(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
11. März 2010 (11.03.2010)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2010/026152 A1

(51) Internationale Patentklassifikation:
G05B 19/406 (2006.01) *G06F 21/00* (2006.01)
G05B 19/418 (2006.01) *H04L 29/06* (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2009/061328

(22) Internationales Anmeldedatum:
2. September 2009 (02.09.2009)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
08015433.9 2. September 2008 (02.09.2008) EP

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **SIEMENS AKTIENGESELLSCHAFT** [DE/DE]; Wittelsbacherplatz 2, 80333 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **HERBERTH, Harald** [DE/DE]; Stettiner Straße 23b, 90522 Oberasbach (DE). **KRÖGER, Ulrich** [DE/DE]; Walter-Gropius-Str. 55, 67657 Kaiserslautern (DE). **SOBIHARD, Allan** [SK/SK]; Kuklovska 3, 84104 Bratislava (SK).

(74) Gemeinsamer Vertreter: **SIEMENS AKTIENGESELLSCHAFT**; Postfach 22 16 34, 80506 München (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

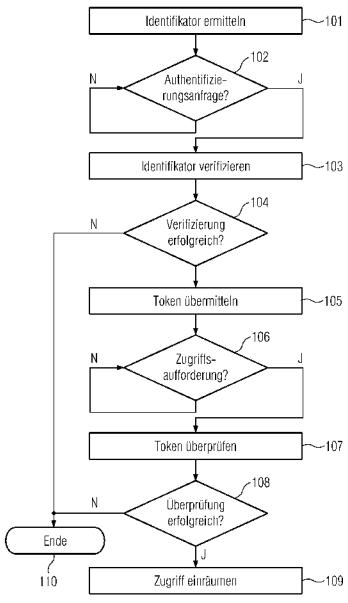
(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU,

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD FOR GRANTING AUTHORIZATION TO ACCESS A COMPUTER-BASED OBJECT IN AN AUTOMATION SYSTEM, COMPUTER PROGRAM, AND AUTOMATION SYSTEM

(54) Bezeichnung : VERFAHREN ZUR EINRÄUMUNG EINER ZUGRIFFSBERECHTIGUNG AUF EIN RECHNERBASIERTES OBJEKT IN EINEM AUTOMATISIERUNGSSYSTEM, COMPUTERPROGRAMM UND AUTOMATISIERUNGSSYSTEM

FIG 1



101 Determine identifier
102 Authentication request?
J Yes
N No
103 Verify identifier
104 Verification successful?
105 Transmit token
106 Access request?
107 Check token
108 Checking process successful?
109 Grant access
110 End

(57) Abstract: In order to grant authorization to access a computer-based object in an automation system, an identifier is determined for a control program, and said identifier is encrypted using a private digital key that is associated with a control and monitoring unit of the automation system. A first service of the automation system is provided on the basis of the computer-based object, and a second service thereof is provided on the basis of the control program. The encrypted identifier is decrypted when being transmitted to an authentication service and is verified by the authentication service. If the verification process has been successful, the authentication service transmits an at least temporarily valid token to the second service. When the control program requests access to the computer-based object, the token is transmitted to the first service for checking purposes. The control program is granted access to the computer-based object if the result of the checking process is positive.

(57) Zusammenfassung: Zur Einräumung einer Zugriffsberechtigung auf ein rechnerbasiertes Objekt in einem Automatisierungssystem wird für ein Steuerungsprogramm ein Identifikator ermittelt, und der Identifikator wird mittels eines einer Steuerungs- und Überwachungseinheit des Automatisierungssystems zugeordneten privaten digitalen Schlüssels verschlüsselt. Anhand des rechnerbasierten Objekts wird ein erster Dienst und anhand des Steuerungsprogramms wird ein zweiter Dienst des Automatisierungssystems bereitgestellt. Der verschlüsselte

[Fortsetzung auf der nächsten Seite]

WO 2010/026152 A1

TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— *mit internationalem Recherchenbericht (Artikel 21 Absatz 3)*

Identifikator wird bei Übermittlung an einen Authentifizierungsdienst entschlüsselt und durch den Authentifizierungsdienst verifiziert. Der Authentifizierungsdienst übermittelt bei erfolgreicher Verifizierung ein zumindest befristet gültiges Token an den zweiten Dienst. Das Token wird bei einer Anforderung eines Zugriffs auf das rechnerbasierte Objekt durch das Steuerungsprogramm an den ersten Dienst zur Überprüfung übermittelt. Ein Zugriff auf das rechnerbasierte Objekt wird bei einem positiven Überprüfungsergebnis für das Steuerungsprogramm eingeräumt.

Beschreibung

Verfahren zur Einräumung einer Zugriffsberechtigung auf ein rechnerbasiertes Objekt in einem Automatisierungssystem, Computerprogramm und Automatisierungssystem

Aufgrund einer ständig steigenden Bedeutung von Informationstechnik für Automatisierungssysteme gewinnen Verfahren zur Sicherung von vernetzten Systemkomponenten wie Überwachungs-, Steuerungs- und Regelungseinrichtungen, Sensoren und Aktoren gegenüber unberechtigtem Zugriff verstärkt an Bedeutung. Im Vergleich zu anderen Anwendungsgebieten der Informationstechnik kommt Datenintegrität in der Automatisierungstechnik eine besonders hohe Bedeutung zu. Insbesondere bei einer Erfassung, Auswertung und Übermittlung von Meß- und Steuerungsdaten ist sicherzustellen, daß vollständige und unveränderte Daten vorliegen. Absichtliche, unabsichtliche oder durch einen technischen Fehler bedingte Veränderungen sind zu vermeiden. Besondere Anforderungen in der Automatisierungstechnik für sicherheitstechnische Verfahren resultieren außerdem aus einem Meldungsverkehr mit verhältnismäßig vielen, aber relativ kurzen Nachrichten. Daneben ist einer Echtzeitfähigkeit eines Automatisierungssystems und seiner Systemkomponenten Rechnung zu tragen.

Insbesondere in Automatisierungssystemen, die auf dienstorientierten Architekturen basieren, sind häufig sehr differenzierte Sicherheits- und Zugriffsrichtlinien für dort bereitgestellte Dienste anzuwenden. Dabei sind Sicherheits- und Zugriffslinien nicht nur in bezug auf Benutzer anzuwenden, sondern auch auf Dienste, die auf andere Dienste zurückgreifen. Daher kommt einer Software-Authentifizierung in derartigen Anwendungsgebieten eine große Bedeutung zu. Insbesondere bestehen dabei Anforderungen hinsichtlich einer schnellen und

effektiven Identifizierung und Zugriffsrechteinräumung für eine Vielzahl von Software-Modulen. Bisherige Lösungen zielen auf eine explizite Implementierung von Software-Authentifizierungsverfahren ab. Dies hat den Nachteil, daß entsprechende Authentifizierungsverfahren fest in Software-Module zu integrieren sind, die entweder Zugriff auf zu schützende Ressourcen anfordern oder diese bereitstellen. Alternative bisherige Lösungsansätze sehen vor, Authentifizierungsverfahren implementierende Software-Module statisch oder dynamisch mit den zu schützende Ressourcen anfordernden oder bereitstellenden Software-Modulen zu binden. Erfolgt ein Binden dynamisch, besteht zumindest eine Möglichkeit, dies durch Konfiguration zu steuern.

Der vorliegenden Erfindung liegt daher die Aufgabe zugrunde, ein schnelles und effektives Verfahren zur Einräumung einer Zugriffsberechtigung auf ein rechnerbasiertes Objekt in einem Automatisierungssystem zu schaffen, sowie eine geeignete technische Realisierung des Verfahrens anzugeben.

Diese Aufgabe wird erfindungsgemäß durch ein Verfahren mit den in Anspruch 1 angegebenen Merkmalen, durch ein Computerprogramm mit den in Anspruch 13 angegebenen Merkmalen sowie durch ein Automatisierungssystem mit den in Anspruch 14 angegebenen Merkmalen gelöst. Vorteilhafte Weiterbildungen der vorliegenden Erfindung sind in den abhängigen Ansprüchen angegeben.

Erfindungsgemäß wird zur Einräumung einer Zugriffsberechtigung auf ein rechnerbasiertes Objekt in einem Automatisierungssystem zunächst für ein Steuerungsprogramm ein Identifikator ermittelt und der Identifikator mittels eines einer Steuerungs- und Überwachungseinheit des Automatisierungssystems zugeordneten privaten digitalen Schlüssels verschlüs-

selt. Dies kann einmalig für das Steuerungsprogramm erfolgen und braucht nicht wiederholt zu werden. Anhand des rechnerbasierten Objekts wird ein erster Dienst und anhand des Steuerungsprogramms wird ein zweiter Dienst des Automatisierungssystems vorzugsweise innerhalb einer dienstorientierten Architektur bereitgestellt. Dienstorientierte bzw. serviceorientierte Architekturen (SOA) zielen darauf ab, Dienste in komplexen Organisationseinheiten zu strukturieren und für eine Vielzahl von Nutzern verfügbar zu machen. Dabei werden beispielsweise vorhandene Komponenten eines Datenverarbeitungssystems, wie Programme, Datenbanken, Server oder Websites, so koordiniert, daß von den Komponenten bereitgestellte Leistungen zu Diensten zusammen gefaßt und berechtigten Nutzern zur Verfügung gestellt werden. Serviceorientierte Architekturen ermöglichen eine Anwendungsintegration, indem Komplexität einzelner Teilkomponenten eines Datenverarbeitungssystems hinter standardisierten Schnittstellen verborgen wird. Hierdurch lassen sich wiederum Zugriffsberechtigungsregelungen vereinfachen.

Rechnerbasierte Objekte sind beispielsweise ohne Beschränkung der Allgemeinheit dieses Begriffs Betriebssysteme, Steuerungs- oder Anwendungsprogramme, durch Betriebssysteme, Steuerungs- oder Anwendungsprogramme bereitgestellte Dienste, Leistungsmerkmale, Funktionen oder Prozeduren, Zugriffsrechte auf Peripheriegeräte sowie auf einem Speichermedium befindliche Daten. Funktionen oder Prozeduren umfassen dabei insbesondere auch eine Freigabe von Zugriffsberechtigungen in einem Automatisierungssystem. Unter einem Rechner sind beispielsweise PCs, Notebooks, Server, PDAs, Mobiltelefone sowie Steuerungs- und Regelungsmodule, Sensoren oder Aktoren in der Automatisierungs-, Fahrzeug-, Kommunikations- oder Medizintechnik zu verstehen - allgemein Einrichtungen, in denen Computerprogramme ablaufen.

Des weiteren wird entsprechend der erfindungsgemäßen Lösung der verschlüsselte Identifikator bei Übermittlung an einen Authentifizierungsdienst entschlüsselt und durch den Authentifizierungsdienst verifiziert. Der Authentifizierungsdienst übermittelt bei erfolgreicher Verifizierung ein zumindest befristet gültiges Token an den zweiten Dienst. Bei einer Anforderung eines Zugriffs auf das rechnerbasierte Objekt wird das Token durch das Steuerungsprogramm an den ersten Dienst zur Überprüfung übermittelt. Bei einem positiven Überprüfungsergebnis wird ein Zugriff auf das rechnerbasierte Objekt für das Steuerungsprogramm eingeräumt, vorzugsweise durch einen Autorisierungsdienst. Die Übermittlung des verschlüsselten Identifikators an den Authentifizierungsdienst kann im Rahmen eines vom zweiten Dienst initiierten Dienstaufrufs erfolgen. In entsprechender Weise kann das Token im Rahmen eines vom zweiten Dienst initiierten Dienstaufrufs an den ersten Dienst übermittelt werden.

Die erfindungsgemäße Lösung bietet den Vorteil, daß Software-Authentifizierungsverfahren für Ressourcen anfordernde bzw. bereitstellende Software-Module konfigurierbar sind und nicht fest in die jeweiligen Software-Module integriert werden müssen. Eine derartige Funktionalität kann somit in Form einer Dienstkomponente genutzt werden und ermöglicht eine schnelle, flexible und wirkungsvolle Nutzung. Entsprechend einer bevorzugten Ausführungsform der vorliegenden Erfindung weist der zweite Dienst hierzu für jedes vom zweiten Dienst umfaßte Steuerungsprogrammodul jeweils eine eigene Dienstkomponente zur Anforderung eines Modulidentifikators, zur Verwaltung eines durch die Steuerungs- und Überwachungseinheit verschlüsselten Modulidentifikators bzw. zur Verwaltung eines aus dem Modulidentifikator durch den Authentifizierungsdienst ermittelten Modultokens auf.

Vorteilhafterweise ist die Steuerungs- und Überwachungseinheit ein Engineering-System zur Konfiguration, Wartung, Inbetriebnahme und/oder Dokumentation des Automatisierungssystems, und der Authentifizierungsdienst wird durch das Engineering-System bereitgestellt. Auf diese Weise lassen sich Software-Authentifizierungsverfahren in verteilten Automatisierungssystemen, die auf dienstorientierten Architekturen beruhen, besonders schnell, sicher und effizient konfigurieren. Hieraus ergibt sich eine erhebliche Verbesserung von Systemsicherheit und -stabilität.

Die Erfindung wird nachfolgend an einem Ausführungsbeispiel anhand der Zeichnung näher erläutert. Es zeigt

Figur 1 ein Ablaufdiagramm für ein Verfahren zur Einräumung einer Zugriffsberechtigung auf ein rechnerbasiertes Objekt in einem Automatisierungssystem,

Figur 2 eine schematische Darstellung eines Automatisierungssystems zur Realisierung des Verfahrens gemäß Figur 1.

Entsprechend dem in Figur 1 veranschaulichten Verfahren zur Einräumung einer Zugriffsberechtigung auf ein rechnerbasiertes Objekt 272 ermittelt ein Engineering-System 201 des Automatisierungssystems gemäß Figur 2 für ein Steuerungsprogramm 282 einen Software-Identifikator (Schritt 101). Außerdem wird der Software-Identifikator mittels eines dem Engineering-System 201 zugeordneten privaten digitalen Schlüssels verschlüsselt. Das Engineering-System 201 ist über ein Kommunikationsnetz 205 mit einer ersten Rechnereinheit 202, einer zweiten Rechnereinheit 203 und einer dritten Rechnereinheit 204 verbunden. Durch die erste Rechnereinheit 202 wird anhand

des rechnerbasierten Objekts 272 ein erster Dienst innerhalb einer dienstorientierten Architektur bereitgestellt, während anhand des Steuerungsprogramms 282 ein zweiter Dienst bereitgestellt wird. Auf einer Festplatte 223, 233 der ersten und der zweiten Rechnereinheit 202, 203 ist jeweils Programmcode 207, 208 zur Implementierung des ersten bzw. zweiten Dienstes gespeichert. Der jeweilige Programmcode 207, 208 umfaßt das rechnerbasierte Objekt 272 bzw. das Steuerungsprogramm 282 und ist in einen Arbeitsspeicher 222, 232 der ersten bzw. zweiten Rechnereinheit 202, 203 ladbar. Außerdem ist der jeweilige Programmcode 207, 208 durch einen Prozessor 221, 231 der ersten bzw. zweiten Rechnereinheit 202, 203 zur Bereitstellung des ersten bzw. zweiten Dienstes ausführbar.

Das rechnerbasierte Objekt 272 ist im vorliegenden Ausführungsbeispiel ein Meßergebnis, das durch die erste Rechnereinheit 202 als computergestützte Sensoreinheit erfaßt wird und vom auf der zweiten Rechnereinheit 203 ablaufenden Steuerungsprogramm 282 angefordert wird. Das Steuerungsprogramm dient zur Ansteuerung von meßtechnischer oder aktorischer Peripherie der zweiten Rechnereinheit 203, wie Sensoren oder Roboter. Im Hinblick auf einen Meldungsaustausch zur Steuerung und Überwachung der Rechnereinheiten 202-204 ist sicherzustellen, daß Meldungen auf einem Weg von einem Sender zu einem Empfänger nicht verfälscht werden. Andernfalls könnte dies zu Störungen oder Schäden im Automatisierungssystem führen. Außerdem kann ein Interesse darin bestehen, daß beispielsweise ein infolge eines Ablaufs eines Steuerungsprogramms erfaßtes Meßergebnis nur durch einen berechtigten Benutzer abfragbar ist und eine übermittelte Meldung mit dem Meßergebnis nicht durch unautorisierte Benutzer abgefangen und ausgelesen werden kann. Ein Benutzer kann hierbei auch ein anderes Gerät innerhalb des Automatisierungssystems sein.

Das Engineering-System 201 dient zur Konfiguration, Wartung, Inbetriebnahme und/oder Dokumentation des Automatisierungssystems und stellt einen Identitätsverwaltungsdienst bereit, durch den die Ermittlung des Identifikators und dessen Verschlüsselung erfolgt. Hierzu ist auf einer Festplatte 213 des Engineering-Systems 201 Programmcode 206 zur Implementierung des Identitätsverwaltungsdienstes gespeichert, der in einen Arbeitsspeicher 212 ladbar und durch einen Prozessor 211 des Engineering-Systems 201 ausführbar ist. Der Authentifizierungsdienst umfaßt eine Dienstkomponente für eine Ver- und Entschlüsselung von Software-Identifikatoren und eine Dienstkomponente für eine Verifizierung von Software-Identifikator-Anforderungen. Programmcode 261, 262 zur Implementierung dieser Dienstkomponenten ist ebenfalls auf der Festplatte 213 des Engineering-Systems 201 gespeichert.

Auf einer Festplatte 243 der dritten Rechnereinheit 204 ist Programmcode 209 zur Implementierung eines Token-Dienstes gespeichert, durch den Token zum Zugriff auf rechnerbasierte Objekte für Steuerungsprogramme bereitgestellt werden. Der Programmcode 209 zur Implementierung des Token-Dienstes ist in einen Arbeitsspeicher 242 der dritten Rechnereinheit 204 ladbar und durch einen Prozessor 241 der dritten Rechnereinheit 204 ausführbar.

Der entsprechend Schritt 101 des in Figur 1 dargestellten Ablaufdiagramms ermittelte und verschlüsselte Software-Identifikator wird auf eine von der zweiten Rechnereinheit 203 an das Engineering-System 201 übermittelte Meldung 234 mit einer Anforderung eines verschlüsselten Software-Identifikators durch den Identitätsverwaltungsdienst erstellt. Nach erfolgreicher Verifizierung der Anfrage und Erstellung des verschlüsselten Software-Identifikators 214 wird dieser an die zweite Rechnereinheit 203 übermittelt und dort in einer dem

zweiten Dienst zugeordneten Datenbank 283 abgespeichert, die auch Informationen zur Konfiguration des zweiten Dienstes umfaßt. Vorzugsweise wird auch eine unverschlüsselte Version des Software-Identifikators an die zweite Rechnereinheit 203 übermittelt und dort gespeichert.

Nach Erstellung und Übermittlung des verschlüsselten Software-Identifikators an die zweite Rechnereinheit 203 überprüft der Token-Dienst fortlaufend, ob von der zweiten Rechnereinheit 203 eine Authentifizierungsanfrage vorliegt, die eine Meldung 235 mit einer Anforderung eines Tokens für zweiten Dienst zum Zugriff auf das rechnerbasierte Objekt 272 umfaßt (Schritt 102). Eine Meldung 235 mit einer Anforderung eines Tokens umfaßt auch den verschlüsselten Software-Identifikator. Bei Übermittlung einer solchen Meldung an den Token-Dienst wird der verschlüsselte Software-Identifikator durch entsprechende Dienstkomponenten des Token-Dienst entschlüsselt und verifiziert (Schritt 103). Dabei wird insbesondere der entschlüsselte gegen den unverschlüsselten Software-Identifikator abgeglichen, der vorzugsweise von der Meldung 235 mit der Anfrage umfaßt ist. Zwischen Schritt 102 und Schritt 103 kann in praktischen Anwendungsszenarien mitunter eine längere Zeitspanne liegen.

Nachfolgend wird überprüft, ob eine Verifizierung der Anforderung und des verschlüsselten Software-Identifikators erfolgreich verlaufen ist (Schritt 104). Bei negativem Verifizierungsergebnis wird das Verfahren entsprechend Figur 1 im vorliegenden Ausführungsbeispiel beendet (Schritt 110). Ist die Verifizierung dagegen erfolgreich verlaufen, so veranlaßt der Token-Dienst eine Erstellung eines zumindest befristet gültigen Tokens durch den Token-Dienst und eine Übermittlung des Tokens 244 an den zweiten Dienst (Schritt 105). Das Token wird dort in der dem zweiten Dienst zugeordneten Datenbank

283 gespeichert. Vorzugsweise wird der zweite Dienst derart konfiguriert, daß der zweite Dienst bei Ablauf einer Gültigkeitsdauer des Tokens 244 automatisch ein neues Token vom Token-Dienst anfordert.

Entsprechend dem in Figur 1 dargestellten Ablaufdiagramm wird in Schritt 106 fortlaufend durch den ersten Dienst überprüft, ob eine Zugriffsanforderung auf das rechnerbasierte Objekt 272 vorliegt. Liegt eine Zugriffsanforderung 236 mit einem Token durch den zweiten Dienst vor, überprüft der zweite Dienst das Token auf Gültigkeit (Schritt 108). Nachfolgend wird entsprechend Schritt 108 abgefragt, ob eine erfolgreiche Überprüfung vorliegt. Bei einem negativen Überprüfungsergebnis wird das in Figur 1 veranschaulichte Verfahren beendet (Schritt 110). Kann der erste Dienst dagegen für das Token 236 eine erfolgreiche Authentifizierung des Steuerungsprogramms 282 durchführen, wird entsprechend Schritt 109 ein Zugriff auf das rechnerbasierte Objekt 272 durch eine dem ersten Dienst zugeordnete Autorisierungskomponente für das Steuerungsprogramm 282 eingeräumt. Dabei wird im vorliegenden Ausführungsbeispiel eine das rechnerbasierte Objekt 272 umfassende Meldung 224 an die zweite Rechnereinheit 203 übermittelt. Vorzugsweise wird der Zugriff auf das rechnerbasierte Objekt 272 für das Steuerungsprogramm 282 erst dann eingeräumt wird, wenn der verschlüsselte Software-Identifikator 214 durch das Steuerungsprogramm 282 in den Arbeitsspeicher 232 der zweiten Rechnereinheit 203 geladen ist.

Der zweite Dienst weist für jedes vom zweiten Dienst umfaßte Steuerungsprogrammodul jeweils eine eigene Dienstkomponente zur Anforderung eines Modulidentifikators, zur Verwaltung eines durch die Steuerungs- und Überwachungseinheit verschlüsselten Modulidentifikators und/oder zur Verwaltung eines aus dem Modulidentifikator durch den Token-Dienst ermittelten Mo-

dultokens auf. Eine derartige Dienstkomponente implementierender Programmcode 281 ist ebenfalls auf der Festplatte 233 der zweiten Rechnereinheit 203 gespeichert. Für Anwendungsfälle, in denen der erste Dienst auf andere Dienste zurückgreift, ist ebenfalls eine entsprechende Dienstkomponente für den ersten Dienst vorgesehen, deren Programmcode 271 auf der Festplatte 223 der ersten Rechnereinheit gespeichert ist. Etwaige Software-Identifikatoren oder Token werden gemeinsam mit Daten zur Konfiguration des ersten Dienstes in einer der ersten Rechnereinheit 202 zugeordneten Datenbank 283 gespeichert.

Das vorangehend beschriebene Verfahren wird auf Seiten des Engineering-Systems vorzugsweise durch ein in einen Arbeitsspeicher des Engineering-Systems 202 ladbares Computerprogramm implementiert. Das Computerprogramm weist zumindest einen Codeabschnitt auf, bei dessen Ausführung für ein Steuerungsprogramm ein Identifikator ermittelt und der Identifikator mittels eines einer Steuerungs- und Überwachungseinheit des Automatisierungssystems zugeordneten privaten digitalen Schlüssels verschlüsselt wird, wenn das Computerprogramm im Rechner abläuft. Dabei sind anhand des rechnerbasierten Objekts ein erster Dienst und anhand des Steuerungsprogramms ein zweiter Dienst des Automatisierungssystems innerhalb einer dienstorientierten Architektur bereitstellbar. Außerdem wird bei einer Übermittlung des verschlüsselten Identifikators an einen Authentifizierungsdienst dessen Entschlüsselung und Verifizierung durch den Authentifizierungsdienst veranlaßt. Darüber hinaus wird bei einer erfolgreichen Verifizierung eine Übermittlung eines zumindest befristet gültigen Tokens durch den Authentifizierungsdienst an den zweiten Dienst veranlaßt. Dabei ist das Token zur Überprüfung an den ersten Dienst übermittelbar und zur Einräumung eines Zugriffs auf

das rechnerbasierte Objekt für das Steuerungsprogramm überprüfbar.

Die Anwendung der vorliegenden Erfindung ist nicht auf das beschriebene Ausführungsbeispiel beschränkt.

Patentansprüche

1. Verfahren zur Einräumung einer Zugriffsberechtigung auf ein rechnerbasiertes Objekt in einem Automatisierungssystem, bei dem

- für ein Steuerungsprogramm ein Identifikator ermittelt und der Identifikator mittels eines einer Steuerungs- und Überwachungseinheit des Automatisierungssystems zugeordneten privaten digitalen Schlüssels verschlüsselt wird,
- anhand des rechnerbasierten Objekts ein erster Dienst und anhand des Steuerungsprogramms ein zweiter Dienst des Automatisierungssystems bereitgestellt werden,
- der verschlüsselte Identifikator bei Übermittlung an einen Authentifizierungsdienst entschlüsselt und durch den Authentifizierungsdienst verifiziert wird,
- der Authentifizierungsdienst bei erfolgreicher Verifizierung ein zumindest befristet gültiges Token an den zweiten Dienst übermittelt,
- das Token bei einer Anforderung eines Zugriffs auf das rechnerbasierte Objekt durch das Steuerungsprogramm an den ersten Dienst zur Überprüfung übermittelt wird,
- ein Zugriff auf das rechnerbasierte Objekt bei einem positiven Überprüfungsergebnis für das Steuerungsprogramm eingeräumt wird.

2. Verfahren nach Anspruch 1,
bei dem der erste Dienst und der zweite Dienst innerhalb einer dienstorientierten Architektur bereitgestellt werden.

3. Verfahren nach einem der Ansprüche 1 oder 2,
bei dem ein Zugriff auf das rechnerbasierte Objekt bei einem positiven Überprüfungsergebnis durch eine dem ersten Dienst

zugeordnete Autorisierungskomponente für das Steuerungsprogramm eingeräumt wird.

4. Verfahren nach einem der Ansprüche 1 bis 3,
bei dem der verschlüsselte Identifikator und/oder das Token in einer dem zweiten Dienst zugeordneten Datenbasis gespeichert wird.

5. Verfahren nach Anspruch 4,
bei dem die Datenbasis Informationen zur Konfiguration des zweiten Dienstes umfaßt.

6. Verfahren nach einem der Ansprüche 1 bis 5,
bei dem der Identifikator für das Steuerungsprogramm durch den zweiten Dienst angefordert und durch einen Identitätsverwaltungsdienst ermittelt wird.

7. Verfahren nach Anspruch 6,
bei dem die Steuerungs- und Überwachungseinheit ein Engineering-System zur Konfiguration, Wartung, Inbetriebnahme und/oder Dokumentation des Automatisierungssystems ist, und
bei dem der Identitätsverwaltungsdienst durch das Engineering-System bereitgestellt wird.

8. Verfahren nach einem der Ansprüche 1 bis 7,
bei dem der zweite Dienst derart konfigurierbar ist, daß der zweite Dienst bei Ablauf einer Gültigkeitsdauer des Tokens automatisch ein neues Token vom Authentifizierungsdienst anfordert.

9. Verfahren nach einem der Ansprüche 1 bis 8,
bei dem die Übermittlung des verschlüsselten Identifikators an den Authentifizierungsdienst im Rahmen eines vom zweiten Dienst initiierten Dienstaufrufs erfolgt.

10. Verfahren nach einem der Ansprüche 1 bis 9, bei dem das Token im Rahmen eines vom zweiten Dienst initiierten Dienstaufrufs an den ersten Dienst übermittelt wird.

11. Verfahren nach einem der Ansprüche 1 bis 10, bei dem der Zugriff auf das rechnerbasierte Objekt für das Steuerungsprogramm erst dann eingeräumt wird, wenn der verschlüsselte Identifikator durch das Steuerungsprogramm in einen Arbeitsspeicher einer Rechnereinheit geladen ist, auf der das Steuerungsprogramm abläuft.

12. Verfahren nach einem der Ansprüche 1 bis 11, bei dem der zweite Dienst für jedes vom zweiten Dienst umfaßte Steuerungsprogrammodul jeweils eine eigene Dienstkomponente zur Anforderung eines Modulidentifikators, zur Verwaltung eines durch die Steuerungs- und Überwachungseinheit verschlüsselten Modulidentifikators und/oder zur Verwaltung eines aus dem Modulidentifikator durch den Authentifizierungsdienst ermittelten Modultokens aufweist.

13. Computerprogramm zur Einräumung einer Zugriffsberechtigung, das in einen Arbeitsspeicher eines Rechners ladbar ist und zumindest einen Codeabschnitt aufweist, bei dessen Ausführung

- für ein Steuerungsprogramm ein Identifikator ermittelt und der Identifikator mittels eines einer Steuerungs- und Überwachungseinheit des Automatisierungssystems zugeordneten privaten digitalen Schlüssels verschlüsselt wird, wobei anhand des rechnerbasierten Objekts ein erster Dienst und anhand des Steuerungsprogramms ein zweiter Dienst des Automatisierungssystems bereitstellbar sind,

- bei einer Übermittlung des verschlüsselten Identifikators an einen Authentifizierungsdienst dessen Entschlüsselung und Verifizierung durch den Authentifizierungsdienst veranlaßt wird,
- bei einer erfolgreichen Verifizierung eine Übermittlung eines zumindest befristet gültigen Tokens durch den Authentifizierungsdienst an den zweiten Dienst veranlaßt wird, wobei das Token zur Überprüfung an den ersten Dienst übermittelbar und zur Einräumung eines Zugriffs auf das rechnerbasierte Objekt für das Steuerungsprogramm überprüfbar ist,

wenn das Computerprogramm im Rechner abläuft.

14. Automatisierungssystem mit

- mehreren über ein Kommunikationsnetz miteinander verbundenen Rechnereinheiten an Netzknoten des Automatisierungssystems,
- zumindest einer Rechnereinheit zur Bereitstellung eines ersten Dienstes anhand eines rechnerbasierten Objekts und eines zweiten Dienstes anhand eines Steuerungsprogramms,
- einer Steuerungs- und Überwachungseinheit zur Ermittlung eines Identifikators für das Steuerungsprogramm und zur Verschlüsselung des Identifikators mittels eines einer Steuerungs- und Überwachungseinheit zugeordneten privaten digitalen Schlüssels,
- einer einem Authentifizierungsdienst zugeordneten Rechnereinheit zur Entschlüsselung und Verifizierung eines verschlüsselten Identifikators und zur Übermittlung eines zumindest befristet gültigen Tokens an den zweiten Dienst bei einer erfolgreichen Verifizierung, wobei das Token zur Überprüfung an den ersten Dienst übermittelbar und zur Einräumung eines Zugriffs auf das rechnerbasierte Objekt für das Steuerungsprogramm überprüfbar ist.

FIG 1

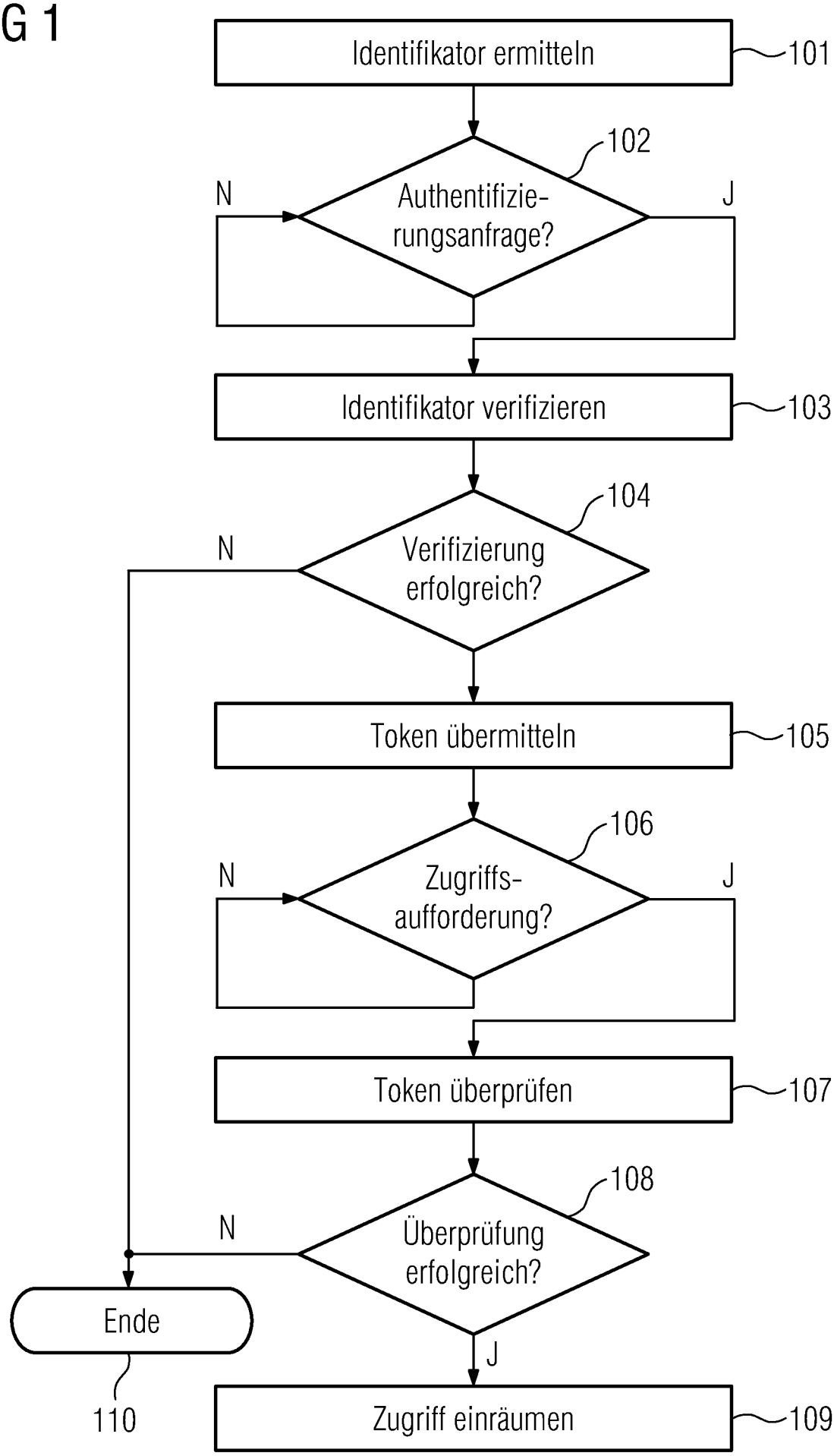
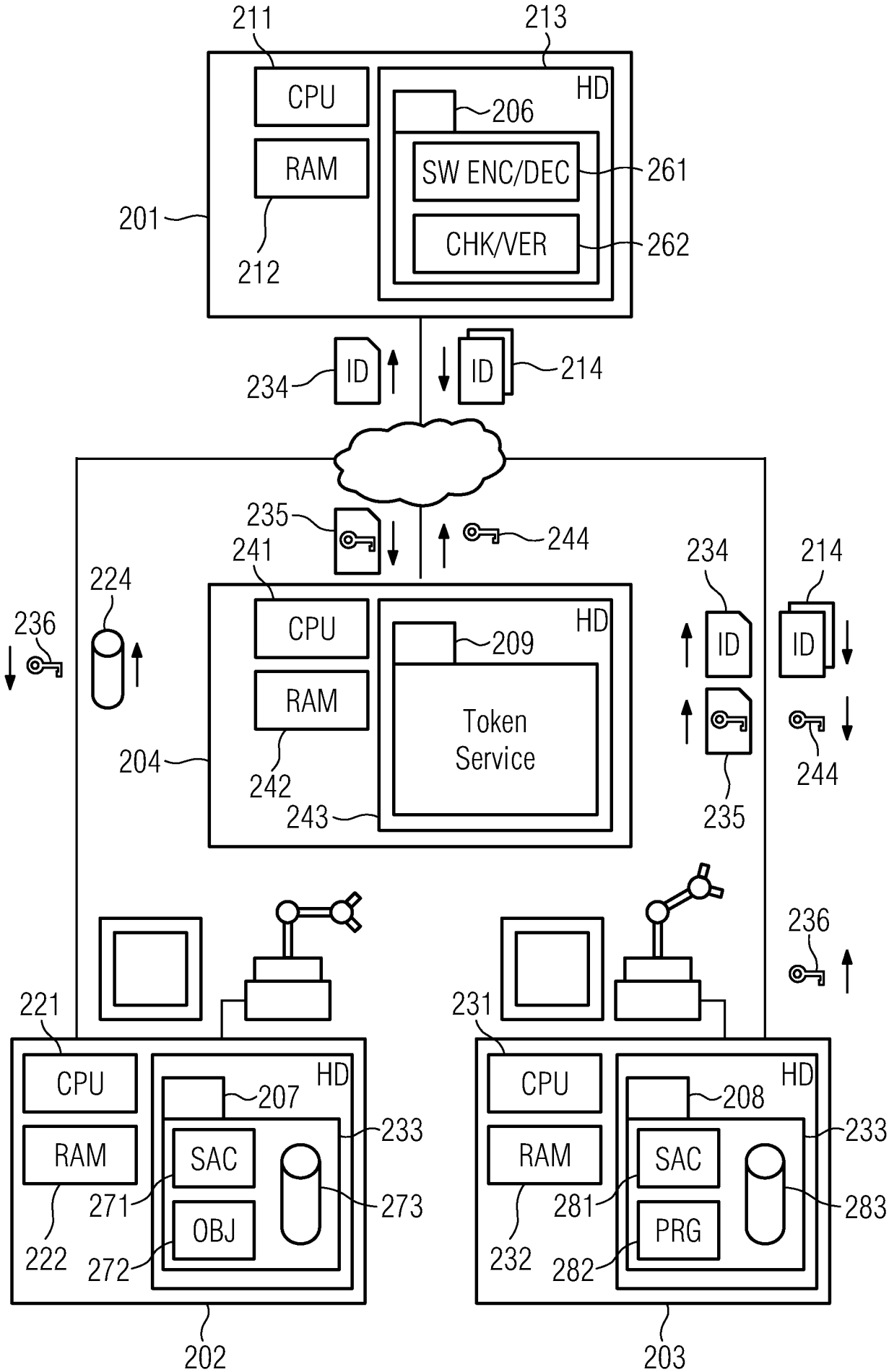

Identifikator ermitteln
101
102
Authentifizie-
rungsanfrage?
N
J
Identifikator verifizieren
103
104
Verifizierung
erfolgreich?
N
Token übermitteln
105
106
Zugriffs-
aufforderung?
N
J
Token überprüfen
107
108
Überprüfung
erfolgreich?
N
Ende
110
J
Zugriff einräumen
109

FIG 2


211
213
CPU
HD
206
RAM
SW ENC/DEC
261
201
CHK/VER
262
212
234
ID
ID
214
235
244
241
224
234
214
236
CPU
HD
209
ID
ID
RAM
Token
Service
204
242
243
244
235
236
221
231
CPU
HD
207
208
CPU
HD
233
RAM
SAC
233
271
273
281
283
OBJ
PRG
222
272
232
282
202
203

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2009/061328

A. CLASSIFICATION OF SUBJECT MATTER
INV. G05B19/406 G05B19/418 G06F21/00 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G05B H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 1 624 350 A (SIEMENS AG [DE]) 8 February 2006 (2006-02-08) paragraphs [0005] - [0015], [0018], [0022] - [0026]; claims 1-8; figures 1-3	1-3,6-8, 10,13-14
Y	EP 1 621 944 A (ROCKWELL AUTOMATION TECH INC [US]) 1 February 2006 (2006-02-01) paragraphs [0054] - [0056]	1,9,13
Y	EP 1 496 664 A (SIEMENS AG [DE]) 12 January 2005 (2005-01-12) paragraphs [0006], [0007], [0012] - [0014], [0018] - [0021], [0030] - [0035], [0039], [0041] - [0043], [0046]; figures 1-4	1-3,10, 13-14

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 October 2009	02/11/2009

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Hristov, Stefan

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2009/061328

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 2008/022606 A (SIEMENS AG [DE]; GERLACH HENDRIK [DE]; TALANIS THOMAS [DE]) 28 February 2008 (2008-02-28) page 2, line 30 - page 6, line 38 page 7, lines 16-26 page 8, line 8 - page 9, line 28 page 15, line 8 - page 16, line 23; figure 1	1,3,8, 10,13-14
Y	EP 1 696 378 A (NOVELL INC [US]) 30 August 2006 (2006-08-30) paragraphs [0005], [0009], [0013] - [0015], [0018] - [0021], [0024], [0026], [0034] - [0036], [0039], [0046], [0048], [0050]; figures 1-4	1-2,6-7, 9
Y	DE 102 00 681 A1 (SIEMENS AG [DE]) 31 July 2003 (2003-07-31) the whole document	1
A	US 2005/287990 A1 (MONONEN RISTO [FI] ET AL) 29 December 2005 (2005-12-29) the whole document	1-14

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2009/061328

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1624350 A	08-02-2006	US 2006026436 A1	02-02-2006
EP 1621944 A	01-02-2006	CN 1737719 A	22-02-2006
		US 2006026672 A1	02-02-2006
EP 1496664 A	12-01-2005	DE 10331307 A1	10-02-2005
WO 2008022606 A	28-02-2008	DE 112006004090 A5	30-07-2009
EP 1696378 A	30-08-2006	US 2006195347 A1	31-08-2006
DE 10200681 A1	31-07-2003	NONE	
US 2005287990 A1	29-12-2005	CN 1977514 A	06-06-2007
		EP 1763947 A1	21-03-2007
		WO 2006003499 A1	12-01-2006

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2009/061328

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. G05B19/406 G05B19/418 G06F21/00 H04L29/06

Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
G05B H04L G06F

Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	EP 1 624 350 A (SIEMENS AG [DE]) 8. Februar 2006 (2006-02-08) Absätze [0005] - [0015], [0018], [0022] - [0026]; Ansprüche 1-8; Abbildungen 1-3	1-3,6-8, 10,13-14
Y	EP 1 621 944 A (ROCKWELL AUTOMATION TECH INC [US]) 1. Februar 2006 (2006-02-01) Absätze [0054] - [0056]	1,9,13
Y	EP 1 496 664 A (SIEMENS AG [DE]) 12. Januar 2005 (2005-01-12) Absätze [0006], [0007], [0012] - [0014], [0018] - [0021], [0030] - [0035], [0039], [0041] - [0043], [0046]; Abbildungen 1-4	1-3,10, 13-14

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen [X] Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
26. Oktober 2009	02/11/2009

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Hristov, Stefan

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	WO 2008/022606 A (SIEMENS AG [DE]; GERLACH HENDRIK [DE]; TALANIS THOMAS [DE]) 28. Februar 2008 (2008-02-28) Seite 2, Zeile 30 - Seite 6, Zeile 38 Seite 7, Zeilen 16-26 Seite 8, Zeile 8 - Seite 9, Zeile 28 Seite 15, Zeile 8 - Seite 16, Zeile 23; Abbildung 1	1,3,8, 10,13-14
Y	EP 1 696 378 A (NOVELL INC [US]) 30. August 2006 (2006-08-30) Absätze [0005], [0009], [0013] - [0015], [0018] - [0021], [0024], [0026], [0034] - [0036], [0039], [0046], [0048], [0050]; Abbildungen 1-4	1-2,6-7, 9
Y	DE 102 00 681 A1 (SIEMENS AG [DE]) 31. Juli 2003 (2003-07-31) das ganze Dokument	1
A	US 2005/287990 A1 (MONONEN RISTO [FI] ET AL) 29. Dezember 2005 (2005-12-29) das ganze Dokument	1-14

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2009/061328

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 1624350 A	08-02-2006	US 2006026436 A1	02-02-2006
EP 1621944 A	01-02-2006	CN 1737719 A	22-02-2006
		US 2006026672 A1	02-02-2006
EP 1496664 A	12-01-2005	DE 10331307 A1	10-02-2005
WO 2008022606 A	28-02-2008	DE 112006004090 A5	30-07-2009
EP 1696378 A	30-08-2006	US 2006195347 A1	31-08-2006
DE 10200681 A1	31-07-2003	KEINE	
US 2005287990 A1	29-12-2005	CN 1977514 A	06-06-2007
		EP 1763947 A1	21-03-2007
		WO 2006003499 A1	12-01-2006