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

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

PCT

(43) Internationales Veröffentlichungsdatum
28. Februar 2008 (28.02.2008)

(10) Internationale Veröffentlichungsnummer
WO 2008/022606 A1

(51) **Internationale Patentklassifikation:**
G05B 19/05 **(2006.01)** ***G05B 19/418*** **(2006.01)**
G06F 21/00 **(2006.01)** ***H04L 29/06*** **(2006.01)**

(21) **Internationales Aktenzeichen:** **PCT/DE2006/001481**

(22) Internationales Anmeldedatum:
23. August 2006 (23.08.2006)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(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):* **GERLACH, Hendrik** [DE/DE]; Oppelner Str. 7, 91058 Erlangen (DE). **TALANIS, Thomas** [DE/DE]; Adenauerstr. 22, 91336 Heroldsbach (DE).

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

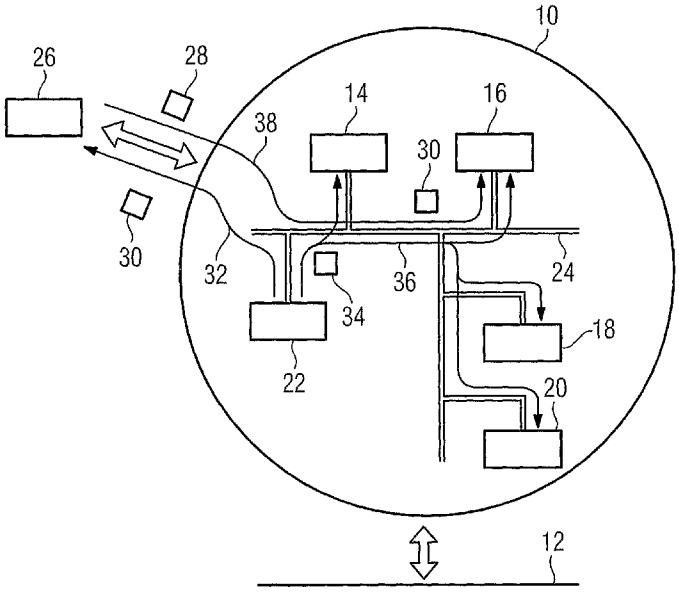
(81) **Bestimmungsstaaten** *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart):* AE, AG, AL, AM, AT, AU, AZ, BA, **BB,** BG, **BR,** BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, **DK,** DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HN, **HR,** HU, **ID, IL,** IN, **IS, JP,** KE, KG, KM, KN, **KP, KR,** KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, **PH,** PL, PT, **RO,** RS, RU, SC, SD, SE, SG, SK, SL, SM, 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, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC,

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD FOR AUTHENTICATION IN AN AUTOMATION SYSTEM

(54) Bezeichnung: VERFAHREN ZUR AUTHENTIFIZIERUNG IN EINEM AUTOMATISIERUNGSSYSTEM



(57) Abstract: The invention specifies a method for authenticating a Communications subscriber (26), also referred to as a client, in an automation System (10) with automation appliances (14, 16, 18, 20) which are connected to one another for the purpose of communication, in which the Communications subscriber (26) sends an identifier (28) to the automation System (10), the identifier (28) is checked in the area of the automation System (10) and, if the check is successful, a certificate (30) is produced or selected and is transmitted to the Communications subscriber (26), and the client can be authenticated to a respective target appliance by transmitting the certificate (30) to said appliance, particularly one of the automation appliances (14-20).

[Fortsetzung auf der nächsten Seite]

WO 2008/022606 A1

NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

Veröffentlicht:
— *mit internationalem Recherchenbericht*

(57) Zusammenfassung: Es wird ein Verfahren zur Authentifizierung eines auch als Client bezeichneten Kommunikations teilnehmers (26) in einem Automatisierungssystem (10) mit untereinander kommunikativ verbundenen Automatisierungsgerate (14, 16, 18, 20) angegeben, bei dem der Kommumkationsteilnehmer (26) eine Kennung (28) an das Automatisierungssystem (10) sendet, im Bereich des Automatisierungssystems (10) die Kennung (28) überprüft und bei erfolgreicher Prüfung ein Zertifikat (30) erzeugt oder ausgewählt und dieses dem Kommumkationsteilnehmer (26) übermittelt wird, und dass das Zertifikat (30) zur Authentifizierung des Clients gegenüber einem jeweiligen Zielgerat an dieses, insbesondere eines der Automatisierungsgerate (14-20), ubermittelbar ist

Beschreibung

Verfahren zur Authentifizierung in einem Automatisierungs¬system

Die Erfindung betrifft ein Verfahren zur Authentifizierung eines Kommunikationsteilnehmers in einem Automatisierungssys¬tem.

Als Automatisierungssystem wird dabei eine Mehrzahl unterein¬ander kommunikativ verbundener Automatisierungsgeräte sowie ggf. weiterer Geräte aufgefasst, die einzeln oder in Kombina¬tion zur Steuerung und/oder Überwachung eines technischen Prozesses bestimmt sind. Der Begriff „Automatisierungsgerät" umfasst sämtliche Geräte, Einrichtungen oder Systeme, also neben z. B. Steuerungen, wie speicherprogrammierbaren Steue–rungen, Prozessrechnern, (Industrie-) Computern, dezentralen Peripheriegeräten, Bedien- und Beobachtungsgeräten und der¬gleichen auch Antriebs- oder sonstige Aggregat Steuerungen, Frequenzumrichter und Ähnliches, wie sie zur Steuerung, Rege¬lung und/oder Überwachung technologischer Prozesse z. B. zum Umformen oder Transportieren von Material, Energie oder In¬formation etc. eingesetzt werden oder einsetzbar sind, wobei insbesondere über geeignete technische Einrichtungen, wie z. B. Sensoren oder Aktoren, Energie aufgewandt oder gewan–delt wird. Als Automatisierungsgeräte werden dabei auch sol¬che Kommunikationsteilnehmer in einem Automatisierungssystem aufgefasst, die nicht unmittelbar mit dem jeweiligen techni¬schen Prozess interagieren, sondern z. B. zu Diagnosezwecken oder für Bedien- und Beobachtungsfunktionen, ggf. auch nur temporär, Bestandteil des Automatisierungssystems sind.

Ethernet- und IP-Kommunikation dringt im Bereich der Automa¬tisierungstechnik auch auf die so genannte Feldbus-Ebene, al–so z. B. bis auf das Niveau einzelner Automatisierungszellen, vor. Damit werden die Sicherheitsbedrohungen über Netzwerk¬verbindungen auch für die Feldebene relevant. Diese neuen Be–drohungen erhöhen die Ansprüche an den Schutz von Automat!-

sierungsgeräten. Neben anderen Sicherheitsmechanismen spielt dabei auch der Zugriffsschutz auf Basis von Rechten eine zentrale Rolle. Für einen Zugriffsschutz muss ein Client (ein Bediener/Benutzer oder ein von diesem verwendetes Gerät) zunächst identifiziert und authentifiziert werden, wobei die Authentifizierung als Nachweis dafür gilt, dass der jeweilige Client derjenige ist, für den er sich ausgibt, ehe auf dieser Basis eine Rechtzuteilung, also eine Autorisierung, erfolgen kann.

Automatisierungsgeräte sind bisher, wenn überhaupt, durch vergleichsweise einfache Mechanismen, z. B. Passworte, in besonderen Ausführungsformen dezentral gespeicherte Passworte, geschützt. Der jeweilige Client muss sich beim Zugriff auf solche Geräte immer wieder neu authentifizieren. Zur Unterstützung solcher Bedienvorgänge sind Hilfsmittel bekannt, die z. B. ein zuletzt verwendetes Passwort temporär Zwischenspeichern („cachen"). Speziell eine dezentrale Speicherung der Passworte erschwert jedoch deren Verwaltung. Weiterhin ist es schwierig, die Konsistenz der Passwörter in einem Automatisierungssystem oder Automatisierungsverbund manuell sicherzustellen. Der Begriff Automatisierungsverbund wird hier und im Folgenden z. B. für ein Automatisierungssystem verwendet, das zur Steuerung und/oder Überwachung einer einen großräumigen technischen Prozess umfassenden Gesamtanlage vorgesehen ist. Ein Automatisierungssystem wird im Folgenden auch kurz einfach als System bezeichnet. Entsprechendes gilt auch für Begriffe wie Automatisierungsverbund oder dergleichen.

Bei dem Verfahren, auf das sich die Erfindung bezieht, steht im Vordergrund, dass eine Authentifizierung in dem Automatisierungssystem (Kommunikationsverbund), also mit Wirkung für das System oder gegenüber dem System erfolgt. D. h. eine mehrfache Authentifizierung gegenüber einer Mehrzahl von einzelnen Geräten, die als Kommunikationsteilnehmer in dem System fungieren, soll vermieden werden. Eine solche, einmalige Authentifizierung wird nach dem mittlerweile üblichen Sprachgebrauch mit dem eingeführten Begriff als „Single-Sign-On"

(SSO) bezeichnet. Entsprechend wird dieser Begriff auch im Folgenden verwendet .

Verfahren zum „Single-Sign-On" sind allgemein, z . B . aus der WO 00/67415, bekannt.

Eine Aufgabe der Erfindung besteht darin, die Vorteile, die sich durch eine nur einmalige Authentifizierung (Single-Sign-On) ergeben, auch im Bereich der Automatisierungstechnik bereitzustellen. Als Vorteil ist dabei insbesondere eine erleichterte Bedienbarkeit oder die Vermeidung des mit der Notwendigkeit, sich eine Vielzahl von Zugangsberechtigungsinformationen merken zu müssen, einhergehenden Wachteils zu nennen.

Diese Aufgabe wird erfindungsgemäß mit den Merkmalen des Anspruchs 1 gelöst. Dazu ist bei einem Verfahren zur Authentifizierung eines Kommunikationsteilnehmers in oder gegenüber einem Automatisierungssystem mit einer Mehrzahl kommunikativ verbundener Automatisierungsgeräte in einem ersten Schritt vorgesehen, dass der Kommunikationsteilnehmer eine Kennung an das Automatisierungssystem sendet. Der Kommunikationsteilnehmer ist dabei ein dauerhaft oder temporär mit dem Automatisierungssystem kommunikativ verbundenes Gerät, z . B . ein Programmiergerät , mit dem ein Benutzer Zugriff auf das Automatisierungssystem und davon zumindest temporär umfasste Automatisierungsgeräte nehmen kann. Die durch den Kommuni kationsteilnehmer an das Automatisierungssystem gesendete Kennung identifiziert entweder das jeweilige Gerät oder den Benutzer oder beides, nachfolgend zusammenfassend als „Client" bezeichnet. Eine solche Kennung kann einen Benutzernamen und ein Passwort umfassen. Diese Kennung wird in einem nächsten Schritt im Bereich des Automatisierungssystems, also z . B . durch ein vom Automatisierungssystem umfasstes Gerät, überprüft. Bei erfolgreicher Prüfung, wenn also die Kennung für das Automatisierungssystem zugelassen ist, wird in einem weiteren Schritt ein Zertifikat erzeugt oder ein bereits erzeugtes Zertifikat ausgewählt. Das Erzeugen oder Auswählen des

Zertifikats erfolgt dabei anhand der Kennung. Daraufhin wird in einem nochmals weiteren Schritt das Zertifikat dem Kommunikationsteilnehmer/Client übermittelt. Dieser kann in einem nicht notwendig unmittelbar anschließenden Schritt das Zertifikat an sämtliche von dem Automatisierungssystem umfassten Kommunikations teilnehmer, also insbesondere die darin kommunikativ untereinander verbundenen Automatisierungsgeräte, übermitteln. Eine Übermittlung des Zertifikats an einen Kommunikationsteilnehmer in dem Automatisierungssystem, im Folgenden als „Zielgerät" bezeichnet, führt normalerweise zu einer Authentifizierung des Kommunikationsteilnehmers/Clients, der das Zertifikat übermittelt. Wenn das Zielgerät eines der von dem Automat isierungs system umfassten Automatisierungsgeräte ist, ist der Client damit für das jeweilige Automatisierungsgerät, also einen Zugriff auf dieses Gerät, authentifiziert .

Die weiter oben genannten Probleme werden durch das vorstehende .Verfahren, sowie ein Gerät oder ein System, mit dem oder durch das das Verfahren implementiert wird, gelöst, indem es dem Client erlaubt, sich einmalig zu authentifizieren und dann auf Basis dieser Authentifizierung auf Komponenten des Automatisierungssystems zuzugreifen. Der Zugriff erfolgt dann üblicherweise unter Prüfung von Rechten, die dem Client auf Basis seiner Authentifizierung zugeteilt werden. Der Begriff Komponenten schließt alle Geräte ein, die direkt oder indirekt zur Erfüllung von Automatisierungsaufgaben dienen, also z . B . Automatisierungsgeräte, aber auch z . B . Netzwerkkomponenten und dergleichen. Der Begriff der einmaligen Authentif izierung ist hier und im Folgenden in dem Sinne zu verstehen, dass sich der Client einmal anmeldet und dann auf andere Komponenten zugreifen kann, ohne sich erneut zu authentifizieren. Dies schließt jedoch nicht aus, dass die erworbene Authentifizierung eine zeitliche Beschränkung hat, nach deren Ablauf eine erneute Authentifizierung notwendig werden kann.

Zur sprachlichen Unterscheidung soll hier noch die Bezeichnung „Automatisierungsdomäne" eingeführt werden, die einen gemeinsamen, so genannten Vertrauensbereich bezeichnet, in dem sich Geräte oder Komponenten mit automatisierungstechnischer Funktion befinden. Die Bezeichnungen Automatisierungsdomäne und Automatisierungssystem werden dabei synonym verwendet. Innerhalb der Automatisierungsdomäne ist eine einmal erworbene Authentifizierung eines Clients überall gültig, d. h. alle Geräte „vertrauen" einer gemeinsamen Instanz, die von dem Automatisierungssystem umfasst ist und auch Basis für die Durchführung der Authentifizierung ist. Eine zur Automatisierung eines technischen Prozesses vorgesehene Automatisierungslösung kann eine oder auch mehrere Automatisierungsdomänen umfassen.

Ein wesentlicher Vorteil der erfindungsgemäßen Lösung besteht darin, dass sich der Client nicht an jedem Gerät neu anmelden/authentifizieren muss, sondern eine einmalige Anmeldung an der Automatisierungsdomäne, also eine Authentifizierung in oder gegenüber dem jeweiligen Automatisierungssystem, ausreicht. Darüber hinaus ergibt sich eine einfache Benutzerverwaltung, die zentral für die gesamte Automatisierungsdomäne erfolgen kann und damit nicht auf jedem einzelnen Gerät oder mit Wirkung für jedes einzelne Gerät erfolgen muss und eine damit einhergehende erhöhte Sicherheit und bessere Konsistenz. Letzteres wirkt sich besonders bei der Benutzerverwaltung aus, wenn z. B. ein neuer Client für die Automatisierungsdomäne zugelassen oder eine Berechtigung eines zukünftig nicht mehr zugelassenen Clients zurückgenommen werden soll. Bei neu in die Automatisierungsdomäne eingefügten Geräten benötigen diese keinen Passwortsatz. Zudem muss sich der jeweilige Client nur ein Passwort merken, woraus sich für diesen nicht nur eine Zeitersparnis ergibt.

Zweckmäßige Weiterbildungen dieses Verfahrens sind Gegenstand weiterer Ansprüche.

Bevorzugt umfasst das Automatisierungssystem zumindest einen Authentifizierungsserver, wobei die Kennung durch den jeweiligen Koxnmunikationsteilnehmer/Client an den Authentifizierungsserver gesandt wird und das Zertifikat daraufhin vom Authentifizierungsserver erzeugt oder ausgewählt wird. Auf diese Art und Weise werden die vom Automatisierungssystem umfassten Geräte, insbesondere die zur Steuerung und/oder Überwachung des technischen Prozesses vorgesehenen Automatisierungsgeräte, von administrativen Funktionen, wie z. B. der Authentifizierung von Geräten oder Nutzern (Clients), entlastet. Des Weiteren kann die Erzeugung, Auswahl und Speicherung von Zertifikaten einem dafür vorgesehenen Gerät oder einer Gerätegruppe, nämlich dem Authentifizierungsserver, zugewiesen werden, so dass insoweit auch eine Trennung zwischen „Automatisierungsressourcen" und „Administrationsressourcen" möglich wird. Bevorzugt sind zumindest dem Authentifizierungsserver zumindest ein privater Schlüssel und ein zu dem oder jedem privaten Schlüssel gehöriger öffentlicher Schlüssel zugeordnet. Der Authentifizierungsserver signiert das ausgewählte oder erzeugte Zertifikat mit dem oder einem privaten Schlüssel. Dieser ist im Automatisierungssystem bekannt oder wird im Automatisierungssystem, z. B. nach Auswahl oder Erzeugung des Zertifikats oder im Zusammenhang mit der Signierung des Zertifikats, bekannt gemacht. Eine solche Bekanntmachung erfolgt zweckmäßig indem der zu dem bei der Signierung verwendeten privaten Schlüssel gehörige öffentliche Schlüssel an die anderen Kommunikationsteilnehmer in dem Automatisierungssystem, insbesondere die davon umfassten Automatisierungsgeräte, übermittelt wird.

Das Zertifikat fungiert dabei für den Kommunikationsteilnehmer, der um eine Authentifizierung in dem Automatisierungssystem oder für das Automatisierungssystem nachsucht, als Soft-Token, das zum Nachweis der Authentizität einzelnen oder mehreren Geräten in dem Automatisierungssystem „vorgelegt", d. h. übermittelt, werden kann. Mit der Signierung wird das Zertifikat zu einem Soft-Token, das gegen Veränderung geschützt ist. Eine Signierung einer Dateneinheit ist an sich

bekannt und auch im Zusammenhang mit der beschriebenen Ausführungsform der vorliegenden Erfindung kommen die bekannten Signaturverfahren grundsätzlich in Betracht. Ebenfalls bekannt ist das Erkennen von eventuellen Veränderungen von Dateneinheiten anhand der jeweiligen Signatur. Auch diese insoweit bekannten Verfahren sollen im Zusammenhang mit dieser Ausführungsform der Erfindung eingesetzt werden.

Zur Übermittlung des Zertifikats, insbesondere zur Übermittlung des signierten Zertifikats durch den Client an ein Zielgerät oder auch bereits bei der erstmaligen Übermittlung an den Client, wird bevorzugt ein sicherer Kommunikationskanal verwendet. Auf diese Art und Weise wird z. B. sichergestellt, dass keine unberechtigten Benutzer in den Besitz des Zertifikats kommen können. Zumindest wird ein solcher unberechtigter Zugriff erschwert. Auf Seiten des Automatisierungssystems wird im Zusammenhang mit einer Übermittlung des Zertifikats durch den Client an ein Zielgerät das Zertifikat anhand von Zusatzinformationen über den Ursprung des Zertifikats durch das jeweilige Zielgerät entweder abgewiesen oder akzeptiert. Diese Zusatzinformationen beziehen sich dabei bevorzugt auf die Signierung des Zertifikats durch insbesondere den Authentifizierungsserver, wobei z. B. das Zielgerät die Signatur des übermittelten Zertifikats anhand des durch den Authentifizierungsserver bekannt gemachten öffentlichen Schlüssels überprüft.

Zwischen dem jeweiligen Kommunikationsteilnehmer einerseits, also dem Client, und dem Automatisierungssystem andererseits, insbesondere dem Authentifizierungsserver, sowie nachfolgend zwischen Client und dem jeweiligen Zielgerät oder zwischen dem Authentifizierungsserver und anderen, als Zielgerät in Frage kommenden Kommunikationsteilnehmern im Automatisierungssystem, werden sensitive Daten übertragen, für die je nach Anwendungsszenario des Automatisierungssystem eine starke Authentifizierung erforderlich sein kann. Entsprechend ist gemäß der Erfindung vorgesehen, diese Kommunikationsbeziehungen auch bei einer Kommunikation im Rahmen des Single-Sign-On

mit sicheren Kanälen zu schützen, um eine sichere Authentifizierung oder Autorisierung zu ermöglichen. Zur Kanal Sicherung kann SSL, IPSEC, Kerberos oder dergleichen verwendet werden. Mit der Verwendung sicherer Kanäle ist neben dem primären Sicherheitsgewinn der Vorteil verbunden, dass die übertragenen Informationen nicht applikativ gesichert werden müssen.

Auf Basis des so genannten SSL-Protokolls zum Aufbau eines sicheren Kommunikationskanals ergibt sich danach z. B. folgendes Szenario: Ein Client arbeitet an einem zumindest temporär an einem Automatisierungssystem angeschlossenen Kommunikationsteilnehmer, z. B. einem Programmiergerät. Von dort aus authentifiziert sich der Client gegenüber dem Automatisierungssystem, z. B. am Authentifizierungsserver . Diese Authentifizierung erfolgt unter Anwendung üblicher Mechanismen durch Übertragung einer benutzerspezifischen Kennung. Eine solche Kennung kann z. B. Benutzernamen und/oder Passwort, oder eine so genannte RFID, etc. umfassen oder auf biometrische Daten oder dergleichen gestützt sein. Diese Authentifizierungsinformationen werden zwischen Client und Authentifizierungsserver üblicherweise auf einen gesicherten Kanal übertragen. Hierfür wird ein SSL-Kanal genutzt. Nach erfolgreicher Authentifizierung generiert der Authentifizierungsserver ein diesbezügliches Zertifikat für den Client, das dieser über den gesicherten Kanal zurück erhält. Dieses Zertifikat kann der Nutzer nachfolgend zum Nachweis seiner Authentizität bei anderen Kommunikationsteilnehmern im Automatisierungssystem, z. B. vom Automatisierungssystem umfassten Automatisierungsgeräten, vorlegen. Das Zertifikat kann in lokalen, so genannten Certificate Stores des Clients installiert werden. Das ausgestellte Zertifikat wird vom Authentifizierungsserver signiert. Dazu verwendet der Authentifizierungsserver einen privaten Schlüssel. Der zugehörige öffentliche Schlüssel wird in Form eines so genannten Stammzertifikats an alle Mitglieder der Automatisierungsdomäne, also insbesondere die vom Automatisierungssystem umfassten Automatisierungsgeräte, verteilt. Dies kann auch in einem vorgelager-

ten Konfigurationsschritt, z. B. während einer so genannten Projektierung, erfolgen.

Wenn der Client auf einen als Zielgerät fungierenden Kommunikationsteilnehmer im Automatisierungssystem, z. B. ein Automatisierungsgerät, zugreifen will, wird dieses Zertifikat „vorgelegt", also durch den Client an das jeweilige Zielgerät übermittelt. Ein damit auf diese Weise vom Client initiierter Request veranlagst den Aufbau eines sicheren so genannten SSL-Tunnels zwischen Client und Zielgerät. Über diesen sicheren Kanal wird das Zertifikat des Clients zum Zielgerät übertragen und kann dort zur Zuweisung und/oder zum Prüfen entsprechender Berechtigungen führen, ohne dass der Client sich erneut an dem jeweiligen Zielgerät oder am Authentifizierungsserver anmelden muss.

Das Zielgerät wird in der Regel nicht jedem vorgelegten Zertifikat vertrauen, sondern prüfen, ob es sich bei dem jeweiligen Aussteller, also der Quelle des Zertifikats, um eine vertrauenswürdige so genannte Standzertifizierungsstelle handelt, wobei sich die Vertrauenswürdigkeit z. B. daraus ergeben kann, dass der Aussteller der Authentifizierungsserver der eigenen Domäne ist. Liegt daraufhin sowohl ein gültiges, wie auch vertrauenswürdiges Zertifikat vor, kann der Client im Rahmen der ihm zugewiesenen Rechte auf das Zielgerät zugreifen, ohne dass dazu eine weitere Authentifizierung erforderlich gewesen wäre.

Der Vorteil des Verfahrens gemäß der beschriebenen Ausführungsform der Erfindung gegenüber anderen Single-Sign-On-Verfahren - wie z. B. Kerberos - liegt darin, dass es sich bei dem SSL-Protokoll um ein weit verbreitetes Protokoll handelt, das auf einer Vielzahl von Geräten verfügbar ist. SSL ermöglicht das transparente Verpacken von TCP-Telegrammen in einem SSL-Kanal, so dass für TCP-basierte Applikationen keinerlei Modifikationen erforderlich sind. Der Einsatz von z. B. Kerberos erfordert in der Regel eine Anpassung des je-

weiligen Applikationsprotokolls, wobei man bei Kerberos von einer „Kerberisierung" spricht.

In einer besonders bevorzugten Ausführungsform des Ansatzes gemäß der Erfindung handelt es sich bei dem Zertifikat um ein so genanntes X509~Zertifikat, das zum Nachweis der Authentizität des Clients verwendet wird. Zertifikate, und damit insbesondere X509-Zertifikate, lassen sich unter Verwendung von insbesondere gesicherten Datenübertragungsprotokollen, z. B. SSL, vergleichsweise einfach zu einem der Automatisierungsgeräte im Automatisierungssystem transportieren, wo anhand des Zertifikats die Authentifizierung des Clients, also des Kommunikationsteilnehmers, von dem das Zertifikat gesendet wird, überprüft wird. Zertifikate können in unter vielen Plattformen vorhandenen gesicherten Speicherbereichen hinterlegt werden, so dass einerseits ein Zugriffsschutz besteht und andererseits eine Kompatibilität zu vorhandenen Plattformen gewährleistet ist.

Eine Alternative zu der Verwendung von X509-Zertifikaten besteht in der Verwendung so genannter Kerberos-Trust-Mechanismen, die in Büroumgebungen häufig im Zusammenhang mit einer Authentifizierung zum Einsatz kommen. Gemäß einer weiteren Ausführungsform der Erfindung ist entsprechend vorgesehen, dass ein insbesondere in einer Büroumgebung erworbener Authentifizierungsnachweis in Form eines so genannten Kerberos-Tickets für die Authentifizierung in einer Automatisierungsdomäne verwendet wird. Dazu werden Kerberos-Trust-Mechanismen verwendet, deren Vorteil vor allem in der vergleichsweise einfachen Realisierbarkeit besteht, wenn Kerberos bereits auf den beteiligten Geräten implementiert ist. Darüber hinaus ergibt sich eine InterOperabilität mit Domänen, die auf Betriebssystemen wie Windows, UNIX, o. ä. basieren, in denen die Clients dann nicht doppelt geführt werden müssen. Des Weiteren besteht eine Möglichkeit der Trennung der Benutzerverwaltung, z. B. derart, dass die Automatisierungsdomäne der Bürodomäne „vertraut", aber nicht umgekehrt, so dass in der Bürodomäne nicht bekannte Clients, z. B. temporäre

Clients mit Wartungsaufgaben, nur in der Automatisierungsdomäne verwaltet werden.

Kerberos nutzt standardmäßig so genannte „Shared Secrets". Kerberos ist zudem nach bestem Wissen der Anmelderin in Automatisierungsgeräten bisher noch nicht eingesetzt worden, da dieses erhebliche Probleme, unter anderem im Zusammenhang mit einer so genannten Kerberisierung der Applikationsprotokolle, mit sich bringt. Dem gegenüber hat die alternative Verwendung von X509-Zertifikaten den Vorteil, dass sich ein so genanntes Trust-Verhältnis einfach anhand der jeweiligen Signatur prüfen lässt und kein Rückgriff auf Shared Secrets oder dergleichen erforderlich ist. Es müssen insoweit keine sensitiven Daten, nämlich z.B. die Shared Secrets, auf sicherem Weg zwischen den beteiligten Kommunikationsteilnehmern übertragen werden. Im Gegensatz zu den Shared Secrets müssen besondere Stammzertifikate nicht in einem sicheren Speicher gehalten werden, da sie keine geheimen Informationen erhalten. Im Gegensatz zu Shared Secrets können Zertifikate eine zeitliche Begrenzung der Gültigkeitsdauer haben. Selbst wenn unberechtigte Dritte Zugriff auf Zertifikate erhalten, ist damit ein eventuell unberechtigter Zugriff nur zeitlich begrenzt möglich. Unter Nutzung einer so genannten PKI-Infrastruktur können Stammzertifikate zurückgezogen werden, wenn ein Authentifizierungsserver oder dessen öffentlicher Schlüssel kompromittiert wurde. Alle von ihm ausgestellten Zertifikate werden dann ungültig und dem Authentifizierungsserver kann ein neuer privater Schlüssel zugewiesen werden, so dass auf dessen Basis neue Zertifikate ausstellbar sind, mit denen sich Clients dann wieder authentifizieren können.

In einer besonders bevorzugten Ausführungsform kann vorgesehen sein, dass nach einer einmaligen Zertifizierung eines Clients dessen weitere Autorisierung oder Authentifizierung nur noch, also ausschließlich, zertifikatsbasiert erfolgt. Als Vorteil ist damit eine Durchgängigkeit des Konzepts verbunden, wobei zusätzlich keine Shared Secrets für die Authen-

tifizierung bei den jeweiligen Geräten, auf die ein Zugriff erfolgen soll, nötig ist.

Zur weiteren Erhöhung der Sicherheit kann vorgesehen sein, dass das Single-Sign-On-System so ausgelegt ist, dass die vom Authentifizierungsserver für den Client ausgestellten Zertifikate eine festgelegte oder festlegbare Gültigkeitsdauer haben. Nach Ablauf der Gültigkeitsdauer benötigt der Client ein neues Zertifikat, um weiterhin Zugriff auf das Automatisierungssystem zu bekommen. In einer besonders bevorzugten Ausführungsform kann dazu vorgesehen sein, dass ein solches neues Zertifikat unter Verwendung eines alten, insbesondere abgelaufenen oder kurz vor Ablauf stehenden Zertifikats beim Authentifizierungsserver angefordert wird. Eine solche Anforderung kann automatisch erfolgen. Damit ist der Vorteil verbunden, dass der Client sein Passwort auch bei einer erforderlichen Erneuerung des Zertifikats nicht noch einmal angeben muss .

Die Verwendung von gegen Veränderung geschützten Zertifikaten, also insbesondere von X509-Zertif ikaten, kommt auch für die Sicherung von Autorisierungsinf ormationen für den Zugriff auf Automatisierungskomponenten in Betracht. Autorisierungsinformationen können Privilegien, Rechte, so genannte Rollen, usw. sein. Damit ist auch der Transfer solcher Autorisierungsinf ormationen in besonderer Weise gesichert. Bei dieser Ausgestaltung des erfindungsgemäßen Verfahrens ist z . B . folgendes Szenario denkbar: Der Client meldet sich an einem Authentifizierungsserver an und erhält von diesem ein Zertifikat zurück, das ihn zukünftig als authentifizierten Client ausweist. Der Authentifizierungsserver hat das Zertifikat signiert, so dass jedes Zielgerät prüfen kann, ob die Authentifizierung als vertrauenswürdig eingestuft wird. Im Zertifikat sind nun ein oder mehrere Rollen hinterlegt. Eine dieser Rollen umfasst z . B . Informationen, wie „Bediener", „Wartungspersonal" oder dergleichen. Diese Rolleninformation wird mit der Übertragung des Zertifikats an das Zielgerät übermittelt. Das Zielgerät extrahiert nach einer Verifikation der

Authentifizierung die Rolleninformation. Anhand lokal hinterlegter Rechte-Tabellen kann das Zielgerät nun dem jeweiligen Client über die Rolle Rechte zuteilen. Damit ergibt sich der Vorteil, dass die Rechte-Tabellen keinerlei Benutzerinformationen umfassen, so dass sie beim Entfernen von Clients oder beim Aufnehmen von neuen Clients nicht geändert werden müssen. Darüber hinaus werden die Rolleninformationen zusammen mit der Authentifizierungsinformation sicher zum jeweiligen Zielgerät übertragen.

Die mit der Anmeldung eingereichten Patentansprüche sind Formulierungsvorschläge ohne Präjudiz für die Erzielung weitergehenden Patentschutzes. Die Anmelderin behält sich vor, noch weitere, bisher nur in der Beschreibung und/oder Zeichnung offenbarte Merkmalskombination zu beanspruchen.

Das oder jedes Ausführungsbeispiel ist nicht als Einschränkung der Erfindung zu verstehen. Vielmehr sind im Rahmen der vorliegenden Offenbarung zahlreiche Abänderungen und Modifikationen möglich, insbesondere solche Varianten und Kombinationen, die zum Beispiel durch Kombination oder Abwandlung von einzelnen in Verbindung mit den im allgemeinen oder speziellen Beschreibungsteil beschriebenen sowie in den Ansprüchen und/oder der Zeichnung enthaltenen Merkmalen bzw. EIementen oder Verfahrensschritten für den Fachmann im Hinblick auf die Lösung der Aufgabe entnehmbar sind und durch kombinierbare Merkmale zu einem neuen Gegenstand oder zu neuen Verfahrensschritten bzw. Verfahrensschrittfolgen führen.

In Unteransprüchen verwendete Rückbeziehungen weisen auf die weitere Ausbildung des Gegenstandes des Hauptanspruches durch die Merkmale des jeweiligen Unteranspruches hin; sie sind nicht als ein Verzicht auf die Erzielung eines selbständigen, gegenständlichen Schutzes für die Merkmalskombinationen der rückbezogenen Unteransprüche zu verstehen. Des Weiteren ist im Hinblick auf eine Auslegung der Ansprüche bei einer näheren Konkretisierung eines Merkmals in einem nachgeordnet en

Anspruch davon auszugehen, dass eine derartige Beschränkung in den jeweils vorangehenden Ansprüchen nicht vorhanden ist.

Nachfolgend wird ein Ausführungsbeispiel der Erfindung anhand der Zeichnung näher erläutert. Einander entsprechende Gegenstände oder Elemente sind in allen Figuren mit den gleichen Bezugszeichen versehen.

Darin zeigt die einzige Figur

FIG 1 eine schematisch vereinfachte Darstellung von Kommunikationsbeziehungen zwischen einem zur Steuerung eines technischen Prozesses vorgesehenen Automatisierungssystem und einem Client, mit dem ein Zugriff auf das Automatisierungssystem erfolgen soll.

FIG 1 zeigt ein Automatisierungssystem 10, das zur Steuerung und/oder Überwachung eines nicht näher dargestellten technischen Prozesses 12 vorgesehen ist. Das Automatisierungssystem 10 umfasst eine Anzahl kommunikativ miteinander verbundener Kommunikationsteilnehmer. Bei einigen der vom Automatisierungssystem 10 umfassten Kommunikationsteilnehmer handelt es sich um Automatisierungsgeräte 14, 16, 18, 20 entsprechend der eingangs angegebenen Definition, nämlich ein erstes und zweites Automatisierungsgerät 14, 16 sowie weitere Automatisierungsgeräte 18, 20. Von dem Automatisierungssystem 10 ebenfalls umfasst ist ein Authentifizierungsserver 22. Die Automatisierungsgeräte 14-20, der Authentifizierungsserver 22, sowie ggf. weitere, nicht dargestellte Geräte oder Komponenten sind kommunikativ über einen Bus 24, insbesondere einen Feldbus, verbunden. Über den Bus 24 ist auch ein dauerhafter oder temporärer Anschluss eines weiteren Kommunikationsteilnehmers *26 an* das Automatisierungssystem 10 möglich.

Für den weiteren Kommunikationsteilnehmer 26 wird für die weitere Beschreibung angenommen, dass dieser von einem Bediener benutzt wird, der Zugriff auf das Automatisierungssystem 10, d.h.z.B. auf zumindest eines der Automatisierungsgerä-

te 14-20, nehmen möchte. Die Bezeichnungen Kommunikations¬teilnehmer oder weiterer Kommunikationsteilnehmer 26, sowie eine Bezeichnung des entsprechenden Gerätes und des das Gerät bedienenden Benutzers, werden im Folgenden synonym verwendet. Zur zusammenfassenden Bezeichnung wird auch der Begriff „Client" verwendet.

Zum Zugriff auf das Automatisierungssystem 10 im Rahmen des erfindungsgemäßen Single-Sign-On Ansatzes übermittelt der Client dem Automatisierungssystem 10 eine Kennung 28 (ver¬deutlicht durch den Doppelpfeil) . Die Kennung 28 wird durch eines der vom Automatisierungssystem 10 umfassten Geräte, im vorliegenden Szenario durch den Authentifizierungsserver 22, empfangen und überprüft. Bei erfolgreicher Prüfung wird ein Zertifikat 30 erzeugt oder ausgewählt. Das Erzeugen oder Aus¬wählen des Zertifikats 30 erfolgt bevorzugt ebenfalls durch den Authentifizierungsserver 22 . Das erzeugte oder ausgewähl¬te Zertifikat 30 wird, insbesondere durch den Authentifizie¬rungsserver 22, an den Client übermittelt (verdeutlicht durch eine erste Kommunikationsbeziehung 32 im Rahmen des Single-Sign-On Verfahrens) .

In einer bevorzugten Ausführungsform ist das dem Client über¬mittelte Zertifikat 30 durch z . B . den Authentifizierungsser-ver 22 signiert. Für eine solche Signierung kommt ein dem Au¬thentifizierungsserver 22 zugeordneter privater Schlüssel (nicht dargestellt) in Betracht. Im Falle eines signierten Zertifikats 30 kann dessen „Unversehrtheit" durch Prüfen der Signatur erkannt werden. Dazu sendet der Authentifizierungs-Server 22 einen zu dem privaten Schlüssel gehörigen öffentli¬chen Schlüssel 34 zumindest auch an die vom Automatisierungs-system 10 umfassten Automatisierungsgeräte 14-20. Bei dieser Übermittlung handelt es sich um eine zweite Kommunikationsbe-ziehung 36 im Rahmen des Single-Sign-On Verfahrens.

Mit dem Erhalt des Zertifikats 30 kann der Client zum Zugriff auf einzelne Komponenten des Automatisierungssystems 10, z . B . eines der Automatisierungsgeräte 14-20, bei diesen, im

Folgenden zur Unterscheidung als Zielgerät bezeichnet, das Zertifikat 30 vorlegen. Bei dieser Übermittlung handelt es sich um eine dritte Kommunikationsbeziehung 38 im Rahmen des Single-Sign-On Verfahrens.

Das jeweilige Zielgerät, im dargestellten Beispiel das zweite Automatisierungsgerät 16, prüft das übermittelte Zertifikat 30, insbesondere anhand des zuvor vom Authentifizierungsserver 22 übermittelten öffentlichen Schlüssels 34. Das Zertifikat 30 wird nach einer solchen Prüfung, sowie ggf. nach einer Prüfung, ob das Zertifikat 30 aus einer als vertrauenswürdig eingestuften Quelle stammt, also insbesondere einem vom Automatisierungssystem 10 selbst umfassten Gerät, nämlich z. B. dem Authentifizierungsserver 22, akzeptiert. Dem jeweiligen Client wird danach Zugriff auf das angesprochene Zielgerät gewährt. Wenn der Client auf andere Zielgeräte zugreifen will, reicht, solange eine eventuell vorgesehene zeitliche Beschränkung der Gültigkeit des Zertifikats 30 nicht abgelaufen ist, eine Vorlage des Zertifikats 30 bei diesem Zielgerät, um darauf Zugriff zu nehmen, insbesondere nachdem im Rahmen einer nachgeschalteten Autorisierung dem Client bestimmte Rechte, insbesondere in Ansehung des übermittelten Zertifikats 30, zugeteilt werden.

Zusammenfassend lässt sich die vorliegende Erfindung damit kurz wie folgt beschreiben: Es wird ein Verfahren zur Authentifizierung eines auch als Client bezeichneten Kommunikationsteilnehmers 26 in einem Automatisierungssystem 10 mit untereinander kommunikativ verbundenen Automatisierungsgeräte 14, 16, 18, 20 angegeben, bei dem der Kommunikationsteilnehmer 26 eine Kennung 28 an das Automatisierungssystem 10 sendet, im Bereich des Automatisierungssystems 10 die Kennung 28 überprüft und bei erfolgreicher Prüfung ein Zertifikat 30 erzeugt oder ausgewählt und dieses dem Kommunikationsteilnehmer 26 übermittelt wird, und dass das Zertifikat 30 zur Authentifizierung des Clients gegenüber einem jeweiligen Zielgerät an dieses, insbesondere eines der Automatisierungsgeräte 14-20, übermittelbar ist.

Patentansprüche

1. Verfahren zur Authentifizierung eines Kommunikationsteilnehmers (26) in einem Automatisierungssystem (10) mit einer Mehrzahl untereinander kommunikativ verbundener Automatisierungsgeräte (14-20),
dadurch gekennzeichnet, dass
der Kommunikations teilnehmer (26) eine Kennung (28) an das Automatisierungssystem (10) sendet,
dass im Bereich des Automatisierungssystems (10) die Kennung (28) überprüft und bei erfolgreicher Prüfung ein Zertifikat (30) erzeugt oder ausgewählt wird,
dass das Zertifikat (30) dem Kommunikationsteilnehmer (26) übermittelt wird und
dass das Zertifikat (30) von dem Kommunikationsteilnehmer (26) an sämtliche Automatisierungsgeräte (14-20) übermittelbar ist und zu einer Authentifizierung des Kommunikationsteilnehmers (26) für das jeweilige Automatisierungs gerät (14-20) führt.

2. Verfahren nach Anspruch 1, wobei das Automatisierungssystem (10) zumindest einen Authentifizierungs Server (22) umfasst und wobei die Kennung (28) an den Authentifizierungsserver (22) gesandt wird und das Zertifikat (30) daraufhin vom Authentifizierungs Server (22) erzeugt oder ausgewählt wird.

3. Verfahren nach Anspruch 2, wobei dem Authentifizierungsserver (22) zumindest ein privater Schlüssel und ein zu dem oder jedem privaten Schlüssel gehöriger öffentlicher Schlüssel zugeordnet ist, wobei der Authentifizierungs Server (22) das Zertifikat (30) mit dem oder einem privaten Schlüssel signiert und wobei zugehörige öffentliche Schlüssel im Automatisierungssystem (10) bekannt ist oder bekannt gemacht wird.

4. Verfahren nach einem der vorangehenden Ansprüche, wobei beim Übertragen des Zertifikats (30) durch den Kommunika-

tionsteilnehmer (26) an ein Automatisierungsgerät (14-20) ein sicherer Kommunikationskanal verwendet wird.

5. Verfahren nach einem der vorangehenden Ansprüche, wobei im Zusammenhang mit einer Übermittlung des Zertifikats (30) durch den Kommunikationsteilnehmer (26) an ein Automatisierungsgerät (14-20) das oder jedes Automatisierungsgerät (14-20) das Zertifikat (30) anhand von Zusatzinformationen über den Ursprung des Zertifikats (30) abweist oder akzeptiert.

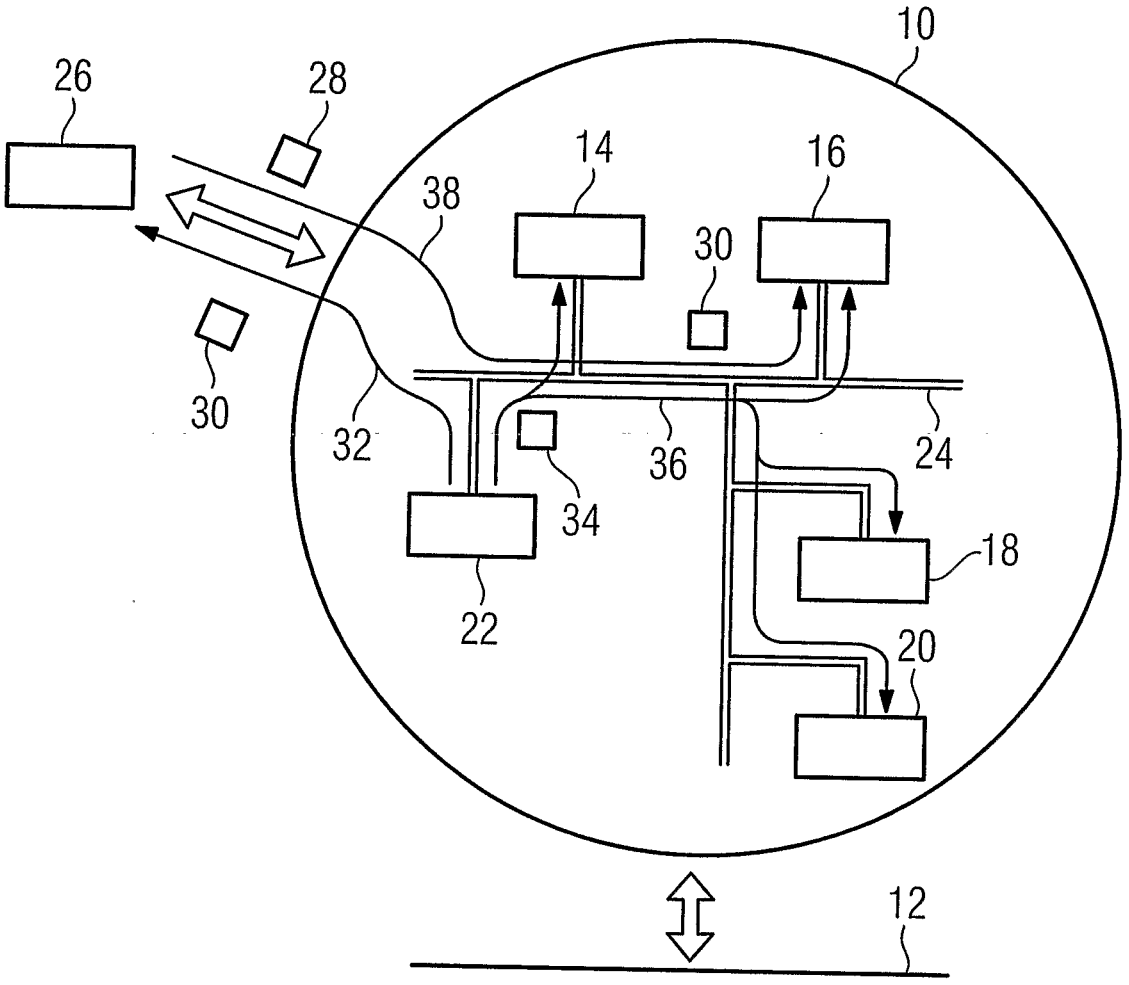
6. Verfahren nach einem der vorangehenden Ansprüche, wobei es sich bei dem Zertifikat (30) um ein X509-Zertifikat handelt.

7. Verfahren nach einem der vorangehenden Ansprüche, wobei das Zertifikat (30) nach einer vorgegebenen oder vorgebbaren Zeitspanne verfällt.

8. Verfahren nach einem der vorangehenden Ansprüche, wobei zu einem ablaufenden Zertifikat (30) automatisch ein neues Zertifikat angefordert wird.

9. Computerprogramm mit durch einen Computer ausführbaren Programmcodeanweisungen zur Implementierung des Verfahrens nach einem der Ansprüche 1 bis 8 wenn das Computerprogramm auf einem Computer ausgeführt wird.

10. Computerprogrammprodukt, insbesondere Speichermedium, mit einem durch einen Computer ausführbaren Computerprogramm gemäß Anspruch 9.


10
26
28
14
16
38
30
30
32
36
24
34
18
22
20
12

INTERNATIONAL SEARCH REPORT

International applIcation No
PCT/DE2006/001481

A. CLASSIRCATION OF SUBJECT MATTER
INV. G05B19/05 606F21/00 G05B19/418 H04L29/06

AccordIngto International Palent Classification (IPC) orto both national classIfIcallon and IPG

B. FIELDS SEARCHED

Minimum documentatIon searched (Classification System followed by Classification Symbols)
G05B G06F H04L

DocunπentallOn searched other than minimum documentation to the extent that such documents are Includβd in the flelds searchθd

Electronic data base consulted during th9 International search (name of data bass and, wherℯ practical, search terms used)
EPO-Internal , WPI Data

C. DOCUMENTS CONSIDERED TO BE HELEVANT

Category*	Citation of doument, with indication, where approp πate, of thG retevant passages	Relevant to Claim No
X	EP 1 624 350 A (SIEMENS AG [DE]) 8 February 2006 (2006-02-08) abstract paragraphs [0005], [0009], [0012], [0014], [0015], [0020], [0023] - [0025] Claim 6	1-10
A	DE 102 00 681 Al (SIEMENS AG [DE]) 31 JuIy 2003 (2003-07-31) abstract paragraphs [0014] - [0026]	1-10
A	EP 1 582 950 A (ROCKWELL AUTOMATION TECH INC [US]) 5 October 2005 (2005-10-05) abstract paragraphs [0006] - [0013], [0023]	1-10

-/--

X | Further documents arθ listθd in the conlinuation of Box C

X See patent family annex

* Special categones of cltβd documents

[1]A" document defming the general State of the art which ιs not coπsidered to be of particular releva πce

"E[1] earlier document but published on or after the international filing date

"L' document which maythrow doubts on pπonfy clairrφ) or which ιs αted to establish the publication date of another citation or other special reason (as specrfied)

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

[1]P" document published pπor to the international filing date but later than the pπonty date claimed

"T[1] later document published after the international filing date or pπoπty date and not in conflict with the applIcation but cited to understand the pπnciple or thβory underlying the invention

"X[1] document of particular relevance, the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document ιs taken alone

"Y[1] document of particular relevance, the claimed invention cannot be considered to involve an inventive step when the document ιs combined with one or more other such docu¬ments 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
2 May 2007	11/05/2007
Name and mailing address of the ISA/ Eurapean Patent Office P B 5818 Patentlaan 2 NL - 2280 HV Bijεwijk Tel (+31-70) 340-2040 Tx 31 651 epo nl, Fax (+31-70) 340-3016	Authoπzed officer Dörre, Thorsten

INTERNATIONAL SEARCH REPORT

International applicatlon No
PCT/DE2006/001481

C(Contlnuatlon). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with Indicalion, where appropriate, of the relevant passages	Relevant to Claim No.
A	EP 1 403 749 A (SIEMENS AG [DE]) 31 March 2004 (2004-03-31) abstract paragraphs [0008] - [0023]	1-10

INTERNATIONAL SEARCH REPORT

Information on patent famlly members

International applIcatIon No
PCT/DE2006/001481

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1624350 A	08-02-2006	US 2006026436 Al	02-02-2006
DE 10200681 Al	31-07-2003	NONE	
EP 1582950 A	05-10-2005	US 2005229004 Al	13-10-2005
EP 1403749 A	31-03-2004	DE 10245934 Al	08-04-2004

INTERNATIONALER RECHERCHENBERICHT

Internationales **Aktenzeichen**
PCT/DE2006/001481

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. 605B19/05 G06F21/00 G05B19/418 H04L29/06

Nach der Inlernallonalen Patenlklassiflkatlo π (IPC) oder nach der nationalen Klassifikation und der **IPC**

B. RECHERCHIERTE GEBIETE

Rθchθrchlertar Mindestprufstoff (Klassifikationssystsm und Klassiflkalionssymbole)
G05B G06F H04L

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

Wahrend der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl verwendete Suchbegriffe)
EPO-Internal , WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategone*	Bezeichnung der Veröffentlichung, soweit erfordertich unter Angabe der in Betracht kommenden Teile	Betr Anspruch Nr
X	EP 1 624 350 A (SIEMENS AG [DE]) 8 . Februar 2006 (2006-02-08) abstract Absätze [0005], [0009], [0012], [0014], [0015], [0020], [0023] - [0025] Anspruch 6	1-10
A	DE 102 00 681 Al (SIEMENS AG [DE]) 31. Juli 2003 (2003-07-31) abstract Absätze [0014] - [0026]	1-10
A	EP 1 582 950 A (ROCKWELL AUTOMATION TECH INC [US]) 5 . Oktober 2005 (2005-10-05) abstract Absätze [0006] - [0013], [0023]	1-10

-/--

[X] Weitere Veröffentlichungen sind der Forlsetzung 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
[1]L' Veröffentlichung, die geeignet ist, einen Pnoritatsanspruch zweifelhaft er¬ scheinen zu lassen, oder durch die das Veroffentlichungsdatum 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 vordem internationalen Anmeldedatum aber nach dem beanspruchten Pnorilatsdatum veröffentlicht worden ist
"T' Spatere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Pnontatsdatum 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
[1]X[1] Veröffentlichung von besonderer Bedeutung, die beanspruchte Erfindung kann altem aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
[1]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
2. Mai 2007	11/05/2007

Name und Postanschrift der Internationalen Recherchenbehorde	Bevollmächtigter Bediensteter
Europaisches Patentamt, P B 5618 Patentlaan 2 NL - 2280 HV Rijswijk Tel (+31-70) 340-2040 Tx 31 651 epo nl, Fax- (+31-70) 340-3016	Dörre, Thorsten

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/DE2006/001481

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der In Batracht kommenden Teile	Betr. Anspruch **Nr.**
A	EP 1 403 749 A (SIEMENS AG [DE]) 31. März 2004 (2004-03-31) abstract Absätze [0008] - [0023]	1-10

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/DE2006/001481

Im Recherohenberlcht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
tP 1624350	A	08-02-2006	US 2006026436	Al	02-02-2006
DE 10200681	Al	31-07-2003	KEINE		
EP 1582950	A	05-10-2005	US 2005229004	Al	13-10-2005
EP 1403749	A	31-03-2004	DE 10245934	Al	08-04-2004