



(12)

## Offenlegungsschrift

(21) Aktenzeichen: **10 2011 081 803.0**

(22) Anmeldetag: **30.08.2011**

(43) Offenlegungstag: **28.02.2013**

(51) Int Cl.: **G05B 19/418 (2011.01)**  
**G06F 21/00 (2011.01)**

(71) Anmelder:

**Siemens Aktiengesellschaft, 80333, München, DE**

(72) Erfinder:

**Fries, Steffen, 85598, Baldham, DE; Gessner, Jürgen, 85661, Forstinning, DE; Houyou, Amine Mohamed, 81543, München, DE; Huth, Hans-Peter, 80638, München, DE; Schattleitner, Angela, 83104, Tunttenhausen, DE**

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:

**US 2007 / 0 067 512 A1**

**Huang, R.; Liu, F.: Research on OPC UA based on electronic device description. In: 3rd IEEE Conference on Industrial Electronics and Applications, ICIEA 2008., 2008, S. 2162 -2166.**

**Leitner, Stefan-Helmut; Mahnke, Wolfgang:**

**OPC UA - Service-oriented Architecture for Industrial Applications. In: Workshop der Fachgruppen Objektorientierte Softwareentwicklung, 27. Oktober 2006, S. 1 - 6.**

**Mahnke, W.; Enste, U.: OPC Unified Architecture. In: at - Automatisierungstechnik, Band 59, Juli 2011, Heft 7, S. 397 - 404.**

**Renjie, H.; Feng, L.; Dongbo, P.: Research on OPC UA security. In: Industrial Electronics and Applications (ICIEA), 2010 the 5th IEEE Conference on, 2010, S. 1439 -1444.**

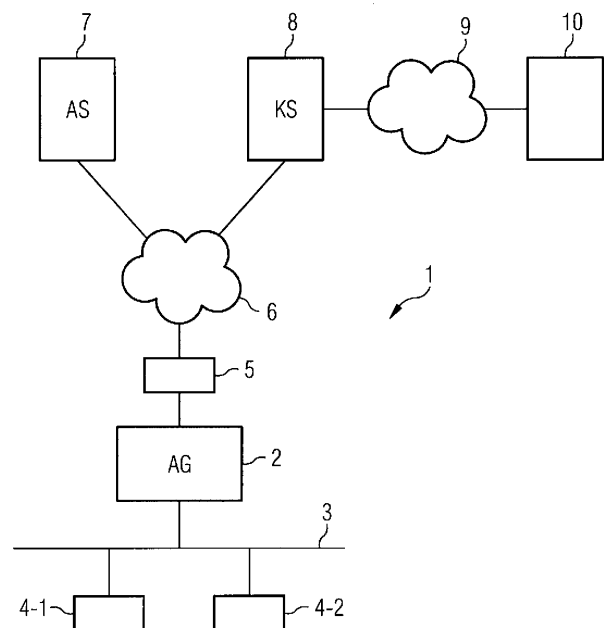
**Zielinski, M.: Digital fieldbus installations use EDDL for simplicity with advanced, full functionality. In: Computing & Control Engineering Journal, Band 6, 2005, S. 24 - 31.**

Prüfungsantrag gemäß § 44 PatG ist gestellt.

**Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen**

(54) Bezeichnung: **Verfahren und System zum Bereitstellen von gerätespezifischen Eigenschaftsdaten für ein Automatisierungsgerät einer Automatisierungsanlage**

(57) Zusammenfassung: Verfahren zum Bereitstellen von gerätespezifischen Eigenschaftsdaten für ein Automatisierungsgerät (2) einer Automatisierungsanlage (1), welches sich mittels mindestens eines Authentisierungs-Credentials gegenüber einem Authentisierungsserver (7) der Automatisierungsanlage (1) authentisiert, wobei die gerätespezifischen Eigenschaftsdaten des Automatisierungsgerätes (2) an das Authentisierungs-Credential des Automatisierungsgerätes (2) gebunden werden.



**Beschreibung**

**[0001]** Die Erfindung betrifft ein Verfahren und ein System zum Bereitstellen von gerätespezifischen Eigenschaftsdaten für ein Automatisierungsgerät einer Automatisierungsanlage, insbesondere für ein Automatisierungssteuergerät, ein SPS-Steuergerät oder ein Feldgerät.

**[0002]** Automatisierungsgeräte müssen im Allgemeinen konfiguriert werden, bevor sie im Zusammenspiel mit anderen Geräten und anderen Automatisierungsgeräten einer Automatisierungsanlage genutzt werden können. In herkömmlichen Automatisierungssystemen bzw. Automatisierungsanlagen erfolgt daher eine Parametrisierung der Automatisierungsgeräte der Automatisierungsgeräte vor dem eigentlichen Einsatz. Diese Parametrisierung kann allgemein Konfigurationsdaten umfassen, die beispielsweise eine Adresse des Automatisierungsgerätes innerhalb des Netzwerkes oder einsatzspezifische Konfigurationsdaten, wie beispielsweise Schaltweiten des Automatisierungsgerätes, aufweisen. Außerdem ist es möglich, während des Betriebes der Automatisierungsanlage eine Rekonfiguration eines Automatisierungsgerätes durchzuführen. Insbesondere ist es für eine automatisierte Konfiguration von Automatisierungsanlagen nötig, die gerätespezifischen Eigenschaften und Anforderungen der Automatisierungsgeräte der Automatisierungsanlage zu kennen und für die Konfiguration zu berücksichtigen. Da Sicherheit gegenüber Datenmanipulationen zunehmend von Bedeutung wird, werden zunehmend Automatisierungsgeräte mit Sicherheitsmerkmalen bzw. Authentisierungs-Credentials ausgeliefert.

**[0003]** Bei herkömmlichen Automatisierungsanlagen erfolgt die Konfiguration von Automatisierungsgeräten der Automatisierungsanlagen weitestgehend ungeschützt, sodass Dritte, welche Zugang zu der Automatisierungsanlage erlangen, gerätespezifische Eigenschaftsdaten des Automatisierungsgerätes der Automatisierungsanlage verändern können. Dies kann während des Betriebes der Automatisierungsanlage zu teilweise katastrophalen Fehlfunktionen führen, da eventuell die Konfiguration der Automatisierungsanlage auf der Grundlage von falschen Eigenschaftsdaten der Automatisierungsgeräte der Automatisierungsanlage durchgeführt wird.

**[0004]** Es ist daher eine Aufgabe der vorliegenden Erfindung, ein Verfahren und ein System zum sicheren Bereitstellen von gerätespezifischen Eigenschaftsdaten für ein Automatisierungsgerät einer Automatisierungsanlage zu schaffen, in der gerätespezifische Eigenschaftsdaten vor Manipulationen Dritter geschützt sind.

**[0005]** Die Aufgabe wird erfindungsgemäß durch ein Verfahren mit den in Patentanspruch 1 angegebenen Merkmalen gelöst.

**[0006]** Die Erfindung schafft demnach ein Verfahren zum Bereitstellen von gerätespezifischen Eigenschaftsdaten für ein Automatisierungsgerät einer Automatisierungsanlage, welches sich mittels mindestens eines Authentisierungs-Credentials gegenüber einem Authentisierungsserver der Automatisierungsanlage authentisiert, wobei die gerätespezifischen Eigenschaftsdaten des Automatisierungsgerätes an das Authentisierungs-Credential des Automatisierungsgerätes gebunden werden.

**[0007]** Bei einer möglichen Ausführungsform des erfindungsgemäßen Verfahrens wird das Authentisierungs-Credential durch ein Gerätezertifikat des Herstellers des Automatisierungsgerätes gebildet.

**[0008]** Bei einer möglichen Ausführungsform des erfindungsgemäßen Verfahrens weisen die gerätespezifischen Eigenschaftsdaten des Automatisierungsgerätes Eigenschaftsdaten zur Beschreibung technischer Eigenschaften des Automatisierungsgerätes auf.

**[0009]** Bei einer weiteren möglichen Ausführungsform des erfindungsgemäßen Verfahrens weisen die gerätespezifischen Eigenschaftsdaten des Automatisierungsgerätes Eigenschaftsdaten zur Beschreibung von Leistungsmerkmalen des Automatisierungsgerätes auf.

**[0010]** Bei einer weiteren möglichen Ausführungsform des erfindungsgemäßen Verfahrens weisen die gerätespezifischen Eigenschaftsdaten des Automatisierungsgerätes Eigenschaftsdaten zur Beschreibung eines Ressourcen-Verbrauchs des Automatisierungsgerätes auf.

**[0011]** Bei einer weiteren möglichen Ausführungsform des erfindungsgemäßen Verfahrens weisen die gerätespezifischen Eigenschaftsdaten des Automatisierungsgerätes Eigenschaftsdaten zur Beschreibung von geforderten Parametern von Geräten, die durch das Automatisierungsgerät gesteuert werden, auf.

**[0012]** Bei einer weiteren möglichen Ausführungsform des erfindungsgemäßen Verfahrens weisen die gerätespezifischen Eigenschaftsdaten des Automatisierungsgerätes Eigenschaftsdaten zur Beschreibung zulässiger Betriebsbereiche des Automatisierungsgerätes auf.

**[0013]** Bei einer möglichen Ausführungsform des erfindungsgemäßen Verfahrens liegen die gerätespezi-

fischen Eigenschaftsdaten als EDDL-(Electronic Device Description Language)Daten vor.

**[0014]** Bei einer möglichen Ausführungsform des erfindungsgemäßen Verfahrens werden die gerätespezifischen Eigenschaftsdaten des Automatisierungsgerätes als Attributdaten in das Gerätezertifikat des Herstellers des Automatisierungsgerätes eingeschrieben, um die gerätespezifischen Eigenschaftsdaten an das Gerätezertifikat des Automatisierungsgerätes zu binden.

**[0015]** Bei einer möglichen Ausführungsform des erfindungsgemäßen Verfahrens wird eine Adresse zur Adressierung der gerätespezifischen Eigenschaftsdaten des Automatisierungsgerätes in das Gerätezertifikat des Herstellers des Automatisierungsgerätes eingeschrieben, um die gerätespezifischen Eigenschaftsdaten an das Gerätezertifikat des Automatisierungsgerätes zu binden.

**[0016]** Bei einer möglichen Ausführungsform des erfindungsgemäßen Verfahrens wird die Adresse zur Adressierung der gerätespezifischen Eigenschaftsdaten anhand einer gerätespezifischen Seriennummer, die in dem Gerätezertifikat des Automatisierungsgerätes enthalten ist, ermittelt.

**[0017]** Bei einer weiteren möglichen Ausführungsform des erfindungsgemäßen Verfahrens werden die gerätespezifischen Eigenschaftsdaten des Automatisierungsgerätes als codierte Attributdaten in das Gerätezertifikat des Automatisierungsgerätes eingeschrieben, um die gerätespezifischen Eigenschaftsdaten an das Gerätezertifikat des Automatisierungsgerätes zu binden.

**[0018]** Bei einer möglichen Ausführungsform des erfindungsgemäßen Verfahrens erfolgt das Binden der gerätespezifischen Eigenschaftsdaten an das Authentisierungs-Credential des Automatisierungsgerätes durch einen Konfigurationsserver.

**[0019]** Bei einer weiteren möglichen Ausführungsform des erfindungsgemäßen Verfahrens erfolgt das Binden der gerätespezifischen Eigenschaftsdaten an das Authentisierungs-Credential des Automatisierungsgerätes durch einen Policy-Enforcement-Server der Automatisierungsanlage.

**[0020]** Bei einer möglichen Ausführungsform des erfindungsgemäßen Verfahrens bindet der Konfigurationsserver oder der Policy-Enforcement-Server die gerätespezifischen Eigenschaftsdaten des Automatisierungsgerätes, die von einem beim Hersteller bereitgestellten Capability Server abgeholt werden, an das Authentisierungs-Credential, nachdem der Authentisierungsserver dem Konfigurationsserver oder dem Policy-Enforcement-Server eine erfolgreiche Authentisierung des Automatisierungsge-

rätes gegenüber dem Authentisierungsserver gemeldet hat.

**[0021]** Bei einer möglichen Ausführungsform des erfindungsgemäßen Verfahrens werden die gerätespezifischen Eigenschaftsdaten des Automatisierungsgerätes digital signiert.

**[0022]** Bei einer möglichen Ausführungsform des erfindungsgemäßen Verfahrens weist das mindestens eine Authentisierungs-Credential ein Gerätezertifikat des Herstellers des Automatisierungsgerätes und/oder einen kryptographischen Schlüssel und/oder ein kryptographisches Schlüsselpaar auf.

**[0023]** Die Erfindung schafft ferner ein System zur Bereitstellung von gerätespezifischen Eigenschaftsdaten für ein Automatisierungsgerät einer Automatisierungsanlage mit den in Patentanspruch 12 angegebenen Merkmalen.

**[0024]** Die Erfindung schafft demnach ein System zum Bereitstellen von gerätespezifischen Eigenschaftsdaten für ein Automatisierungsgerät einer Automatisierungsanlage, die sich mittels mindestens eines Authentisierungs-Credentials gegenüber einem Authentisierungsserver der Automatisierungsanlage authentisiert, wobei die gerätespezifischen Eigenschaftsdaten des Automatisierungsgerätes an das Authentisierungs-Credential des Automatisierungsgerätes gebunden werden.

**[0025]** Bei einer möglichen Ausführungsform des erfindungsgemäßen Systems weist das Automatisierungsgerät ein Automatisierungssteuergerät, ein SPS-Steuergerät oder ein Feldgerät auf.

**[0026]** Im Weiteren werden mögliche Ausführungsformen des erfindungsgemäßen Verfahrens und des erfindungsgemäßen Systems zum Bereitstellen von gerätespezifischen Eigenschaftsdaten für ein Automatisierungsgerät einer Automatisierungsanlage unter Bezugnahme auf die beiliegenden Figuren näher beschrieben.

**[0027]** Es zeigen:

**[0028]** [Fig. 1](#) ein Blockschaltbild zur Darstellung eines Ausführungsbeispiels des erfindungsgemäßen Systems zum Bereitstellen von gerätespezifischen Eigenschaftsdaten für ein Automatisierungsgerät einer Automatisierungsanlage;

**[0029]** [Fig. 2](#) ein Ausführungsbeispiel für ein bei dem erfindungsgemäßen Verfahren und System eingesetzten Authentisierungs-Credential;

**[0030]** [Fig. 3](#) ein weiteres Ausführungsbeispiel für ein bei dem erfindungsgemäßen Verfahren und System eingesetzten Authentisierungs-Credential.

**[0031]** Im Folgenden wird ein Ausführungsbeispiel für ein erfindungsgemäßes System und Verfahren zum Bereitstellen von gerätespezifischen Eigenschaftsdaten für ein Automatisierungsgerät einer Automatisierungsanlage unter Bezugnahme auf [Fig. 1](#) näher beschrieben. Wie man aus [Fig. 1](#) erkennen kann, weist eine Automatisierungsanlage **1** mindestens ein Automatisierungsgerät **2** auf. Bei dem Automatisierungsgerät **2** kann es sich beispielsweise um ein Automatisierungssteuergerät handeln, das über einen Bus, insbesondere einen Feldbus **3**, weitere Geräte **4-1**, **4-2** ansteuern kann, wie in [Fig. 1](#) dargestellt. Bei dem Automatisierungsgerät **2** kann es sich beispielsweise um ein SPS-Steuergerät handeln. Weiterhin kann es sich bei dem Automatisierungsgerät auch um ein Feldgerät handeln. Das Automatisierungsgerät ist über einen Netzzugangsswitch **5** an ein Datennetzwerk **6** angeschlossen, wobei an dem Datennetzwerk **6** bei dem in [Fig. 1](#) dargestellten Ausführungsbeispiel ferner ein Authentisierungsserver **7**, ein Konfigurationsserver bzw. Engineering-Server **8** angeschlossen sind. Weiterhin kann die Automatisierungsanlage **1** bei einer möglichen Ausführungsform einen in [Fig. 1](#) nicht dargestellten Policy-Enforcement-Server aufweisen. Der Authentisierungsserver **7** ist bei einer möglichen Ausführungsform ein AAA-Server zur Durchführung einer Geräteauthentisierung und einer Zugangskontrolle. Bei einem Ausführungsbeispiel kann es sich bei dem Authentisierungsserver **7** um einen RADIUS-Server handeln. Der Konfigurationsserver **8** kann in dem in [Fig. 1](#) dargestellten Ausführungsbeispiel über ein weiteres Netzwerk **9** an einen Server **10** des Geräteherstellers angeschlossen sein. Bei dem Gerätehersteller kann es sich beispielsweise um den Hersteller des Automatisierungsgerätes **2** handeln. Bei dem erfindungsgemäßen System und Verfahren zum Bereitstellen von gerätespezifischen Eigenschaftsdaten für ein Automatisierungsgerät **2** der Automatisierungsanlage **1** sind die gerätespezifischen Eigenschaftsdaten des Automatisierungsgerätes **2** an ein Authentisierungs-Credential des Automatisierungsgerätes **2** gebunden. Dieser Authentisierungs-Credential verwendet das Automatisierungsgerät **2** zu seiner Authentisierung gegenüber dem Authentisierungsserver **7**. Bei dem Authentisierungs-Credential kann es sich bei einer möglichen Ausführungsform um ein Gerätezertifikat des Herstellers des Automatisierungsgerätes **2** handeln. Bei einer weiteren möglichen Ausführungsform weist das Authentisierungs-Credential einen kryptographischen Schlüssel und/oder ein kryptographisches Schlüsselpaar auf. Das Binden der gerätespezifischen Eigenschaftsdaten an das Authentisierungs-Credential des Automatisierungsgerätes **2** erfolgt bei einer möglichen Ausführungsform durch den in [Fig. 1](#) dargestellten Konfigurationsserver **8**. Alternativ kann das Binden der gerätespezifischen Eigenschaftsdaten an das Authentisierungs-Credential auch durch einen Policy-Enforcement-Server der Automatisierungsanlage **1** erfolgen. Alternativ ist es

auch möglich, dass das Binden der gerätespezifischen Eigenschaftsdaten an das Authentisierungs-Credential direkt durch den Authentisierungsserver **7** der Automatisierungsanlage erfolgt.

**[0032]** Das Binden der gerätespezifischen Eigenschaftsdaten des Automatisierungsgerätes **2** an das Authentisierungs-Credential, beispielsweise an das Gerätezertifikat des Herstellers des Automatisierungsgerätes **2**, erfolgt bei einer möglichen Ausführungsform durch den Konfigurationsserver **8** bzw. einen Policy-Enforcement-Server nachdem der Authentisierungsserver **7** den Konfigurationsserver **8** bzw. den Policy-Enforcement-Server eine erfolgreiche Authentisierung des Automatisierungsgerätes **2** gegenüber dem Authentisierungsserver **7** gemeldet hat. Bei einer möglichen Ausführungsform werden die gerätespezifischen Eigenschaftsdaten von einem Capability-Server des Herstellers des jeweiligen Automatisierungsgerätes **2** abgeholt bzw. geladen. Bei einer möglichen Ausführungsform werden die gerätespezifischen Eigenschaftsdaten des Automatisierungsgerätes **2** digital signiert. Die gerätespezifischen Eigenschaftsdaten des Automatisierungsgerätes **2** können verschiedene Daten und Datentypen umfassen. Die gerätespezifischen Eigenschaftsdaten umfassen demnach bei einer möglichen Ausführungsform Eigenschaftsdaten zur Beschreibung technischer Eigenschaften des Automatisierungsgerätes **2**. Weiterhin können die gerätespezifischen Eigenschaftsdaten des Automatisierungsgerätes **2** Leistungsmerkmale des Automatisierungsgerätes **2** bzw. Gerätetyps des Automatisierungsgerätes **2** angeben. Die gerätespezifischen Eigenschaftsdaten können ferner Eigenschaftsdaten zur Beschreibung eines Ressourcen-Verbrauchs des Automatisierungsgerätes **2**, beispielsweise eines Energieverbrauchs, aufweisen. Die gerätespezifischen Eigenschaftsdaten des Automatisierungsgerätes können ferner Eigenschaftsdaten zur Beschreibung von geforderten Parametern von Geräten angeben, die durch das Automatisierungsgerät **2** angesteuert werden. Beispielsweise können die Eigenschaftsdaten Parameter von den in [Fig. 1](#) dargestellten Geräten **4-1**, **4-2** enthalten, die durch das Automatisierungsgerät **2** über den Feldbus **3** angesteuert werden. Handelt es sich bei einem der gesteuerten Geräte **4-1** z.B. um einen Schrittmotor, so können die Eigenschaftsdaten einen Drehzahlbereich des angesteuerten Schrittmotors angeben, welcher durch das Automatisierungsgerät **2** angesteuert werden kann. Weiterhin können die gerätespezifischen Eigenschaftsdaten des Automatisierungsgerätes **2** Eigenschaftsdaten zur Beschreibung zulässiger Betriebsbereiche des Automatisierungsgerätes **2** aufweisen, beispielsweise einen zulässigen Betriebstemperaturbereich. Die gerätespezifischen Eigenschaftsdaten können bei einer möglichen Ausführungsform als EDDL-(Electronic Device Description Language) Daten vorliegen.

**[0033]** Bei einer möglichen Ausführungsform werden die gerätespezifischen Eigenschaftsdaten des Automatisierungsgerätes **2** als Attributdaten in ein Gerätezertifikat Z des Herstellers des Automatisierungsgerätes **2** eingeschrieben, um die gerätespezifischen Eigenschaftsdaten an das Gerätezertifikat Z des Automatisierungsgerätes **2** zu binden. Bei einer alternativen Ausführungsform des erfindungsgemäßen Verfahrens und Systems wird eine Adresse zur Adressierung der gerätespezifischen Eigenschaftsdaten des Automatisierungsgerätes **2** in das Gerätezertifikat Z des Herstellers des Automatisierungsgerätes **2** eingeschrieben, um die gerätespezifischen Eigenschaftsdaten an das Gerätezertifikat Z des Automatisierungsgerätes **2** zu binden. Bei einer möglichen Ausführungsform wird diese Adresse zur Adressierung der gerätespezifischen Eigenschaftsdaten anhand einer gerätespezifischen Seriennummer, die in dem Gerätezertifikat des Automatisierungsgerätes **2** enthalten ist, automatisch ermittelt. Bei einer weiteren möglichen Ausführungsvariante werden die gerätespezifischen Eigenschaftsdaten des Automatisierungsgerätes **2** als codierte Attributdaten in das Gerätezertifikat Z des Automatisierungsgerätes **2** eingeschrieben, um die gerätespezifischen Eigenschaftsdaten an das Gerätezertifikat des Automatisierungsgerätes **2** zu binden. Bei einer möglichen Ausführungsform fragt das Automatisierungsgerät **2** in regelmäßigen Zeitabständen oder bei Auftreten eines bestimmten Ereignisses an, ob aktuelle gerätespezifische Eigenschaftsdaten des Herstellers für das Automatisierungsgerät **2** vorhanden sind. Bei dem erfindungsgemäßen Verfahren und System wird ein Authentisierungs-Credential, insbesondere ein Herstellerzertifikat des Automatisierungsgerätes **2** zum Transport von gerätespezifischen Eigenschaftsdaten benutzt, welche insbesondere die gerätespezifischen Eigenschaftsdaten und Leistungsdaten und/oder Konfigurationsdaten umfassen. Diese gerätespezifischen Eigenschaftsdaten können die generellen Fähigkeiten der Geräteklasse oder auch eines spezifischen Gerätetyps oder des individuellen Automatisierungsgerätes **2** angeben.

**[0034]** Die gerätespezifischen Eigenschaftsdaten des Automatisierungsgerätes **2** können geräte- oder serienspezifisch direkt in das Gerätezertifikat Z des Herstellers encodiert werden. Dabei kann die Größe des Zertifikates Z anwachsen, sodass der dafür notwendige Speicher zur Verfügung gestellt werden muss. Bei einer weiteren möglichen Ausführungsvariante enthält das Gerätezertifikat Z eine geräte- oder serienspezifische Seriennummer, die zusammen mit dem Aussteller und der Seriennummer des Gerätezertifikates Z eine ausreichende Grundlage bietet, mit der ein Server die gerätespezifischen Eigenschaftsdaten von einem Server des Herstellers des Automatisierungsgerätes **2** abfragen kann. Bei einer weiteren möglichen Ausführungsvariante enthält das Gerätezertifikat Z einen Link bzw. eine Adresse auf ei-

ne Webseite des Herstellers des Automatisierungsgerätes **2**, in dem die möglichen gerätespezifischen Eigenschaftsdaten von einer Device Description Database abgelegt sind. Die von dem Hersteller des Automatisierungsgerätes **2** zur Verfügung gestellten Eigenschaftsdaten können digital signiert sein, um die Integrität dieser Daten zu sichern und sie somit für eine Automatisierung in der Planung der Automatisierungsanlage **1** nutzen zu können. Bei einer Ausführungsform kann man eine Logotype-Extension nutzen, um Geräte oder serienspezifische Eigenschaftstypen bzw. Informationen als 1D- oder 2D-Barcode einzucodieren. Die Abfrage der Daten, insbesondere der gerätespezifischen Eigenschaftsdaten von dem Server des Herstellers des Automatisierungsgerätes **2** kann dabei online oder offline, beispielsweise über eine mitgelieferte Datenbank, realisiert werden.

**[0035]** Das Ausführen von sicherheitsrelevanten Aktionen während einer Anbindung eines Automatisierungsgerätes **2** an eine Automatisierungsanlage bzw. ein Netzwerk ist einer der ersten Schritte, die beim Booten von Automatisierungsgeräten **2** durchgeführt wird. Dies kann vorteilhafterweise mit einer Erstkonfiguration des Automatisierungsgerätes **2** verbunden werden. Bei dem erfindungsgemäßen System ist es möglich, das Automatisierungsgerät **2** autark zu konfigurieren oder über eine zentrale Infrastruktur, welche abhängig von dem hinzugefügten Automatisierungsgerät **2** eine bestehende Systemkonfiguration adaptieren kann. Bei einer Einbettung in ein Gerätezertifikat Z können die Eigenschaftsdaten des Automatisierungsgerätes **2** zudem kryptographisch gesichert werden. Die Anbindung von gerätespezifischen Eigenschaftsdaten an einen Gerätetyp oder auch an ein spezifisches Automatisierungsgerät **2** unterstützt darüber hinaus auch einen Prozess der automatisierten Planung oder Commissioning von Automatisierungsanlagen **1** basierend auf den gerätespezifischen Eigenschaftsdaten der Automatisierungsgeräte.

**[0036]** [Fig. 2](#) zeigt ein Ausführungsbeispiel des Gerätezertifikates Z, bei dem gerätespezifische Eigenschaftsdaten als zusätzliches Attribut in dem Gerätezertifikat Z enthalten sind.

**[0037]** Das Zertifikat Z weist eine Zertifikat-ID, beispielsweise eine Seriennummer SN auf. Ferner enthält das Zertifikat Z den Namen N1 desjenigen, für den es ausgestellt wurde, sowie den Namen N2 des Ausstellers. Weiterhin gibt das Zertifikat Z an, ab wann es gültig ist, d. h. einen Zeitpunkt T1, und bis wann es gültig ist, d. h. einen Zeitpunkt T2. Ferner umfasst das Zertifikat Z einen öffentlichen Schlüssel PK und Attribute Att, beispielsweise Attribute Att-A, Att-B. Weiterhin weist das Zertifikat Z bei der in [Fig. 2](#) dargestellten Ausführungsform als Attribut gerätespezifische Eigenschaftsdaten ED auf. Das Zer-



tifikat Z kann ferner eine Signatur SIG des Herstellers aufweisen.

**[0038]** Fig. 3 zeigt eine alternative Ausführungsvariante, in der in dem Zertifikat Z des Geräteherstellers ein Link L zu dem Server des Geräteherstellers des Automatisierungsgerätes 2 eingeschrieben ist.

**[0039]** Die automatische Konfiguration eines Automatisierungsgerätes 2 in Abhängigkeit der Eigenschaftsdaten des Automatisierungsgerätes 2 kann beim Anmelden des Automatisierungsgerätes 2 an einem Netzwerk erfolgen. Dazu wird das Herstellerzertifikat 2 zur Netzanmeldung benutzt. Nach erfolgreicher Netzanmeldung wird das Gerätezertifikat bzw. der Link zu den Eigenschaftsdaten an einen Konfigurationsserver 8 übermittelt, der daraufhin das Automatisierungsgerät 2 entsprechend konfigurieren kann.

**[0040]** Im Einzelnen können bei einer möglichen Ausführungsform hierbei die folgenden Schritte ausgeführt werden.

**[0041]** Zunächst authentisiert sich das Automatisierungsgerät 2 mittels seines Authentisierungs-Credentials gegenüber dem Authentisierungsserver 7 der Automatisierungsanlage 1, um Zugang zu dem Netzwerk zu erhalten. Bei dem Authentisierungsserver 7 handelt es sich beispielsweise um einen RADIUS-Server. Das herstellerspezifische Authentisierungs-Credential wird verwendet, um das Automatisierungsgerät 2 gegenüber dem Authentisierungsserver 7 zu authentisieren, wobei dieses Credential dem Server 7 bekannt ist. Handelt es sich beispielsweise bei dem Authentisierungs-Credential um ein Gerätezertifikat, können bei einer möglichen Ausführungsvariante zertifikatsbasierte EAP-Methoden, wie beispielsweise EAP-TSF, verwendet werden. Das Authentisierungs-Credential kann bei einer möglichen Ausführungsform ein Link auf eine Gerätebeschreibungsdatenbank des Herstellers des Automatisierungsgerätes 2 enthalten.

**[0042]** Nach erfolgreicher Authentisierung gegenüber dem Authentisierungsserver 7 sendet der Authentisierungsserver 7 dem Network Access Switch 5 eine Mitteilung, dass es das Automatisierungsgerät 2 an das Netzwerk 6 anbinden darf. Anschließend kann eine Adresskonfiguration des Automatisierungsgerätes 2 beispielsweise mit einer IP-Adresse erfolgen.

**[0043]** Der Authentisierungsserver 7 meldet die erfolgreiche Authentisierung des Automatisierungsgerätes 2 beispielsweise an den in Fig. 1 dargestellten Konfigurationsserver 8. Dabei kann optional das Gerätezertifikat des Automatisierungsgerätes 2 mitgeschickt werden.

**[0044]** Mittels eines Links auf die Gerätebeschreibungsdatenbank bzw. den Server des Herstellers kann der Konfigurationsserver 8 dann die notwendigen Daten über das Netzwerk 9 bei einem Server 10 des Herstellers des Automatisierungsgerätes 2 abfragen, um die Konfiguration des Automatisierungsgerätes 2 bzw. gemäß einem Anlagenplan der Automatisierungsanlage 1 durchzuführen. Dabei sendet der Server 10 des Herstellers die gerätespezifischen Eigenschaftsdaten zu dem Konfigurationsserver 8. Der Konfigurationsserver 8 ermittelt anlagenspezifische Konfigurationsparameter für das Automatisierungsgerät 2 und sendet diese anschließend an das Automatisierungsgerät 2 über das Netzwerk 6 und das Netzzugangsswitch 5.

**[0045]** Durch das erfindungsgemäße Verfahren und System wird der Konfigurationsaufwand zur Konfiguration eines Automatisierungsgerätes 2 innerhalb einer Automatisierungsanlage 1 im Vergleich zu herkömmlichen Anlagen erheblich vermindert. Die Konfiguration eines Automatisierungsgerätes 2 mithilfe der übermittelten Eigenschaftsdaten kann dabei innerhalb kurzer Zeit abgeschlossen werden. Nach erfolgreicher Authentisierung des Automatisierungsgerätes 2 kann unmittelbar anschließend eine automatische Konfiguration des Automatisierungsgerätes 2 erfolgen, ohne dass es irgendeiner manuellen Konfiguration des Automatisierungsgerätes 2 bedarf. Darüber hinaus erfolgt die Konfiguration in geschützter Form, sodass Manipulationen an Eigenschaftsdaten des Automatisierungsgerätes 2 durch Dritte nicht möglich sind.

### Patentansprüche

1. Verfahren zum Bereitstellen von gerätespezifischen Eigenschaftsdaten für ein Automatisierungsgerät (2) einer Automatisierungsanlage (1), welches sich mittels mindestens eines Authentisierungs-Credentials gegenüber einem Authentisierungsserver (7) der Automatisierungsanlage (1) authentisiert, wobei die gerätespezifischen Eigenschaftsdaten des Automatisierungsgerätes (2) an das Authentisierungs-Credential des Automatisierungsgerätes (2) gebunden werden.

2. Verfahren nach Anspruch 1, wobei das Authentisierungs-Credential durch ein Gerätezertifikat (Z) des Herstellers des Automatisierungsgerätes (2) gebildet wird.

3. Verfahren nach Anspruch 1 oder 2, wobei die gerätespezifischen Eigenschaftsdaten des Automatisierungsgerätes (2)

- Eigenschaftsdaten zur Beschreibung technischer Eigenschaften des Automatisierungsgerätes (2),
- Eigenschaftsdaten zur Beschreibung von Leistungsmerkmalen des Automatisierungsgerätes (2),

– Eigenschaftsdaten zur Beschreibung eines Ressourcenverbrauches des Automatisierungsgerätes (2), – Eigenschaftsdaten zur Beschreibung von geforderten Parametern von Geräten (4), die durch das Automatisierungsgerät (2) gesteuert werden, und  
– Eigenschaftsdaten zur Beschreibung zulässiger Betriebsbereiche des Automatisierungsgerätes (2) aufweisen.

4. Verfahren nach einem der vorangehenden Ansprüche 1 bis 3, wobei die gerätespezifischen Eigenschaftsdaten als EDDL- (Electronic Device Description Language) Daten vorliegen.

5. Verfahren nach einem der vorangehenden Ansprüche 1 bis 4, wobei die gerätespezifischen Eigenschaftsdaten des Automatisierungsgerätes (2) als Attributdaten in das Gerätezertifikat (Z) des Herstellers des Automatisierungsgerätes (2) eingeschrieben werden, um die gerätespezifischen Eigenschaftsdaten an das Gerätezertifikat (Z) des Automatisierungsgerätes (2) zu binden.

6. Verfahren nach einem der vorangehenden Ansprüche 2 bis 4, wobei eine Adresse zur Adressierung der gerätespezifischen Eigenschaftsdaten des Automatisierungsgerätes (2) in das Gerätezertifikat (Z) des Herstellers des Automatisierungsgerätes (2) eingeschrieben wird, um die gerätespezifischen Eigenschaftsdaten an das Gerätezertifikat (Z) des Automatisierungsgerätes (2) zu binden.

7. Verfahren nach Anspruch 6, wobei die Adresse zur Adressierung der gerätespezifischen Eigenschaftsdaten anhand einer gerätespezifischen Seriennummer, die in dem Gerätezertifikat (Z) des Automatisierungsgerätes (2) enthalten ist, ermittelt wird.

8. Verfahren nach einem der vorangehenden Ansprüche 2 bis 4, wobei die gerätespezifischen Eigenschaftsdaten des Automatisierungsgerätes (2) als codierte Attributdaten in das Gerätezertifikat (Z) des Automatisierungsgerätes (2) eingeschrieben werden, um die gerätespezifischen Eigenschaftsdaten an das Gerätezertifikat (Z) des Automatisierungsgerätes (2) zu binden.

9. Verfahren nach einem der vorangehenden Ansprüche 1 bis 8, wobei der Konfigurationsserver (8) oder der Policy- Enforcement-Server die gerätespezifischen Eigenschaftsdaten des Automatisierungsgerätes (2) von einem beim Hersteller bereitgestellten Capability Server, nachdem der Authentisierungsserver (7) dem Konfigurationsserver (8) oder dem Policy- Enforcement-Server eine erfolgreiche Authentisierung des Automatisierungsgerätes (2) gegenüber dem Authentisierungsserver (7) gemeldet hat und an das Authentisierungs-Credential des Automatisierungsgerätes (2) bindet.

10. Verfahren nach einem der vorangehenden Ansprüche 1 bis 9, wobei die gerätespezifischen Eigenschaftsdaten des Automatisierungsgerätes (2) digital signiert werden.

11. Verfahren nach einem der vorangehenden Ansprüche 1 bis 10, wobei das mindestens eine Authentisierungs-Credential ein Gerätezertifikat (Z) des Herstellers des Automatisierungsgerätes und/oder einen kryptographischen Schlüssel und/oder ein kryptographisches Schlüsselpaar aufweist.

12. System zum Bereitstellen von gerätespezifischen Eigenschaftsdaten für ein Automatisierungsgerät (2) einer Automatisierungsanlage (1), welches sich mittels mindestens eines Authentisierungs-Credentials gegenüber einem Authentisierungsserver (7) der Automatisierungsanlage (1) authentisiert, wobei die gerätespezifischen Eigenschaftsdaten des Automatisierungsgerätes (2) an das Authentisierungs-Credential des Automatisierungsgerätes (2) gebunden werden.

13. System nach Anspruch 12, wobei das Automatisierungsgerät (2) ein Automatisierungssteuergerät, ein SPS-Steuergerät oder ein Feldgerät aufweist.

Es folgen 2 Blatt Zeichnungen

Anhängende Zeichnungen

FIG 1

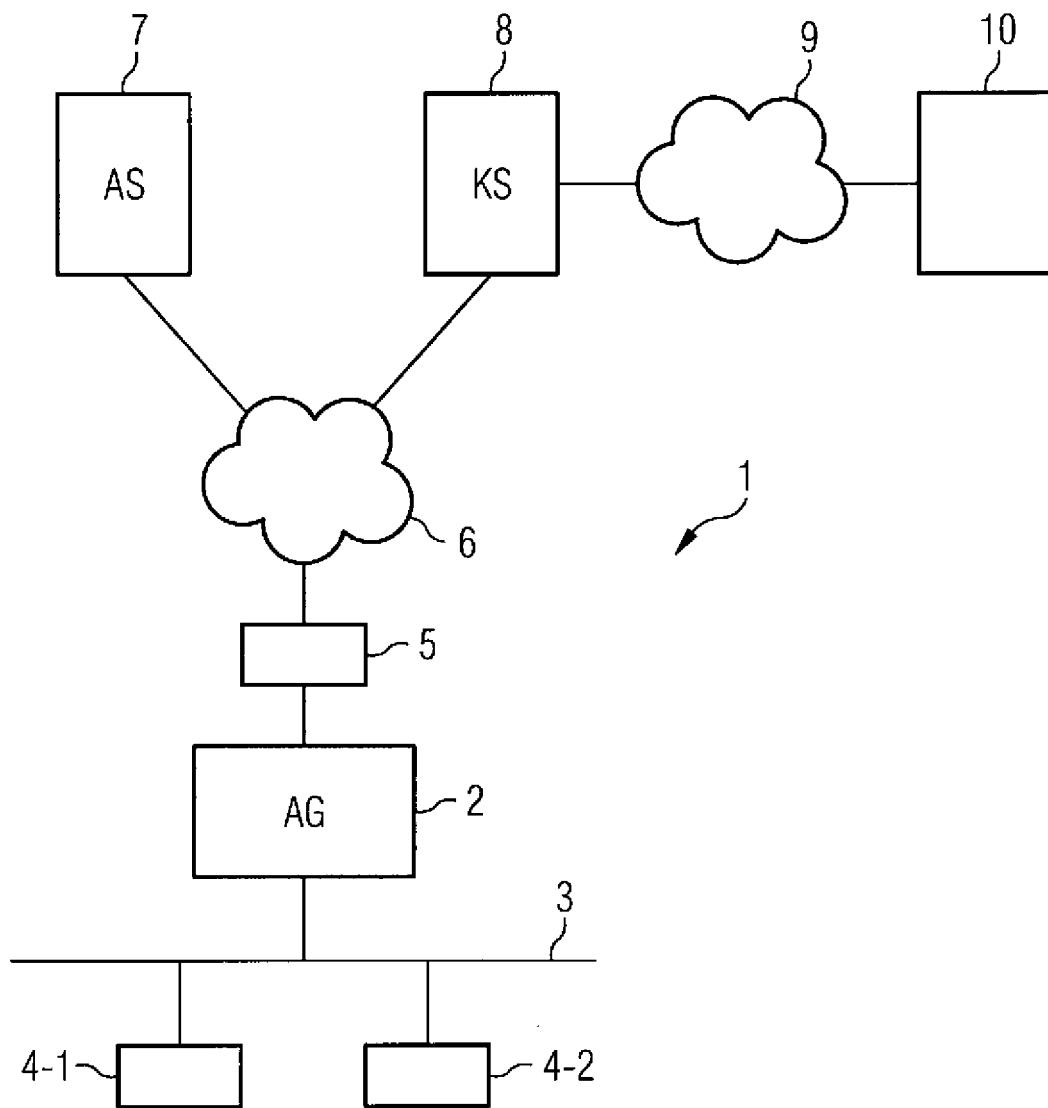




FIG 2

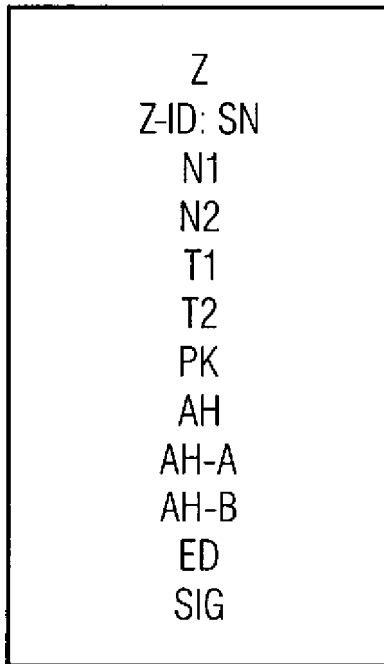
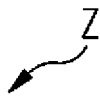


FIG 3

