befehl in einer vorkonfigurierten Liste von Befehlen enthalten ist, wobei der erkannte Befehl zum Ausführen eingeleitet wird;
als Reaktion auf den Schritt des Erkennens des Befehls, Ermitteln eines Satzes von Parametern und von vorkonfigurierten Bedingungen, die dem erkannten Befehl zugehörig sind, durch den Computer;
beruhend auf dem Satz von Parametern und den vorkonfigurierten Bedingungen Erzeugen von XML-Daten (Extensible Markup Language) durch den Computer;
Austauschen von Daten mit externen Systemen durch den Computer über eine generische externe Systemsteuerungsroutine unter Verwendung der XML-Daten über SOAP über eine HTTPS-Schicht (Hypertext Transfer Protocol over Transport Security Layer), wobei die externen Systeme ein Ticketsystem für das IT-System und ein Auftragsablauf-Steuerungssystem für das IT-System umfassen;
als Reaktion auf den Schritt des Austauschens von Daten, Aufnahme einer Verbindung mit dem Ticketsystem in dem konfigurationsabhängigen Arbeitsablauf durch den Computer, wodurch ermittelt wird, ob für den erkannten Befehl eine genehmigte Änderungssteuerung vorhanden ist;
als Reaktion auf den Schritt des Austauschens von Daten, Aufnahme einer Verbindung mit dem Auftragsablauf-Steuerungssystem in dem konfigurationsabhängigen Arbeitsablauf durch den Computer, wodurch ermittelt wird, ob Sicherungskopien innerhalb eines vorher festgelegten Zeitraums vor dem Abfangen des erkannten Befehls als gültig eingestuft werden; und
wenn die genehmigte Änderungssteuerung vorhanden ist und die Sicherungskopien als gültig eingestuft werden, Fortfahren mit dem Ausführen des erkannten Befehls durch den Computer, bzw. wenn die genehmigte Änderungssteuerung nicht vorhanden ist, Beenden des Ausführens des erkannten Befehls durch den Computer, so dass das IT-System durch die schädliche Aktion nicht beeinträchtigt wird, oder, wenn die Sicherungskopien als nicht gültig eingestuft werden, Beenden des Ausführens des erkannten Befehls durch den Computer, so dass das IT-System durch die schädliche Aktion beeinträchtigt wird.

25. Computerprogrammprodukt, aufweisend:
ein durch einen Computer lesbares Speichermedium und einen durch einen Computer lesbaren Programmcode, der in dem durch einen Computer lesbaren Speichermedium gespeichert ist, wobei der durch einen Computer lesbare Programmcode An-

weisungen umfasst, die von einer zentralen Verarbeitungseinheit (CPU) eines Computersystems ausgeführt werden, um ein Verfahren zum Bereitstellen eines konfigurationsabhängigen Arbeitsablaufs in einem IT-System umzusetzen, wobei das Verfahren die folgenden Schritte aufweist:

Abfangen eines Befehls, der eine für das IT-System schädliche Aktion einleitet, von einem Software-Werkzeug durch das Computersystem;

Erkennen durch das Computersystem, dass der abgefangene Befehl in einer vorkonfigurierten Liste von Befehlen enthalten ist, wobei der erkannte Befehl zum Ausführen eingeleitet wird;

als Reaktion auf den Schritt des Erkennens des Befehls, Ermitteln eines Satzes von Parametern und von vorkonfigurierten Bedingungen, die dem erkannten Befehl zugehörig sind, durch das Computersystem;

beruhend auf dem Satz von Parametern und den vorkonfigurierten Bedingungen Erzeugen von XML-Daten (Extensible Markup Language) durch das Computersystem;

Austauschen von Daten mit externen Systemen durch das Computersystem über eine generische externe Systemsteuerungsroutine unter Verwendung der XML-Daten über SOAP über eine HTTPS-Schicht (Hypertext Transfer Protocol over Transport Security Layer), wobei die externen Systeme ein Ticketsystem für das IT-System und ein Auftragsablauf-Steuerungssystem für das IT-System umfassen;

als Reaktion auf den Schritt des Austauschens von Daten, Aufnahme einer Verbindung mit dem Ticketsystem in dem konfigurationsabhängigen Arbeitsablauf durch das Computersystem, wodurch ermittelt wird, ob für den erkannten Befehl eine genehmigte Änderungssteuerung vorhanden ist;

als Reaktion auf den Schritt des Austauschens von Daten, Aufnahme einer Verbindung mit dem Auftragsablauf-Steuerungssystem in dem konfigurationsabhängigen Arbeitsablauf durch das Computersystem, wodurch ermittelt wird, ob Sicherungskopien innerhalb eines vorher festgelegten Zeitraums vor dem Abfangen des erkannten Befehls als gültig eingestuft werden; und

wenn die genehmigte Änderungssteuerung vorhanden ist und die Sicherungskopien als gültig eingestuft werden, Fortfahren mit dem Ausführen des erkannten Befehls durch das Computersystem, bzw. wenn die genehmigte Änderungssteuerung nicht vorhanden ist, Beenden des Ausführens des erkannten Befehls durch das Computersystem, so dass das IT-System durch die schädliche Aktion nicht beeinträchtigt wird, oder, wenn die Sicherungskopien als nicht gültig eingestuft werden, Beenden des Ausführens des erkannten Befehls durch das Computersystem, so dass das IT-System durch die schädliche Aktion beeinträchtigt wird.

Es folgen 6 Seiten Zeichnungen

Anhängende Zeichnungen

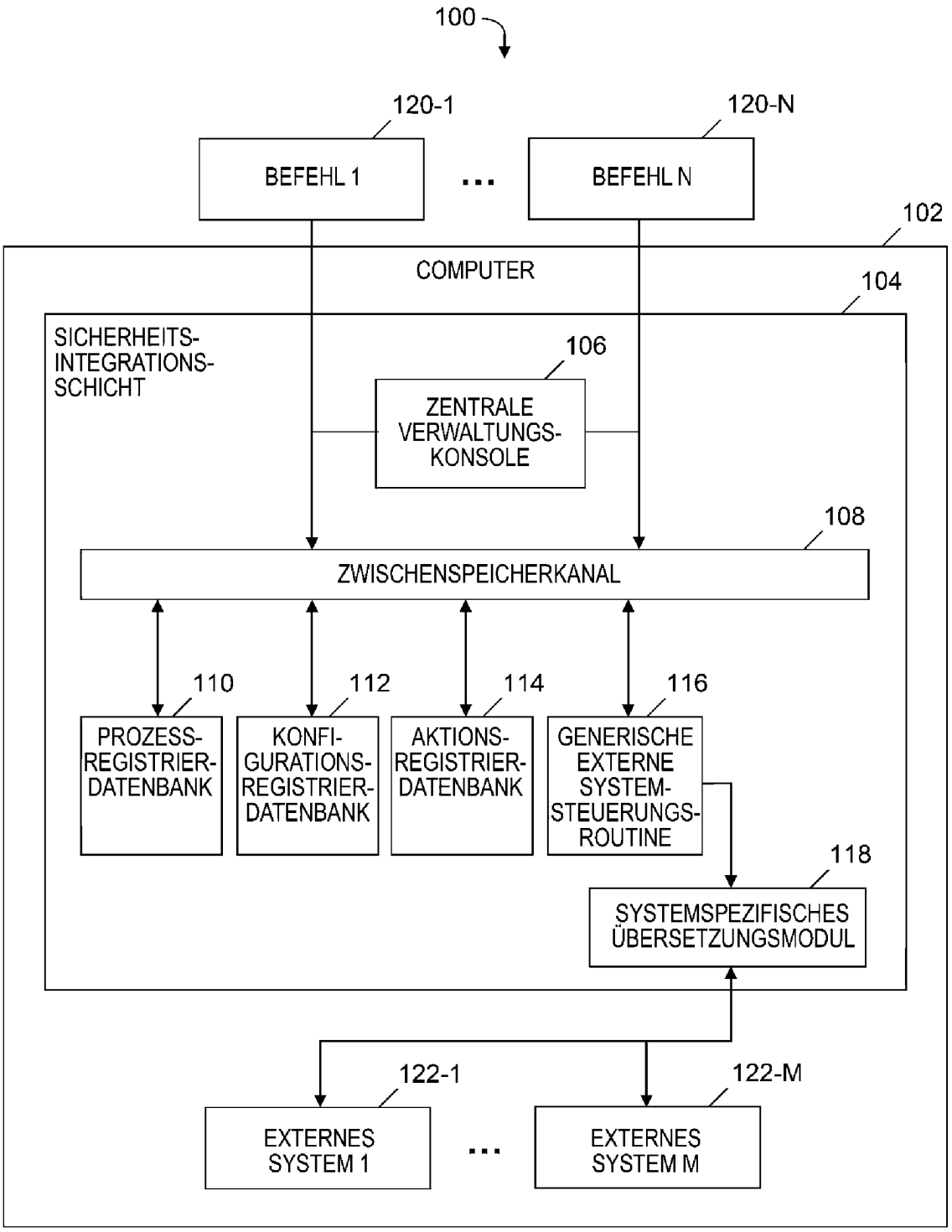


FIG. 1

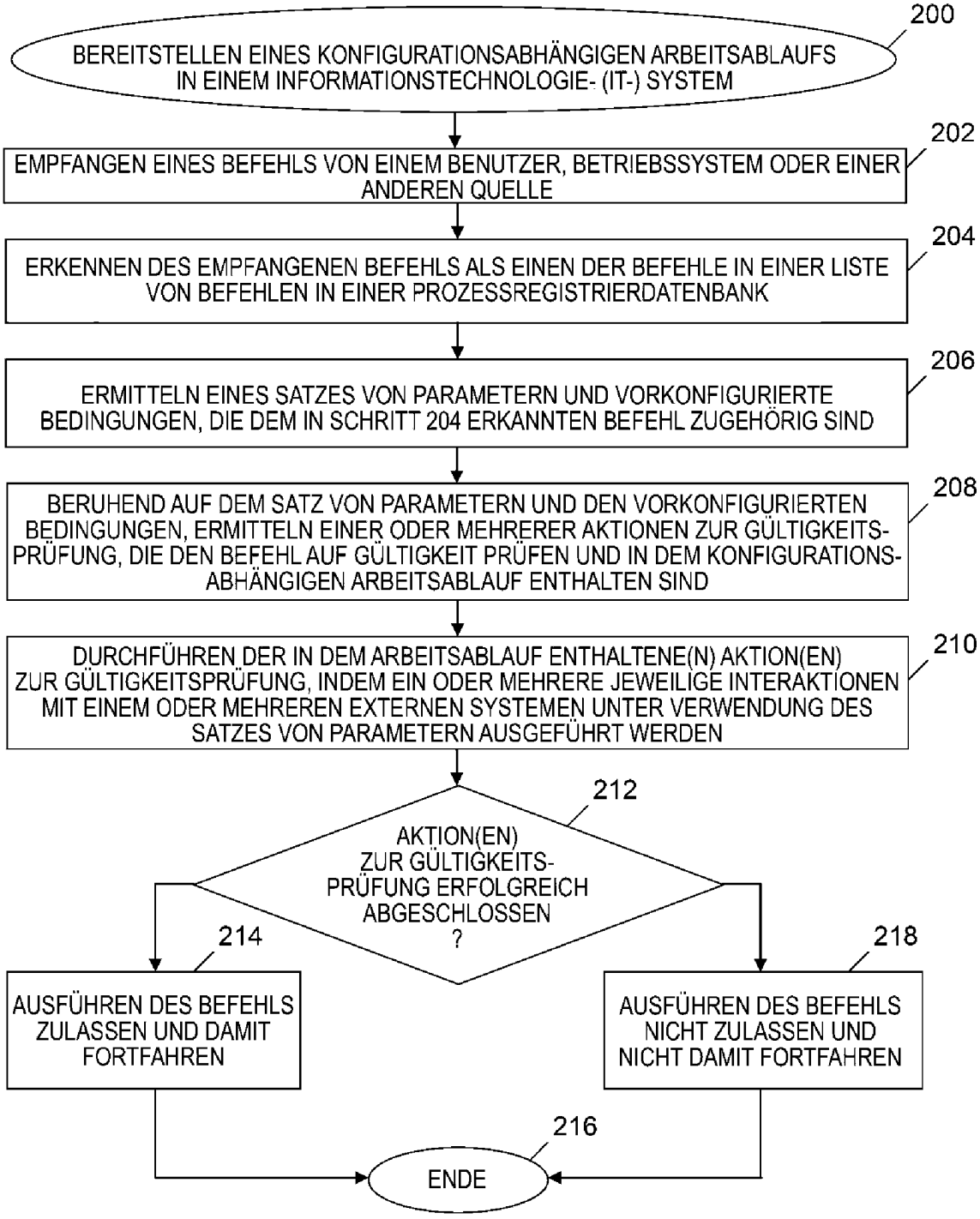

200
BEREITSTELLEN EINES KONFIGURATIONSABHÄNGIGEN ARBEITSABLAUFS IN EINEM INFORMATIONSTECHNOLOGIE- (IT-) SYSTEM
202
EMPFANGEN EINES BEFEHLS VON EINEM BENUTZER, BETRIEBSSYSTEM ODER EINER ANDEREN QUELLE
204
ERKENNEN DES EMPFANGENEN BEFEHLS ALS EINEN DER BEFEHLE IN EINER LISTE VON BEFEHLEN IN EINER PROZESSREGISTRIERDATENBANK
206
ERMITTELN EINES SATZES VON PARAMETERN UND VORKONFIGURIERTE BEDINGUNGEN, DIE DEM IN SCHRITT 204 ERKANNTEN BEFEHL ZUGEHÖRIG SIND
208
BERUHEND AUF DEM SATZ VON PARAMETERN UND DEN VORKONFIGURIERTEN BEDINGUNGEN, ERMITTELN EINER ODER MEHRERER AKTIONEN ZUR GÜLTIGKEITS-PRÜFUNG, DIE DEN BEFEHL AUF GÜLTIGKEIT PRÜFEN UND IN DEM KONFIGURATIONS-ABHÄNGIGEN ARBEITSABLAUF ENTHALTEN SIND
210
DURCHFÜHREN DER IN DEM ARBEITSABLAUF ENTHALTENE(N) AKTION(EN) ZUR GÜLTIGKEITSPRÜFUNG, INDEM EIN ODER MEHRERE JEWEILIGE INTERAKTIONEN MIT EINEM ODER MEHREREN EXTERNEN SYSTEMEN UNTER VERWENDUNG DES SATZES VON PARAMETERN AUSGEFÜHRT WERDEN
212
AKTION(EN) ZUR GÜLTIGKEITS-PRÜFUNG ERFOLGREICH ABGESCHLOSSEN ?
214
AUSFÜHREN DES BEFEHLS ZULASSEN UND DAMIT FORTFAHREN
218
AUSFÜHREN DES BEFEHLS NICHT ZULASSEN UND NICHT DAMIT FORTFAHREN
216
ENDE

FIG. 2

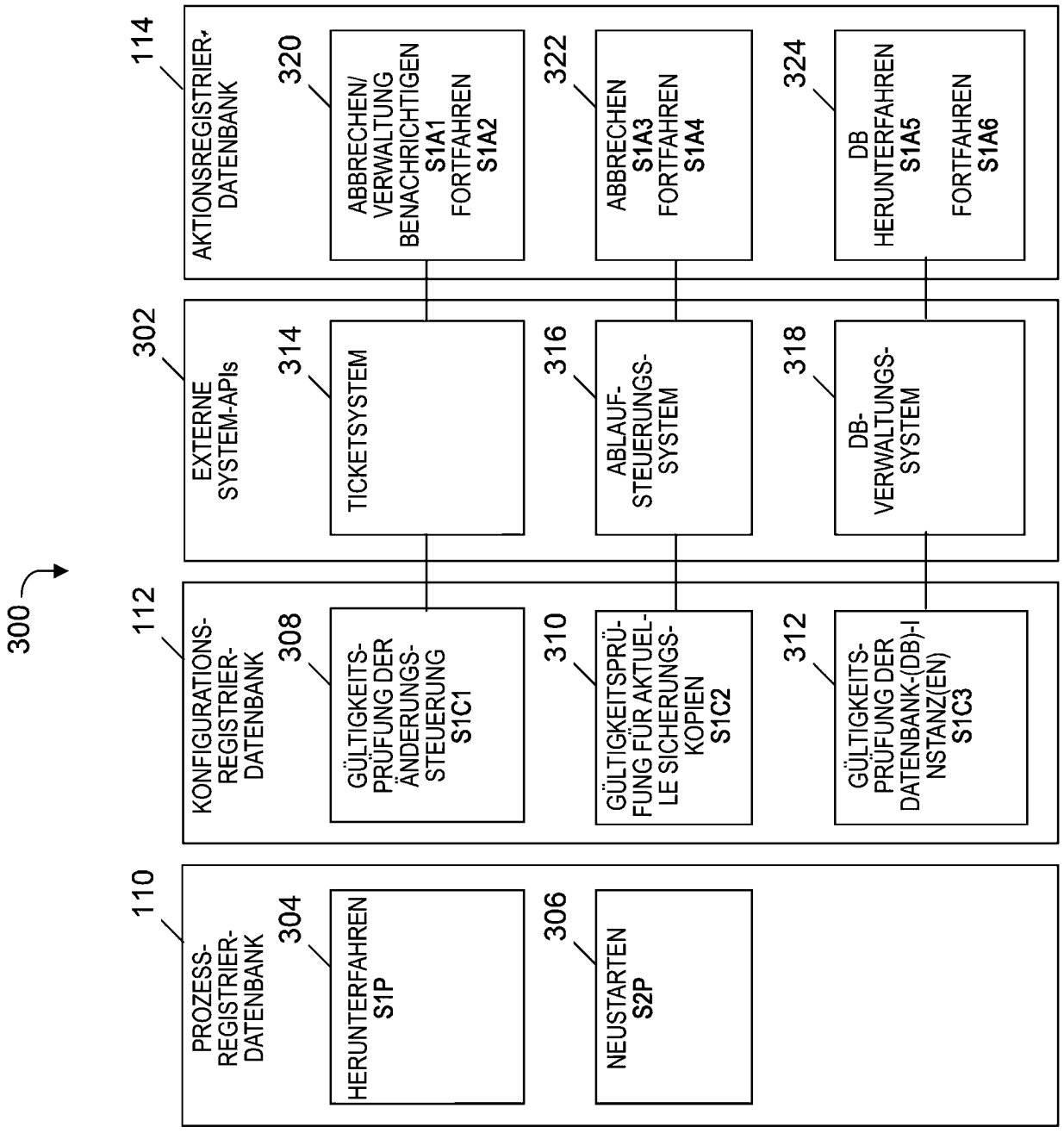

300
110
PROZESS-REGISTRIER-DATENBANK
304
HERUNTERFAHREN S1P
306
NEUSTARTEN S2P
112
KONFIGURATIONS-REGISTRIER-DATENBANK
308
GÜLTIGKEITS-PRÜFUNG DER ÄNDERUNGS-STEUERUNG S1C1
310
GÜLTIGKEITSPRÜ-FUNG FÜR AKTUEL-LE SICHERUNGS-KOPIEN S1C2
312
GÜLTIGKEITS-PRÜFUNG DER DATENBANK-(DB)-I NSTANZ(EN) S1C3
302
EXTERNE SYSTEM-APIs
314
TICKETSYSTEM
316
ABLAUF-STEUERUNGS-SYSTEM
318
DB-VERWALTUNGS-SYSTEM
114
AKTIONSREGISTRIER-DATENBANK
320
ABBRECHEN/ VERWALTUNG BENACHRICHTIGEN S1A1 FORTFAHREN S1A2
322
ABBRECHEN S1A3 FORTFAHREN S1A4
324
DB HERUNTERFAHREN S1A5
FORTFAHREN S1A6

FIG. 3A

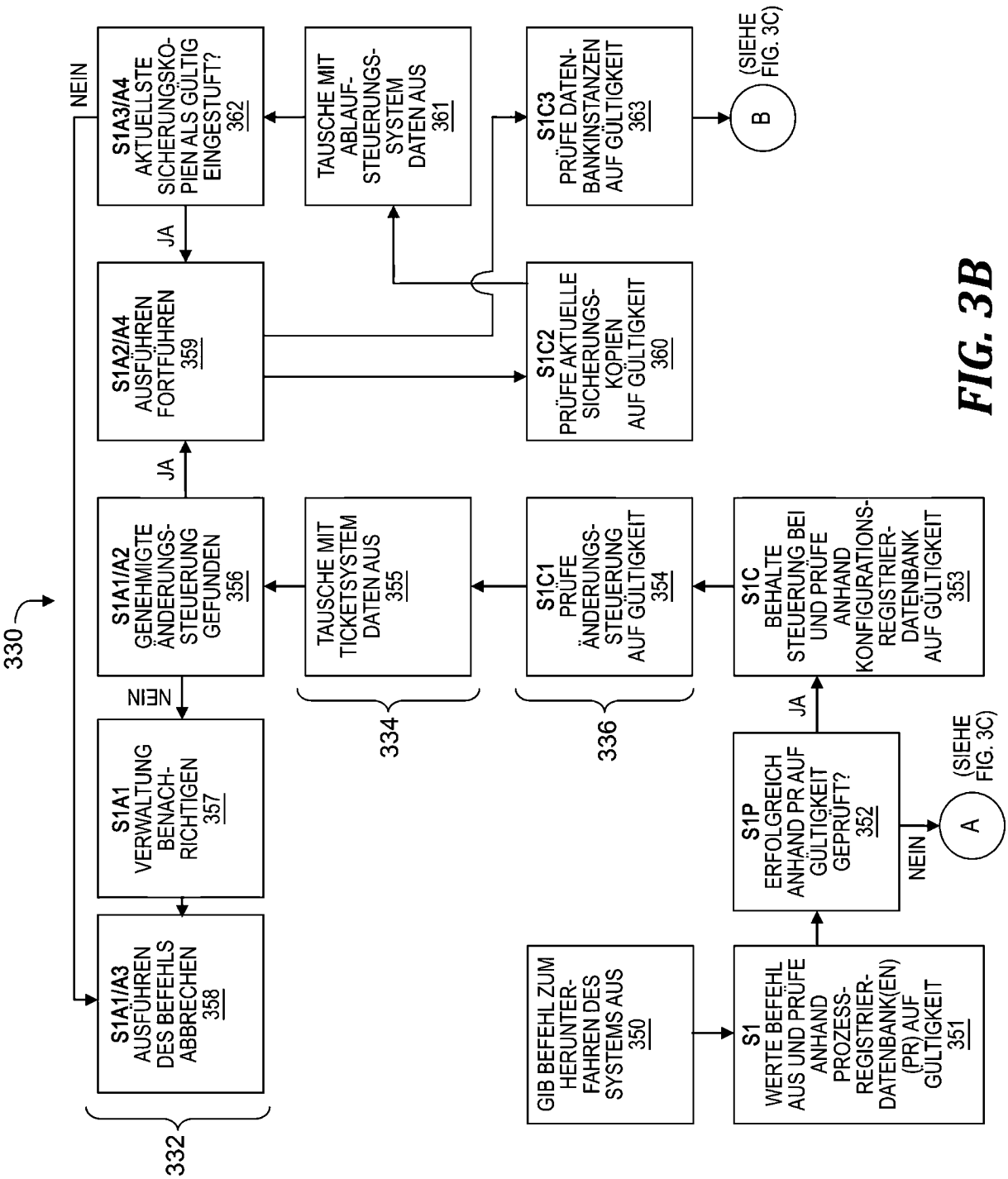

330
GIB BEFEHL ZUM HERUNTER-FAHREN DES SYSTEMS AUS 350
S1 WERTE BEFEHL AUS UND PRÜFE ANHAND PROZESS-REGISTRIER-DATENBANK(EN) (PR) AUF GÜLTIGKEIT 351
S1P ERFOLGREICH ANHAND PR AUF GÜLTIGKEIT GEPRÜFT? 352
NEIN
A (SIEHE FIG. 3C)
JA
S1C BEHALTE STEUERUNG BEI UND PRÜFE ANHAND KONFIGURATIONS-REGISTRIER-DATENBANK AUF GÜLTIGKEIT 353
S1C1 PRÜFE ÄNDERUNGS-STEUERUNG AUF GÜLTIGKEIT 354
TAUSCHE MIT TICKETSYSTEM DATEN AUS 355
S1A1/A2 GENEHMIGTE ÄNDERUNGS-STEUERUNG GEFUNDEN 356
NEIN
S1A1 VERWALTUNG BENACH-RICHTIGEN 357
S1A1/A3 AUSFÜHREN DES BEFEHLS ABBRECHEN 358
332
334
336
JA
S1A2/A4 AUSFÜHREN FORTFÜHREN 359
S1C2 PRÜFE AKTUELLE SICHERUNGS-KOPIEN AUF GÜLTIGKEIT 360
TAUSCHE MIT ABLAUF-STEUERUNGS-SYSTEM DATEN AUS 361
S1A3/A4 AKTUELLSTE SICHERUNGSKO-PIEN ALS GÜLTIG EINGESTUFT? 362
NEIN
S1C3 PRÜFE DATEN-BANKINSTANZEN AUF GÜLTIGKEIT 363
B (SIEHE FIG. 3C)

FIG. 3B

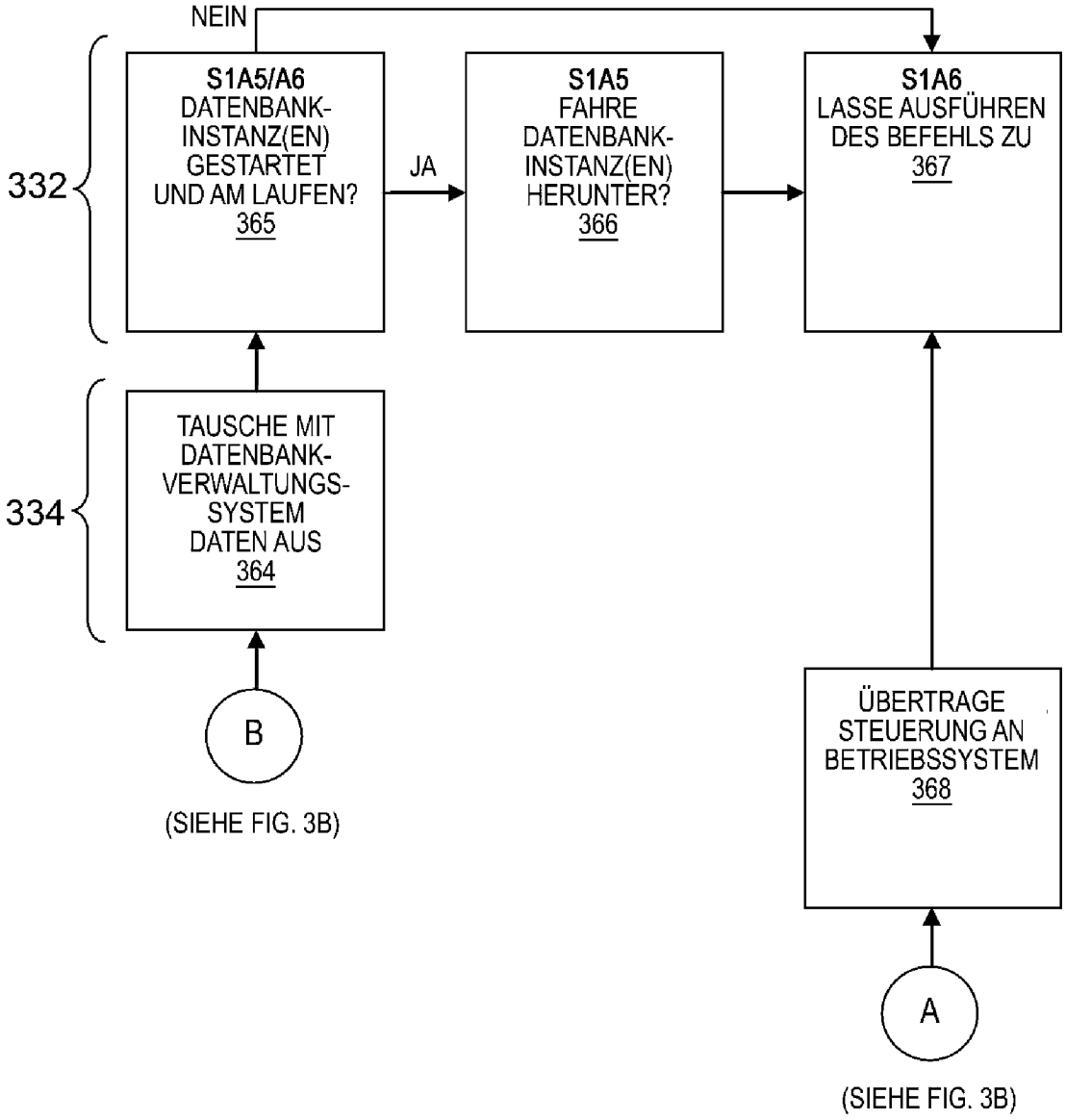

NEIN
S1A5/A6
DATENBANK-INSTANZ(EN) GESTARTET UND AM LAUFEN?
365
JA
S1A5
FAHRE DATENBANK-INSTANZ(EN) HERUNTER?
366
S1A6
LASSE AUSFÜHREN DES BEFEHLS ZU
367
332
TAUSCHE MIT DATENBANK-VERWALTUNGS-SYSTEM DATEN AUS
364
334
B
(SIEHE FIG. 3B)
ÜBERTRAGE STEUERUNG AN BETRIEBSSYSTEM
368
A
(SIEHE FIG. 3B)

FIG. 3C

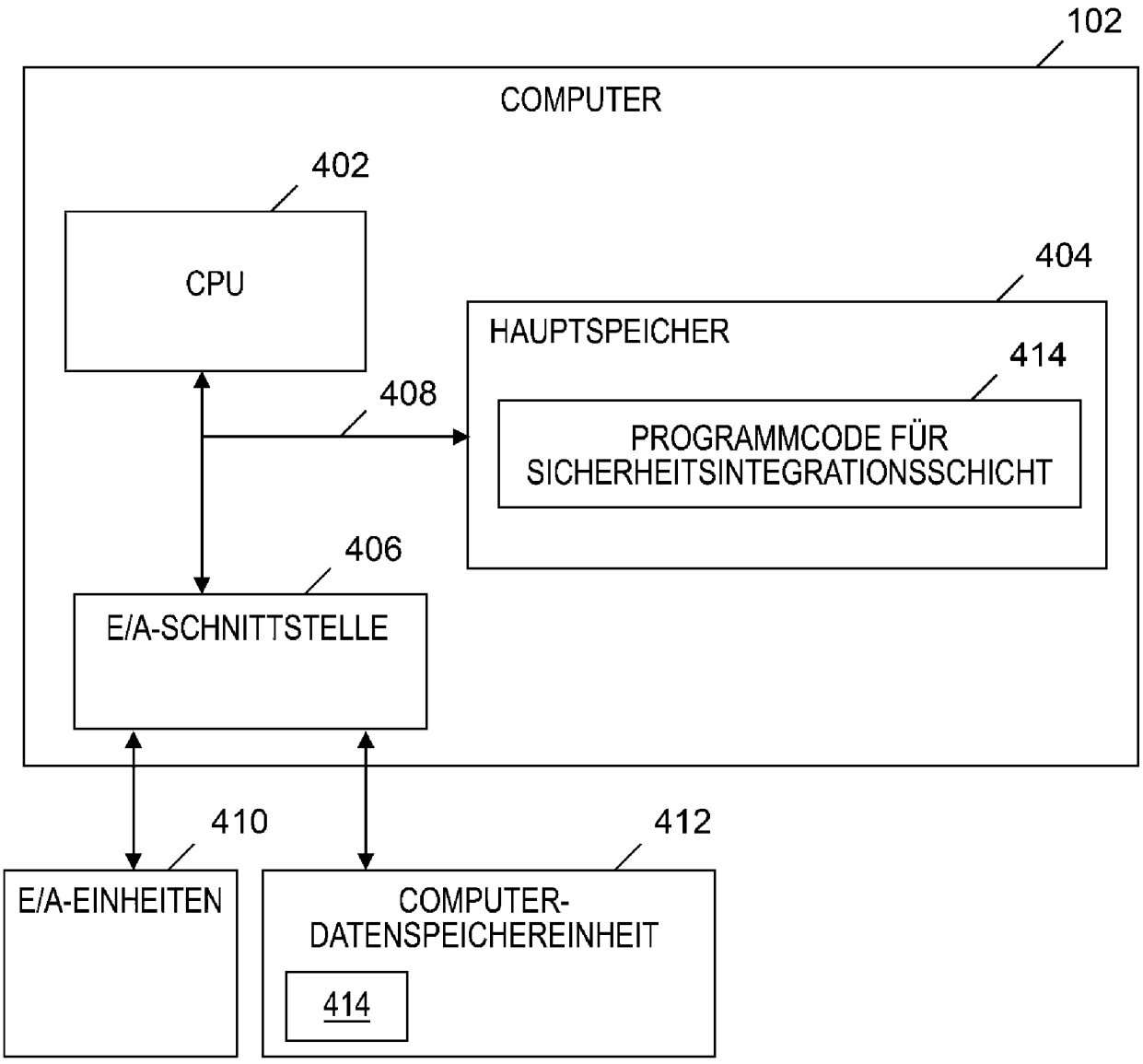

102
COMPUTER
402
CPU
404
HAUPTSPEICHER
414
408
PROGRAMMCODE FÜR
SICHERHEITSINTEGRATIONSSCHICHT
406
E/A-SCHNITTSTELLE
410
412
E/A-EINHEITEN
COMPUTER-
DATENSPEICHEREINHEIT
414

FIG. 4