(19) Deutsches Patent- und Markenamt

(10) **DE 10 2016 220 566 A1** 2018.04.26

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2016 220 566.8**
(22) Anmeldetag: **20.10.2016**
(43) Offenlegungstag: **26.04.2018**

(51) Int Cl.: ***H04L 9/32*** (2006.01)
***H04L 9/30*** (2006.01)

(71) Anmelder:
**Robert Bosch GmbH, 70469 Stuttgart, DE**

(74) Vertreter:
**Thürer, Andreas, Dipl.-Phys., 97816 Lohr, DE**

(72) Erfinder:
**Burchardt, Gunter, 97854 Steinfeld, DE; Rausch, Julien, 97737 Gemünden, DE**

(56) Ermittelter Stand der Technik:

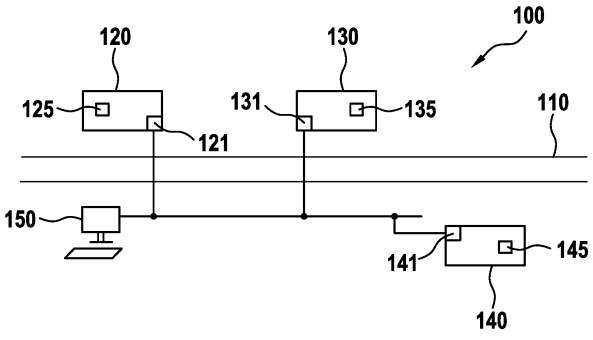
| | | |
|---|---|---|
| **DE** | **10 2014 206 989** | **A1** |
| **US** | **9 030 315** | **B2** |
| **US** | **2014 / 0 229 015** | **A1** |
| **US** | **2015 / 0 169 875** | **A1** |
| **US** | **2015 / 0 363 543** | **A1** |

Rechercheantrag gemäß § 43 PatG ist gestellt.

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

(54) Bezeichnung: **Verfahren zum Starten einer Steuerungskomponente eines Automatisierungssystems, Steuerungskomponente und Automatisierungssystem**

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren zum Starten einer Steuerungskomponente (120, 130, 140) eines Automatisierungssystems (100), das mehrere Steuerungskomponenten (120, 130, 140) umfasst, wobei während eines Startvorgangs automatisiert überprüft wird, ob die Steuerungskomponente (120, 130, 140) ein individuelles kryptographisches Identifikationsmerkmal (125, 135, 145) aufweist, wobei, wenn die Steuerungskomponente (120, 130, 140) ein individuelles kryptographisches Identifikationsmerkmal (125, 135, 145) aufweist, der Startvorgang fortgesetzt wird, und wobei, wenn die Steuerungskomponente (120, 130, 140) kein individuelles kryptographisches Identifikationsmerkmal aufweist, automatisiert ein individuelles Identifikationsmerkmal (125, 135, 145) erzeugt wird und anschließend der Startvorgang fortgesetzt wird, sowie eine solche Steuerungskomponente (120, 130, 140) und ein solches Automatisierungssystem (100).



## Beschreibung

**[0001]** Die vorliegende Erfindung betrifft ein Verfahren zum Starten einer Steuerungskomponente eines Automatisierungssystems, das mehrere Steuerungskomponenten umfasst, eine solche Steuerungskomponente und ein solches Automatisierungssystem.

### Stand der Technik

**[0002]** In der Automatisierungstechnik werden Automatisierungssysteme eingesetzt, die mehrere einzelne Steuerungskomponenten bzw. Steuerungseinheiten (insbesondere sog. SPS, speicherprogrammierbare Steuerungen) umfassen. Solche Automatisierungssysteme werden beispielsweise in der Produktion bzw. in der Fertigung verwendet und können - je nach Einsatzgebiet - verschiedene Steuerungskomponenten umfassen, welche wiederum unterschiedliche Funktionen bzw. Tätigkeiten ausführen.

**[0003]** Aus der US 2015/0363543 A 1 ist beispielsweise bekannt, dass für ein Automatisierungssystem eine Liste mit verwendeten Steuerungskomponenten erstellt werden kann, damit die Steuerungskomponenten bestimmte Operationen durchführen können.

**[0004]** Aus der US 2014/0229015 A1 ist beispielsweise bekannt, dass eine Konfigurationsdatei erstellt werden kann, anhand welcher Steuerungskomponenten identifiziert werden können, mit denen kommuniziert werden sollen.

**[0005]** Aus der US 9 030 315 B2 ist beispielsweise bekannt, dass zur Kommunikation zweier Steuerungskomponenten Identifier verwendet werden, wozu die eine Komponente den Identifier der anderen Komponente empfängt.

### Offenbarung der Erfindung

**[0006]** Erfindungsgemäß werden ein Verfahren zum Starten einer Steuerungskomponente eines Automatisierungssystems, eine Steuerungskomponente und ein Automatisierungssystem mit den Merkmalen der unabhängigen Patentansprüche vorgeschlagen. Vorteilhafte Ausgestaltungen sind Gegenstand der Unteransprüche sowie der nachfolgenden Beschreibung.

**[0007]** Ein erfindungsgemäßes Verfahren dient zum Starten, d.h. zum Hochfahren, einer Steuerungskomponente eines Automatisierungssystems, welches insgesamt mehrere Steuerungskomponenten umfasst. Hierzu wird während eines Startvorgangs automatisiert überprüft, ob die Steuerungskomponente ein individuelles kryptographisches Identifikationsmerkmal aufweist, welches sich zur Verwendung in kryptographischen Verfahren eignet und insbesondere nicht allen anderen Steuerungskomponenten bekannt ist. Unter einem individuellen kryptographischen Identifikationsmerkmal kann ein solches Identifikationsmerkmal verstanden werden, das verschieden von den Identifikationsmerkmalen der übrigen Steuerungskomponenten des Automatisierungssystems ist. Bei einem kryptographischen Identifikationsmerkmal kann es sich beispielsweise um einen Zahlen- und/oder Buchstabencode handeln, der digital lesbar ist. Wenn nun die Steuerungskomponente ein individuelles kryptographisches Identifikationsmerkmal aufweist, wird der Startvorgang fortgesetzt. Andernfalls, d.h. wenn die Steuerungskomponente kein individuelles kryptographisches Identifikationsmerkmal aufweist, wird automatisiert ein individuelles Identifikationsmerkmal erzeugt und anschließend wird der Startvorgang fortgesetzt. Unter der automatisierten Überprüfung bzw. Erzeugung soll hier verstanden werden, dass der entsprechende Vorgang ohne äußere bzw. manuelle Eingriffe erfolgt. Hierzu kann die Steuerungskomponente entsprechend programmiert sein.

**[0008]** Auf diese Weise kann erreicht werden, dass eine Steuerungskomponente eines Automatisierungssystems bereits nach dem Starten, d.h. sobald sie einsatzbereit ist, ein individuelles kryptographisches Identifizierungsmerkmal aufweist, anhand dessen sie innerhalb des Automatisierungssystems eindeutig identifizierbar ist. Damit kann die Steuerungskomponente später beispielsweise gezielt angesprochen werden oder es kann ein gezielter und sicherer (verschlüsselter und/oder signierter) Austausch von Daten, insbesondere Prozessdaten, erfolgen.

**[0009]** Im Vergleich zu bisherigen Verfahren, bei denen die einzelnen Steuerungskomponenten nach dem Starten keine oder zumindest keine geheimen kryptographischen Identifikationsmerkmale aufwiesen, da diese beispielsweise initial bei der Herstellung der Steuerungskomponente von extern hinterlegt werden, ist nun kein manuelles Ändern bzw. Aufbringen der kryptographischen Identifikationsmerkmale bei der Installation bzw. im späteren Betrieb im Rahmen des Automatisierungssystems mehr nötig.

**[0010]** Zudem ergibt sich ein Vorteil gegenüber dem Fall, dass beispielsweise Schlüssel während der Produktion aufgebracht bzw. per Public-Key-Infrastruktur zur Verfügung gestellt werden. Das Risiko dort ist, dass der Schlüssel beim Aufbringen entwendet werden kann. Durch die automatisierte Erzeugung kann dies nicht passieren.

**[0011]** Zweckmäßigerweise können dann auch alle Steuerungskomponenten eines solchen Automatisierungssystems auf die gleiche Weise gestartet werden, wie für eine Steuerungskomponente beschrieben.

**[0012]** Vorzugsweise wird das individuelle kryptographische Identifikationsmerkmal basierend auf wenigstens einer Kenngröße erzeugt, die ausgewählt ist aus: einer Seriennummer, einer Uhrzeit, einer Temperatur, einer mittels Hardware generierten Zufallszahl und einer mittels Software generierten Zufallszahl. All diese Kenngrößen weichen bei unterschiedlichen Steuerungskomponenten voneinander ab und ermöglichen insofern die einfache Erzeugung eines individuellen kryptographischen Identifikationsmerkmals.

**[0013]** Die Seriennummer eines Geräts oder einer Komponente ist dabei einerseits individuell für das Gerät bzw. die Komponente und andererseits in aller Regel auch digital hinterlegt. Als Seriennummer kommt hier zweckmäßigerweise die Seriennummer der Steuerungskomponente in Betracht. Denkbar ist jedoch auch eine Seriennummer eines Bauteils der Steuerungskomponente oder eine Kombination mehrerer solcher Seriennummern. Die Uhrzeit, insbesondere während oder bei Beginn des Erzeugens des Identifikationsmerkmals, ist bei einem Starten der einzelnen Steuerungskomponenten nacheinander bei verschiedenen Steuerungskomponenten verschieden. Die Temperatur der Steuerungskomponenten bzw. an einer gewissen Stelle der Steuerungskomponente, an welcher sie beispielsweise mittels eines Temperatursensors gemessen wird, unterscheidet sich von der Temperatur bei anderen Steuerungskomponenten zumindest in einem Nachkommabereich. Hierzu trägt beispielsweise auch die Ungenauigkeit des Temperatursensors bei. Ebenso unterscheiden sich Zufallszahlen zumindest mit hinreichend hoher Wahrscheinlichkeit bei verschiedenen Steuerungskomponenten. Beispielsweise können dann bei der Erzeugung eines Zertifikats als kryptographisches Identifikationsmerkmal eine oder mehrere (oder alle) eindeutigen Kenngrößen zusätzlich zu einem öffentlichen Schlüssel (beispielsweise einer übergeordneten Steuerung) einfließen.

**[0014]** Vorteilhafterweise wird unter Verwendung des individuellen kryptographischen Identifikationsmerkmals ein Schlüsselpaar, das einen privaten und einen öffentlichen Schlüssel umfasst, erzeugt. Hier kommt beispielsweise ein asymmetrisches Verfahren wie das sog. RSA-Verfahren in Frage. Solche kryptographischen Verfahren ermöglichen eine besonders einfache und effektive Verschlüsselung und Zertifizierung für eine sichere Kommunikation.

**[0015]** Insofern ist es auch zweckmäßig, unter Verwendung des öffentlichen Schlüssels ein kryptographisches Zertifikat zu erzeugen, beispielsweise ein sog. X.509-Zertifkat. Hierbei handelt es sich um ein gängiges und einfaches Zertifikat. In diesem Zusammenhang ist es weiterhin auch zweckmäßig, das kryptographische Zertifikat und/oder den öffentliche Schlüssel an einen öffentlichen Verzeichnisdienst zu übertragen und insbesondere dort zu signieren, da auf diese Weise eine besonders sichere Verschlüsselung erreicht werden kann. In Bezug auf den privaten Schlüssel ist es vorteilhaft, wenn er automatisiert in der Steuerungskomponente hinterlegt wird. Durch die erwähnten Möglichkeiten kann eine sichere Verschlüsselung für die Steuerungskomponente bereitgestellt werden.

**[0016]** Es ist von Vorteil, wenn das individuelle kryptographische Identifikationsmerkmal als Grundlage für eine Kommunikation und/oder einen Datenaustausch mit einer anderen der mehreren Steuerungskomponenten und/oder mit einer übergeordneten Steuerungs- und/oder Bedieneinheit verwendet wird. In Zusammenhang mit den erwähnten Möglichkeiten der Verschlüsselung kann eine solche Kommunikation bzw. ein solcher Datenaustausch auch sehr sicher gemacht werden, was zu einem insgesamt sicheren Automatisierungssystem führt. Das individuelle kryptographische Identifikationsmerkmal kann somit einerseits zum Identifizieren der Steuerungskomponente und andererseits als Basis für die Kommunikation bzw. Verschlüsselung verwendet werden.

**[0017]** Eine erfindungsgemäße Steuerungskomponente für ein Automatisierungssystem, das mehrere Steuerungskomponenten umfasst, ist dazu eingerichtet, ein erfindungsgemäßes Verfahren durchzuführen. Die Steuerungskomponenten kann hierzu insbesondere programmtechnisch entsprechen eingerichtet sein. Vorzugsweise handelt es sich um eine speicherprogrammierbare Steuerung (SPS), numerische Steuerung (numerical control - NC) bzw. CNC-Steuerung (computerized numerical control) oder Bewegungssteuerung (motion control - MC). Vorzugsweise ist die Steuerungskomponente echtzeitfähig, d.h. dass einzelne Rechenschritte innerhalb definierter Zeitspannen abgeschlossen sind. In echtzeitfähigen Umgebungen kann garantiert werden, dass ein Rechenergebnis rechtzeitig vorliegt, so dass insbesondere in Automatisierungssystemen die Bewegungen unterschiedlicher Aggregate auch synchron ablaufen.

**[0018]** Ein erfindungsgemäßes Automatisierungssystem umfasst entsprechend mehrere erfindungsgemäße Steuerungskomponenten. Es versteht sich, dass die einzelnen Verwendungszwecke der jeweiligen Steuerungskomponenten innerhalb des Automatisierungssystems unterschiedlich sein können und in aller Regel auch sind. Jedoch ist ein solches Automatisierungssystem ohne zusätzlichen, insbesondere manuellen Aufwand sofort nach dem Hochstarten einsatzbereit.

**[0019]** Auch die Implementierung des Verfahrens in Form eines Computerprogramms ist vorteilhaft, da dies besonders geringe Kosten verursacht, insbesondere wenn eine ausführende Steuerungskompo-

nente noch für weitere Aufgaben genutzt wird und daher ohnehin vorhanden ist. Geeignete Datenträger zur Bereitstellung des Computerprogramms sind insbesondere magnetische, optische und elektrische Speicher, wie z.B. Festplatten, Flash-Speicher, EEPROMs, DVDs u.a.m. Auch ein Download eines Programms über Computernetze (Internet, Intranet usw.) ist möglich.

**[0020]** Weitere Vorteile und Ausgestaltungen der Erfindung ergeben sich aus der Beschreibung und der beiliegenden Zeichnung.

**[0021]** Es versteht sich, dass die vorstehend genannten und die nachfolgend noch zu erläuternden Merkmale nicht nur in der jeweils angegebenen Kombination, sondern auch in anderen Kombinationen oder in Alleinstellung verwendbar sind, ohne den Rahmen der vorliegenden Erfindung zu verlassen.

**[0022]** Die Erfindung ist anhand eines Ausführungsbeispiels in der Zeichnung schematisch dargestellt und wird im Folgenden unter Bezugnahme auf die Zeichnung ausführlich beschrieben.

Figurenliste

**Fig. 1** zeigt schematisch ein erfindungsgemäßes Automatisierungssystem in einer bevorzugten Ausführungsform.

**Fig. 2** zeigt schematisch einen Ablauf eines erfindungsgemäßen Verfahrens in einer bevorzugten Ausführungsform.

Detaillierte Beschreibung der Zeichnung

**[0023]** In **Fig. 1** ist schematisch ein erfindungsgemäßes Automatisierungssystem **100** in einer bevorzugten Ausführungsform dargestellt. Das Automatisierungssystem **100** weist beispielhaft eine Produktionsstraße **110** auf, entlang welcher drei Steuerungskomponenten **120**, **130** und **140** angeordnet sind.

**[0024]** Jeder dieser Steuerungskomponenten kann eine eigenständige Aufgabe im Rahmen eines Produktionsablaufs zugeordnet sein. Bei diesen Steuerungskomponenten kann es sich beispielsweise um SPS oder dergleichen handeln. Diese Steuerungen genügen den Anforderungen der Echtzeitfähigkeit, um eine deterministische Regelung von Produktionsprozessen, wie z. B. Zeitungsdruck oder Lebensmittelverpackungsdruck, zu gewährleisten.

**[0025]** Weiterhin ist eine übergeordnete Bedieneinheit **150**, hier beispielhaft in Form eines PCs, gezeigt. Die Steuerungskomponenten **120**, **130** und **140** sowie die Bedieneinheit **150** verfügen jeweils über eine Kommunikationseinheit, hier beispielhaft Feldbusschnittstellen, z.B. für Sercos, Profibus usw., über welche eine Kommunikation der einzelnen Steuerungskomponenten untereinander sowie jeder der Steuerungskomponenten mit der Bedieneinheit **150** möglich ist. Für die Steuerungskomponenten **120**, **130** und **140** sind die Kommunikationseinheiten mit den Bezugszeichen **121**, **131** bzw. **141** bezeichnet.

**[0026]** Weiterhin weist jede der Steuerungskomponenten **120**, **130** und **140** jeweils ein individuelles kryptographisches Identifikationsmerkmal **125**, **135** bzw. **145** auf. Dabei sind diese Identifikationsmerkmale jeweils verschieden voneinander. Für eine mögliche Erzeugung der individuellen kryptographischen Identifikationsmerkmale sowie mögliche Arten der individuellen Identifikationsmerkmale sei auf die nachfolgende Beschreibung verwiesen.

**[0027]** In **Fig. 2** ist schematisch ein Ablauf eines erfindungsgemäßen Verfahrens in einer bevorzugten Ausführungsform dargestellt, wie es beispielsweise für jede bzw. mit jeder der in **Fig. 1** gezeigten Steuerungskomponenten durchführbar ist.

**[0028]** In Schritt **200** wird die Steuerungskomponente zunächst gestartet. Ein solcher Startvorgang kann beispielsweise bei der Inbetriebnahme des gesamten Automatisierungssystems initialisiert werden.

**[0029]** In Schritt **210** wird nun während des Startvorgangs überprüft, ob in der Steuerungskomponente ein individuelles kryptographisches Identifikationsmerkmal - auch als Steuerungsidentität bezeichnet - vorhanden ist.

**[0030]** Wenn in Schritt **210** festgestellt wird, dass bereits ein individuelles kryptographisches Identifikationsmerkmal vorhanden ist, das beispielsweise in einem früheren Startvorgang erzeugt worden ist, so wird zu Schritt **230** übergegangen, d.h. der Startvorgang wird fortgesetzt ohne neue Erzeugung eines individuellen kryptographischen Identifikationsmerkmals.

**[0031]** Wenn in Schritt **210** festgestellt wird, dass kein individuelles kryptographisches Identifikationsmerkmal vorhanden ist, so wird zu Schritt **220** übergegangen. In Schritt **220** wird nun ein individuelles kryptographisches Identifikationsmerkmal für die Steuerungskomponente erzeugt und vorteilhafterweise in einem sicheren, insbesondere nicht extern auslesbaren Speicher gespeichert.

**[0032]** Für die Erzeugung des individuellen kryptographischen Identifikationsmerkmals kann nun auf verschiedene Kenngrößen zurückgriffen werden, die es ermöglichen, ein Identifikationsmerkmal zu erzeugen, das sich von denjenigen der anderen Steuerungskomponenten unterscheidet. Als solche Kenngrößen kommen, wie bereits erwähnt, beispielsweise die Seriennummer der Steuerungskomponente und/oder eines Bauteils davon, die aktuelle Uhrzeit, die

Temperatur der Steuerungskomponente bzw. an einer bestimmten Stelle der Steuerungskomponente und/oder auch Zufallszahlen, die basierend auf Hardware und/oder Software generiert werden, in Frage.

**[0033]** Das Identifikationsmerkmal kann dann auch für ein Verschlüsselungsverfahren, bspw. das RSA-Verfahren, das einen privaten und öffentlichen Schlüssel umfasst, verwendet werden. Während der private Schlüssel für eine spätere Kommunikation auf der Steuerungskomponente verbleiben kann, kann der öffentliche Schlüssel an die Bedieneinheit und darüber oder auch direkt an einen öffentlichen Verzeichnisdienst für eine Signatur übertragen werden. Ebenso kann unter Verwendung des öffentlichen Schlüssels auch ein Zertifikat erzeugt werden, das für die spätere Kommunikation herangezogen werden kann.

**[0034]** Nach der Erzeugung des individuellen kryptographischen Identifikationsmerkmals kann nun zu Schritt **230** übergegangen werden, d.h. der Startvorgang kann weiter fortgesetzt werden.

**[0035]** Das beschriebene Verfahren kann bei jeder Steuerungskomponente durchgeführt werden. Damit wird erreicht, dass nach dem Hochstarten jede der Steuerungskomponenten ein individuelles kryptographisches Identifikationsmerkmal aufweist, auf dessen Grundlage nunmehr die einzelnen Steuerungskomponenten innerhalb des Automatisierungssystems identifizierbar sind.

**[0036]** Dies ermöglicht eine zielgerichtete Kommunikation und einen zielgerichteten Datenaustausch, beispielsweise für Prozessdaten, die während des Betriebs erzeugt werden bzw. anfallen, zum einen zwischen verschiedenen Steuerungskomponenten untereinander und zum anderen zwischen einer Steuerungskomponente und der Bedieneinheit.

**[0037]** Für die Kommunikation selbst kann zudem unter Verwendung der individuellen kryptographischen Identifikationsmerkmale bzw. der damit korrelierten Schlüssel bzw. Zertifikate eine sichere Kommunikation eingerichtet werden. Ebenso kann über die Bedieneinheit eine bestimmte Steuerungskomponente gezielt angesprochen werden. Eine manuelle Vergabe individueller Identifikationsmerkmale ist nicht mehr nötig.

**ZITATE ENTHALTEN IN DER BESCHREIBUNG**

*Diese Liste der vom Anmelder aufgeführten Dokumente wurde automatisiert erzeugt und ist ausschließlich zur besseren Information des Lesers aufgenommen. Die Liste ist nicht Bestandteil der deutschen Patent- bzw. Gebrauchsmusteranmeldung. Das DPMA übernimmt keinerlei Haftung für etwaige Fehler oder Auslassungen.*

**Zitierte Patentliteratur**


- US 2015/0363543 A [0003]
- US 2014/0229015 A1 [0004]
- US 9030315 B2 [0005]

## Patentansprüche

1. Verfahren zum Starten einer Steuerungskomponente (120, 130, 140) eines Automatisierungssystems (100), das mehrere Steuerungskomponenten (120, 130, 140) umfasst, wobei während eines Startvorgangs automatisiert überprüft wird, ob die Steuerungskomponente (120, 130, 140) ein individuelles kryptographisches Identifikationsmerkmal (125, 135, 145) aufweist, wobei, wenn die Steuerungskomponente (120, 130, 140) ein individuelles kryptographisches Identifikationsmerkmal (125, 135, 145) aufweist, der Startvorgang fortgesetzt wird, und wobei, wenn die Steuerungskomponente (120, 130, 140) kein individuelles kryptographisches Identifikationsmerkmal aufweist, automatisiert ein individuelles kryptographisches Identifikationsmerkmal (125, 135, 145) erzeugt wird und anschließend der Startvorgang fortgesetzt wird.

2. Verfahren nach Anspruch 1, wobei das individuelle kryptographische Identifikationsmerkmal (125, 135, 145) basierend auf wenigstens einer Kenngröße erzeugt wird, die ausgewählt ist aus: einer Seriennummer, einer Uhrzeit, einer Temperatur, einer mittels Hardware generierten Zufallszahl und einer mittels Software generierten Zufallszahl.

3. Verfahren nach Anspruch 1 oder 2, wobei unter Verwendung des individuellen kryptographischen Identifikationsmerkmals (125, 135, 145) ein Schlüsselpaar, das einen privaten und einen öffentlichen Schlüssel umfasst, erzeugt wird.

4. Verfahren nach Anspruch 3, wobei unter Verwendung des öffentlichen Schlüssels ein kryptographisches Zertifikat erzeugt wird.

5. Verfahren nach Anspruch 4, wobei das kryptographische Zertifikat an einen öffentlichen Verzeichnisdienst übertragen und insbesondere dort signiert wird.

6. Verfahren nach einem der Ansprüche 3 bis 5, wobei der öffentliche Schlüssel an einen öffentlichen Verzeichnisdienst übertragen und insbesondere dort signiert wird.

7. Verfahren nach einem der Ansprüche 3 bis 6, wobei der private Schlüssel automatisiert in der Steuerungskomponente (120, 130, 140) hinterlegt wird.

8. Verfahren nach einem der vorstehenden Ansprüche, wobei das individuelle kryptographische Identifikationsmerkmal (125, 135, 145) als Grundlage für eine Kommunikation und/oder einen Datenaustausch mit einer anderen der mehreren Steuerungskomponenten (120, 130, 140) und/oder mit einer übergeordneten Steuerungs- und/oder Bedieneinheit (150) verwendet wird.

9. Verfahren zum Starten aller Steuerungskomponenten (120, 130, 140) eines Automatisierungssystems (100), das mehrere Steuerungskomponenten (120, 130, 140) umfasst, wobei jede der Steuerungskomponenten (120, 130, 140) gemäß einem Verfahren nach einem der vorstehenden Ansprüche gestartet wird.

10. Steuerungskomponente (120, 130, 140) für ein Automatisierungssystem (100), das mehrere Steuerungskomponenten (120, 130, 140) umfasst, die dazu eingerichtet ist, ein Verfahren nach einem der vorstehenden Ansprüche durchzuführen.

11. Automatisierungssystem (100) mit mehreren Steuerungskomponenten (120, 130, 140) nach Anspruch 10.

12. Computerprogramm, das eine Steuerungskomponente (120, 130, 140) veranlasst, ein Verfahren nach einem der Ansprüche 1 bis 9 durchzuführen, wenn es auf der Steuerungskomponente (120, 130, 140) ausgeführt wird.

13. Maschinenlesbares Speichermedium mit einem darauf gespeicherten Computerprogramm nach Anspruch 12.

Es folgt eine Seite Zeichnungen

**Anhängende Zeichnungen**

Fig. 1

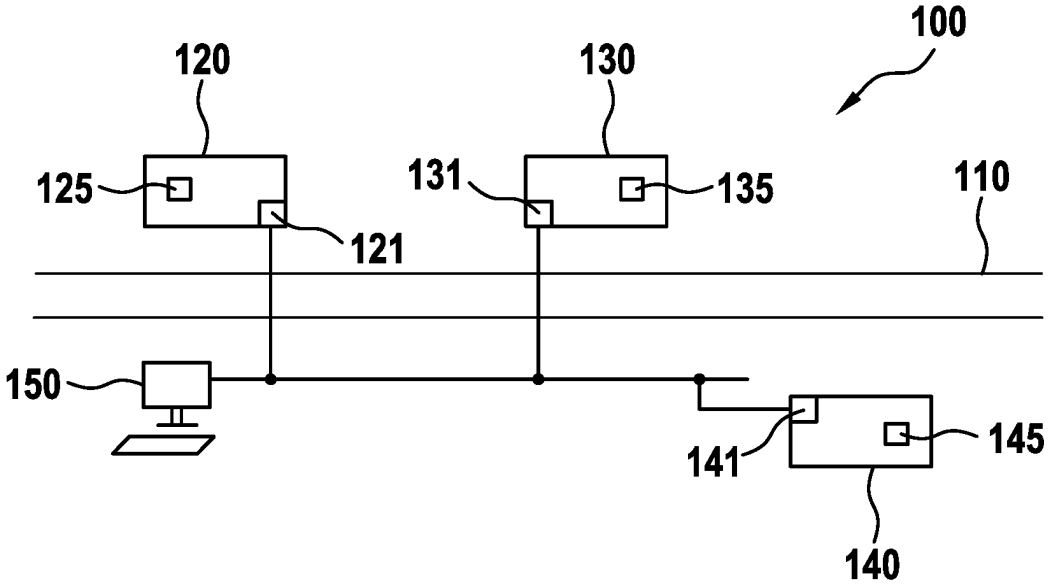



Fig. 2