



(12) **EUROPÄISCHE PATENTANMELDUNG**

(43) Veröffentlichungstag:
22.01.2020 Patentblatt 2020/04

(51) Int Cl.:
G07C 9/00 (2020.01)

(21) Anmeldenummer: **18186555.1**

(22) Anmeldetag: **31.07.2018**

(84) Benannte Vertragsstaaten:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Benannte Erstreckungsstaaten:
BA ME
Benannte Validierungsstaaten:
KH MA MD TN

(71) Anmelder: **EUCHNER GmbH + Co. KG**
70771 Leinfelden-Echterdingen (DE)

(72) Erfinder: **Rothenburg, Jens**
72622 Nürtingen (DE)

(74) Vertreter: **Ruckh, Rainer Gerhard**
Patentanwalt
Jurastrasse 1
73087 Bad Boll (DE)

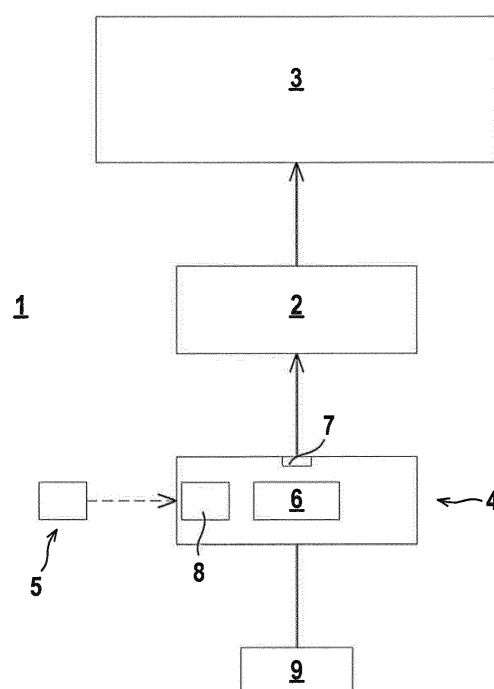
(30) Priorität: **18.07.2018 EP 18184199**

(54) **ZUGANGSSYSTEM**

(57) Die Erfindung betrifft ein Zugangssystem (1) zur Kontrolle eines Zugriffs auf eine von einer Steuerung (2) gesteuerten Anlage (3). Dies erfolgt mittels eines Zugangssystems (1) mit einer Zugangskontrolleinheit (4) und wenigstens einem elektronischen Schlüssel (5). Die Zugangskontrolleinheit (4) ist zum Lesen von in einem elektronischen Schlüssel (5) gespeicherten Schlüssel-

daten ausgebildet. In der Zugangskontrolleinheit (4) sind Kriterien vorgebbbar, anhand derer die Gültigkeit der gelesenen Schlüsseldaten von diesem elektronischen Schlüssel (5) festgestellt werden. Die Zugangskontrolleinheit (4) sendet bei Erkennung eines gültigen elektronischen Schlüssels (5) wenigstens ein Signal an die Steuerung (2).

Fig. 1



Beschreibung

[0001] Die Erfindung betrifft ein Zugangssystem und ein Verfahren zur Kontrolle eines Zugriffs auf eine von einer Steuerung gesteuerten Anlage.

[0002] Derartige Zugangssysteme dienen insbesondere zur Zugangskontrolle zu Anlagen, wobei Anlagen im Sinne der vorliegenden Erfindung auch Maschinen, Arbeitsgeräte und dergleichen umfassen. Generell können bei derartigen Zugangssystemen definiert Berechtigungen derart vorgegeben werden, dass nur bestimmte Personen Zugriff auf die Anlage haben können, wobei weiter individuell der Zugriff auf bestimmte Bereiche oder Funktionen der Anlage begrenzt sein kann.

[0003] Bekannte Zugangssysteme arbeiten beispielsweise mit mechanischen Schlüsselschaltern. Bei diesem Zugangssystem kann ein Schlüsselschalter in unterschiedlichen Dreh- und Rastpositionen in eine Schlüsselaufnahme einer Zugangskontrolleinheit eingeführt werden. Abhängig von der jeweiligen Dreh- und Rastposition können unterschiedliche Zugriffsberechtigungen für einen Zugriff auf die Anlage vorgegeben werden. Nachteilig hierbei ist, dass die Anzahl der Dreh- und Rastpositionen sehr begrenzt ist, so dass nur wenig unterschiedliche Zugriffsberechtigungen vergeben werden können.

[0004] Weiter bekannte Zugangssysteme arbeiten mit elektronischen Schlüsseln, die beispielsweise in Form von Transpondern, USB-Speichern oder Magnetstreifen ausgebildet sind. In den elektronischen Schlüsseln ist jeweils eine Kennung gespeichert, die von einer Zugangskontrolleinheit gelesen werden kann. Wird eine Kennung in der Zugangskontrolleinheit als gültig erkannt, wird über diese ein Zugriff auf die Anlage ermöglicht. In den elektronischen Schlüsseln können auch weitere Informationen abgespeichert sein. In diesem Fall können diese Informationen untereinander oder mit der Kennung verknüpft sein, wodurch unterschiedliche Zugangscodes für den Zugriff auf die Anlage gebildet werden können.

[0005] Weiterhin bekannt sind Zugangssysteme in Form von Passwortsystemen. Vorteilhaft hierbei ist, dass nahezu beliebig viele Passwörter zur Verfügung stehen, so dass entsprechend viele Zugänge zur Anlage zur Verfügung stehen. Nachteilig bei derartigen Zugangssystemen ist, dass sich die Benutzer nicht beliebig viele Passwörter merken können, was benutzerunfreundlich ist. Auch werden Passwörter von den Benutzern typischerweise nicht verändert und oft anderen Personen zugänglich gemacht, so dass die Passwörter letztendlich keinen sicheren Zugangsschutz bilden.

[0006] Schließlich ist es bekannt, durch eine Programmierung der Steuerung der Anlage eine Zugangskontrolle zu realisieren. Nachteilig hierfür ist, dass die Steuerung der Anlage nicht für eine solche Zugangskontrolle ausgelegt ist. Für eine entsprechende Programmierung ist daher ein hoher Aufwand erforderlich.

[0007] Der Erfindung liegt die Aufgabe zugrunde ein Zugangssystem bereitzustellen, welches eine hohe

Funktionalität aufweist.

[0008] Zur Lösung dieser Aufgabe sind die Merkmale der unabhängigen Ansprüche vorgesehen. Vorteilhafte Ausführungsformen und zweckmäßige Weiterbildungen der Erfindung sind in den abhängigen Ansprüchen beschrieben.

[0009] Die Erfindung betrifft ein Zugangssystem zur Kontrolle eines Zugriffs auf eine von einer Steuerung gesteuerten Anlage, mit einer Zugangskontrolleinheit und wenigstens einem elektronischen Schlüssel, wobei die Zugangskontrolleinheit zum Lesen von in einem elektronischen Schlüssel gespeicherten Schlüsseldaten ausgebildet ist. In der Zugangskontrolleinheit sind Kriterien vorgegebbar, anhand derer die Gültigkeit eines elektronischen Schlüssels anhand der von diesem gelesenen Schlüsseldaten festgestellt wird. Bei Erkennung eines gültigen elektronischen Schlüssels sendet die Zugangskontrolleinheit wenigstens ein Signal an die Steuerung.

[0010] Die Erfindung betrifft weiterhin ein entsprechendes Verfahren.

[0011] Mit dem erfindungsgemäßen Zugangssystem können flexibel und angepasst an applikationsspezifische Randbedingungen unterschiedliche Zugriffe auf die Anlage vorgegeben werden. Dabei bildet das Zugangssystem mit der Zugangskontrolleinheit und dieser zugeordneten elektronischen Schlüsseln ein sicheres, insbesondere manipulationssicheres System, mit dem ein Zugriff auf die Anlage kontrolliert werden kann.

[0012] Der Grundgedanke der Erfindung besteht dabei darin, dass in der Zugangskontrolleinheit durch einen Anwender unterschiedliche Kriterien vorgegeben werden können, anhand derer die Gültigkeit eines elektronischen Schlüssels festgestellt werden kann. Der Anwender kann dabei alle oder nur einen Teil der im elektronischen Schlüssel gespeicherten Schlüsseldaten für eine Gültigkeitsprüfung nutzen. Weiterhin ist anhand von Schlüsseldaten auch eine Betriebsartenwahl der Anlage möglich. Eine Betriebsartenwahl kann, wie beispielsweise in DE 10 2015 114 717 A1 beschrieben, einen Automatikbetrieb einer Anlage und/oder einen Betrieb der Anlage mit oder ohne Sicherheitsüberwachung umfassen.

[0013] Die Zugangskontrolleinheit bildet dabei eine programmierbare Einheit mit einem Prozessor oder dergleichen. Durch ein geeignetes Konfigurationssystem mit Eingabemöglichkeit kann ein Anwender einfach und schnell Kriterien für eine Gültigkeit eines elektronischen Schlüssels definieren. Durch die Definition unterschiedlicher Kriterien kann der Anwender auch unterschiedliche Zugriffsberechtigungen derart definieren, dass mit einem elektronischen Schlüssel, dessen Schlüsseldaten von der Zugangskontrolleinheit gelesen und als gültig klassifiziert werden, nur bestimmte Bereiche oder bestimmte Funktionen der Anlage freigegeben werden.

[0014] Vorteilhaft hierbei ist insbesondere, dass sämtliche auf einem elektronischen Schlüssel gespeicherte Schlüsseldaten einzeln oder in Kombination zur Definition von Gültigkeitskriterien herangezogen werden können. Dies ermöglicht eine entsprechende Vielfalt von un-

terschiedlichen Zugriffsberechtigungen für die Anlage.

[0015] Ein wesentlicher Aspekt der Erfindung besteht darin, dass die Kriterien für eine Gültigkeit eines elektronischen Schlüssels allein in der Zugangskontrolleinheit festgelegt werden, wobei ein Anwender hierzu geeignete Eingabebefehle in die Zugangskontrolleinheit eingibt. Dies hat den Vorteil, dass in der Steuerung keinerlei Einheiten, insbesondere keine zu programmierenden Module für eine Zugangskontrolle zur Anlage vorgesehen werden müssen. Vielmehr werden in der Zugangskontrolleinheit Signale an die Steuerung gesendet, die von dieser unmittelbar als Steuerbefehle eingesetzt werden können.

[0016] Mit der Zugangskontrolleinheit kann eine generelle Erkennung der Gültigkeit eines elektronischen Schlüssels durchgeführt werden, insbesondere derart, dass die Gültigkeit eines elektronischen Schlüssels anhand einer in einem nicht beschreibbaren Speicher des elektronischen Schlüssels gespeicherten Kennung festgestellt wird. Bekannterweise weist der elektronische Schlüssel einen Speicher mit einem vom Anwender beschreibbaren und einem nicht beschreibbaren Teil auf.

[0017] Die so im elektronischen Schlüssel gespeicherte Kennung bildet somit einen unveränderlichen, individuellen Code, der zur Identifikation des elektronischen Schlüssels herangezogen werden kann.

[0018] Weiterhin kann eine Gültigkeit eines elektronischen Schlüssels auch anhand eines in diesem gespeicherten Ablaufdatums geprüft werden.

[0019] Schließlich wird die Gültigkeit eines elektronischen Schlüssels anhand einer Prüfsumme für im elektronischen Schlüssel gespeicherte Schlüsseldaten festgestellt.

[0020] Dabei ist zweckmäßig der Umfang der Prüfsumme einstellbar.

[0021] Vorteilhaft schließt die Prüfsumme die im elektronischen Schlüssel gespeicherte Kennung im nicht beschreibbaren Teil des Speichers mit ein.

[0022] Die Prüfsummenkontrolle erfolgt dabei derart, dass anhand der im elektronischen Schlüssel gespeicherten Schlüsseldaten die Prüfsumme in der Zugangskontrolleinheit berechnet und mit einem im elektronischen Schlüssel gespeicherten Wert verglichen wird.

[0023] Mit der Prüfsummenkontrolle wird ein Schutz gegen ein Kopieren des elektronischen Schlüssels ermöglicht, da bei einem Kopieren des Schlüssels die Kennung nicht mitkopiert wird, sondern nur in einem beschreibbaren Speicher gespeicherte weitere Schlüsseldaten. Da das Kopieren auf einen elektronischen Schlüssel mit einer anderen Kennung erfolgt, stimmt nach dem Kopieren die Prüfsumme für diesen neuen elektronischen Schlüssel nicht mehr, wodurch der unerlaubte Kopiervorgang erkannt wird.

[0024] Neben der generellen Erkennung der Gültigkeit eines elektronischen Schlüssels ist erfindungsgemäß auch eine spezielle Erkennung der Gültigkeit eines elektronischen Schlüssels möglich. Hierzu sind als Kriterium für die Gültigkeit eines elektronischen Schlüssels ver-

schiedenartige Schlüsseldaten, die auf diesem elektronischen Schlüssel gespeichert sind, mit einer einstellbaren Logikfunktion verknüpft.

[0025] Dabei wird ausgenutzt, dass verschiedenartige Schlüsseldaten auf unterschiedlichen Bereichen eines beschreibbaren Speichers eines elektronischen Schlüssels gespeichert sind.

[0026] Die Zugangskontrolleinheit kann somit von dem elektronischen Schlüssel die verschiedenartigen Schlüsseldaten in den unterschiedlichen Bereichen des beschreibbaren Speichers auslesen und mit Logikfunktionen zur Definition von Gültigkeitskriterien verknüpfen.

[0027] Als verschiedenartige Daten können Anwender des elektronischen Schlüssels, Angaben über die Anlage, wie das Werk, wo diese installiert ist, ggf. weiter ergänzt durch Bereich oder Abteilung, oder auch spezifische Teile der Anlage im elektronischen Schlüssel gespeichert sein.

[0028] Da insbesondere auch anwenderspezifische Daten des elektronischen Schlüssels gespeichert werden, können auch für elektronische Schlüssel unterschiedlicher Hersteller Gültigkeitskriterien definiert werden, was bedeutet, dass mit elektronischen Schlüsseln unterschiedlicher Hersteller ein Zugriff auf die Anlage möglich ist, wobei durch eine anwenderspezifische Programmierung der Zugangskontrolleinheit, insbesondere eine Vorgabe von Logikfunktion, Art und Umfang des Zugriffs, flexibel vorgegeben werden können.

[0029] Die Zugangskontrolleinheit bietet dabei eine Auswahl unterschiedlicher Logikfunktionen an.

[0030] Insbesondere kann eine beliebige Kombination von Logikfunktionen wie einem "UND", einem "ODER", einem "NICHT" oder einem "VERGLEICHEN" vorgesehen sein.

[0031] Dabei können in der Zugangskontrolleinheit mehrere Logikfunktionen zu einer Logikbedingung zusammengefasst sein, wobei die Logikbedingung ein Kriterium für die Gültigkeit eines elektronischen Schlüssels ist und/oder zur Vorgabe von Funktionen der Anlage dient.

[0032] Insbesondere sind in der Logikbedingung Logikfunktionen mit Klammern gruppiert.

[0033] Ein wesentlicher Aspekt der Erfindung besteht darin, dass die anwenderspezifische Vorgabe der Zugangskontrolle für die Anlage allein in der Zugangskontrolleinheit erfolgt und diese an die Steuerung der Anlage direkt Signale, insbesondere Steuerbefehle, weitergibt, die in der Steuerung direkt eingesetzt werden können.

[0034] Gemäß einer vorteilhaften Ausführungsform ist das an die Steuerung ausgegebene Signal ein EIN-Signal zur Freigabe des Betriebs der Anlage oder ein AUS-Signal zum Stillsetzen der Anlage.

[0035] Alternativ wird mit einem an die Steuerung gesendeten Signal eine Betriebsart der Anlage ausgewählt.

[0036] Dadurch wird die Funktionalität der Zugangskontrolleinheit erheblich erweitert. Insbesondere ist vorteilhaft, dass mit der Zugangskontrolleinheit auch eine sichere, d. h. fehlersichere Betriebsartenwahl im Sinne

der Maschinensicherheit, nicht der Zugangssicherheit bewerkstelligt werden kann, was für einen Einsatz des Zugangssystems im Bereich der Sicherheitstechnik notwendig ist. Generell weist das erfindungsgemäße Zugangssystem eine fehlersichere Funktionalität im Sinne der Maschinensicherheit auf.

[0037] Die Betriebsartenwahl kann durch Lesen eines elektronischen Schlüssels mittels der Zugangskontrolleinheit initiiert werden. Hierzu ist in einem elektronischen Schlüssel als Schlüsseldaten eine Berechtigung für eine Betriebsartenwahl der Anlage gespeichert.

[0038] Vorteilhaft ist für eine Betriebsartenwahl die Zugangskontrolleinheit über ein Bussystem oder eine andere geeignete Kommunikationsschnittstelle, wie zum Beispiel USB, mit einem Bediengerät zum Beispiel mit einem Touchbildschirm als Eingabeeinheit verbunden. Die Zugangskontrolleinheit sendet nach Lesen einer Berechtigung für eine Betriebsartenwahl in einem elektronischen Schlüssel eine Anforderung an das Bediengerät, worauf das Bediengerät eine ausgewählte Betriebsart an die Zugangskontrolleinheit sendet, welche als Signal an die Steuerung weitergegeben wird.

[0039] Für die Verbindung zwischen Zugangskontrolleinheit und Bediengerät ist ein nicht sicheres Bussystem vorgesehen. Dennoch kann eine sichere Betriebsartenwahl durchgeführt werden, indem mit der Zugangskontrolleinheit und/oder dem Bediengerät ein sicheres Auswahlverfahren wie in der Anmeldung DE 10 2015 114 717 A1 für die Betriebsartenwahl bereitgestellt wird.

[0040] Weiter vorteilhaft ist die Betriebsartenwahl konfigurierbar, d. h. der Anwender selbst kann Art und Umfang der Betriebsartenwahl vorgeben.

[0041] Die Erfindung wird im Folgenden anhand der Zeichnungen erläutert. Es zeigen:

Figur 1: Erstes Ausführungsbeispiel des erfindungsgemäßen Zugangssystems.

Figur 2: Schematische Darstellung des Speichers eines elektronischen Schlüssels für das Zugangssystem gemäß Figur 1.

Figur 3: Zweites Ausführungsbeispiel des erfindungsgemäßen Zugangssystems.

[0042] Figur 1 zeigt ein erstes Ausführungsbeispiel des erfindungsgemäßen Zugangssystems 1 zur Kontrolle eines Zugriffs auf eine von einer Steuerung 2 gesteuerte Anlage 3. Die Anlage 3 kann generell auch eine Maschine, ein Arbeitsgerät oder auch ein fahrbares System sein. Die Steuerung 2 kann von einer SPS-Steuerung oder dergleichen gebildet sein.

[0043] Das Zugangssystem 1 weist als wesentliche Komponenten eine Zugangskontrolleinheit 4 und dieser zugeordnete elektronische Schlüssel 5 auf, von welchen in Figur 1 nur einer dargestellt ist. Im vorliegenden Fall bestehen die elektronischen Schlüssel 5 aus einem Transponder. Prinzipiell können die elektronischen

Schlüssel 5 auch von Chips, Magnetstreifen und dergleichen gebildet sein.

[0044] Die Zugangskontrolleinheit 4 weist einen Prozessor 6, insbesondere einen Mikroprozessor auf, der die Funktionen der Zugangskontrolleinheit 4 steuert. Die Zugangskontrolleinheit 4 weist weiterhin eine Ausgangsstruktur 7 mit einem oder mehreren Ausgängen oder/und einem Kommunikationssystem, zum Beispiel Bus auf, über welche die Zugangskontrolleinheit 4 mit der Steuerung 2 verbunden ist. Weiterhin weist die Zugangskontrolleinheit 4 eine Sensoreinheit 8 auf, mit der in einem elektronischen Schlüssel 5 gespeicherte Schlüsseldaten gelesen werden können. Um Schlüsseldaten aus einem elektronischen Schlüssel 5 auslesen zu können, muss der elektronische Schlüssel 5 so dicht an die Zugangskontrolleinheit 4 herangeführt werden, dass er innerhalb eines Leseabstands zur Leseinheit angeordnet ist. Hierzu kann prinzipiell der elektronische Schlüssel 5 durch eine nicht dargestellte Aufnahme der Zugangskontrolleinheit 4 eingeführt werden.

[0045] Schließlich ist die Zugangskontrolleinheit 4 zum Zwecke der Konfiguration mit einer Ein-/Ausgabereinheit 9 mit einer geeigneten Bedienoberfläche verbunden, über welche ein Anwender Eingabegrößen in die Zugangskontrolleinheit 4 bzw. deren Prozessor 6 eingeben kann. Prinzipiell könnte die Ein-/Ausgabereinheit 9 auch in der Zugangskontrolleinheit 4 integriert sein.

[0046] Die Funktionsweise des Zugangssystems 1 ist generell derart, dass aus einem elektronischen Schlüssel 5 ausgelesene Schlüsseldaten in der Zugangskontrolleinheit 4 nach dort vorgegebenen Gültigkeitskriterien geprüft werden, ob ein gültiger elektronischer Schlüssel 5 vorliegt. Wird ein elektronischer Schlüssel 5 als gültig erkannt, gewährt die Zugangskontrolleinheit 4 einen kontrollierten Zugriff auf die Anlage 3. Hierzu sendet die Zugangskontrolleinheit 4 über die Ausgangsstruktur 7 entsprechende Signale an die Steuerung 2.

[0047] Erfindungsgemäß werden anwenderspezifisch, durch geeignete Eingaben des Anwenders über die Ein-/Ausgabereinheit 9, Gültigkeitskriterien für die elektronischen Schlüssel 5 vorgegeben. Die Vergabe von Gültigkeitskriterien und die Prüfung der Erfüllung der Gültigkeitskriterien für die einzelnen elektronischen Schlüssel 5 erfolgt somit in der Zugangskontrolleinheit 4 und nicht in der Steuerung 2. Von der Zugangskontrolleinheit 4 werden bei Erkennen eines gültigen elektronischen Schlüssels 5 Signale in Form von Steuerbefehlen an die Steuerung 2 gesandt, die dort ermittelt bzw. für die Steuerung 2 der Anlage 3 vorgesehen werden können.

[0048] Insbesondere kann das an die Steuerung 2 ausgegebene Signal auch ein EIN-Signal zur Freigabe des Betriebs der Anlage 3 oder ein AUS-Signal zum Stillsetzen der Anlage 3 sein. Weiterhin können Daten an die Anlage 3 gesendet werden, insbesondere um deren Funktionen vorzugeben.

[0049] Figur 2 zeigt schematisch den in unterschiedliche Bereiche a, b1 ... bN unterteilten Speicher eines

elektronischen Schlüssels 5. Der Bereich a bildet einen nicht beschreibbaren Speicher, in welchem eine Kennung des elektronischen Schlüssels 5 hinterlegt ist. Die Bereiche b1 ... bN sind beschreibbare Speicher. In allen elektronischen Schlüsseln 5 ist eine entsprechende Unterteilung des Speichers vorgesehen. In den einzelnen Bereichen b1 ... bN sind jeweils Anwender-Schlüsseldaten hinterlegt. Derartige Schlüsseldaten können Daten betreffend die Anlage 3 sein. Weiterhin kann ein Ablaufdatum für einen elektronischen Schlüssel 5 hinterlegt sein. Schließlich ist ein Bereich für die Speicherung einer vorzugsweise einstellbaren Prüfsumme vorgesehen. Die Prüfsumme umfasst die Kennung und vorzugsweise eine oder alle der weiteren Schlüsseldaten.

[0050] In der Zugangskontrolleinheit 4 erfolgt eine Gültigkeitsprüfung eines elektronischen Schlüssels 5 anhand der aus diesen ausgelesenen Daten, wobei die Gültigkeitskriterien in der Zugangskontrolleinheit 4 von einem Anwender über die Ein-/Ausgabeeinheit 9 vorgegeben werden können.

[0051] Gültigkeitskriterien können zum Beispiel die Erkennung der Kennung, der Prüfsumme und/oder des Ablaufdatums sein.

[0052] Bei Erkennung einer gültigen Kennung oder der Prüfsumme bzw. bei noch nicht abgelaufenen Ablaufdaten wird der elektronische Schlüssel 5 als gültig erkannt und die Zugangskontrolleinheit 4 generiert ein Signal für die Steuerung 2, beispielsweise ein EIN Signal zur Freigabe von Funktionen der Anlage 3. Auch kann, je nach Ergebnis der Gültigkeitsprüfung nur ein Teil der Funktionen der Anlage 3 freigegeben werden.

[0053] Alternativ oder zusätzlich können für eine Gültigkeitsprüfung Schlüsseldaten aus unterschiedlichen Bereichen b1 ... bN durch anwenderspezifisch vorgebbaren Logikfunktionen verknüpft werden. Dabei ist eine Logikfunktion ein "immer WAHR", ein "UND", ein "ODER", ein "NICHT" oder ein "VERGLEICHEN".

[0054] Insbesondere können mehrere Logikfunktionen zu einer Logikbedingung zusammengefasst sein, wobei die Logikbedingung ein Kriterium für die Gültigkeit eines elektronischen Schlüssels 5 ist.

[0055] Dabei können in den Logikbedingungen Logikfunktionen mit Klammern gruppiert werden.

[0056] Die Gültigkeitskriterien können mit unterschiedlichen Zugriffsberechtigungen verknüpft sein, so dass je nach festgestellter Gültigkeit unterschiedliche Zugriffe auf die Anlage 3 freigegeben werden.

[0057] Figur 3 zeigt ein zweites Ausführungsbeispiel des Zugangssystems 1. Dieses Zugangssystem 1 unterscheidet sich von dem Ausführungsbeispiel gemäß Figur 1 nur dadurch, dass die Zugangskontrolleinheit 4 über ein Bussystem 10 oder eine andere Kommunikationsschnittstelle an ein Bediengerät 11 angeschlossen ist. Hierzu weisen die Zugangskontrolleinheit 4 und das Bediengerät 11 einen Busanschluss 12 auf. Das Bussystem 10 ist als nicht sicheres Bussystem 10 ausgebildet. Prinzipiell kann das Bediengerät 11 auch an die Steuerung 2 angeschlossen sein.

[0058] Mittels diesem Zugangssystem 1 kann eine Betriebsartenwahl für die Anlage 3 durchgeführt werden. Eine Betriebsartenwahl wird dadurch initiiert, wenn die Zugangskontrolleinheit 4 einen elektronischen Schlüssel 5 liest, in welchem eine Berechtigung für eine Betriebsartenwahl gespeichert ist. Die Zugangskontrolleinheit 4 sendet darauf eine Anforderung an das Bediengerät 11, das darauf eine ausgewählte Betriebsart zum Beispiel wie in Anmeldung DE 10 2015 114 717 A1 beschrieben sendet, und diese von dem Zugangssystem 1 als Signal an die Steuerung 2 weiterleitet, wo die Betriebsart aktiviert wird. Die Betriebsartenwahl kann fehlersicher erfolgen, obwohl das Bussystem 10 nicht sicher ist. Die erforderliche Sicherheit wird durch sichere Auswahlverfahren in der Zugangskontrolleinheit 4 bzw. in dem Bediengerät 11 erzielt. Die Betriebsartenwahl ist konfigurierbar und kann so von einem Anwender vorgegeben werden.

Bezugszeichenliste

[0059]

- | | |
|---------|--------------------------|
| (1) | Zugangssystem |
| (2) | Steuerung |
| (3) | Anlage |
| (4) | Zugangskontrolleinheit |
| (5) | elektronischer Schlüssel |
| (6) | Prozessor |
| (7) | Ausgangsstruktur |
| (8) | Sensoreinheit |
| (9) | Ein-/Ausgabeeinheit |
| (10) | Bussystem |
| (11) | Bediengerät |
| (12) | Busanschluss |
| a | Bereich |
| b1 - bN | Bereiche |

Patentansprüche

1. Zugangssystem (1) zur Kontrolle eines Zugriffs auf eine von einer Steuerung (2) gesteuerten Anlage (3), mit einer Zugangskontrolleinheit (4) und wenigstens einem elektronischen Schlüssel (5), wobei die Zugangskontrolleinheit (4) zum Lesen von in einem elektronischen Schlüssel (5) gespeicherten Schlüsseldaten ausgebildet ist, **dadurch gekennzeichnet, dass** in der Zugangskontrolleinheit (4) Kriterien vorgebar sind, anhand derer die Gültigkeit eines elektronischen Schlüssels (5) anhand der von diesem gelesenen Schlüsseldaten festgestellt wird, und dass bei Erkennung eines gültigen elektronischen Schlüssels (5) die Zugangskontrolleinheit (4) wenigstens ein Signal an die Steuerung (2) sendet.
2. Zugangssystem (1) nach Anspruch 1, **dadurch gekennzeichnet, dass** die Gültigkeit eines elektroni-

- schen Schlüssels (5) anhand einer in einem nicht beschreibbaren Speicher des elektronischen Schlüssels (5) gespeicherten Kennung festgestellt wird.
3. Zugangssystem (1) nach einem der Ansprüche 1 oder 2, **dadurch gekennzeichnet, dass** die Gültigkeit eines elektronischen Schlüssels (5) anhand einer Prüfsumme für im elektronischen Schlüssel (5) gespeicherte Schlüsseldaten festgestellt wird. 5
 4. Zugangssystem (1) nach Anspruch 3, **dadurch gekennzeichnet, dass** der Umfang der Prüfsumme einstellbar ist. 10
 5. Zugangssystem (1) nach einem der Ansprüche 1 bis 4, **dadurch gekennzeichnet, dass** zur Vorgabe von Funktionen der Anlage und/oder als Kriterium für die Gültigkeit eines elektronischen Schlüssels (5) verschiedenartige Schlüsseldaten, die auf diesem elektronischen Schlüssel (5) gespeichert sind, mit einer oder einer Kombination von einstellbaren Logikfunktionen verknüpft sind, wobei eine Logikfunktion, insbesondere ein "UND", ein "ODER", ein "NICHT" oder ein "VERGLEICHEN" ist. 15
 6. Zugangssystem (1) nach Anspruch 5, **dadurch gekennzeichnet, dass** verschiedenartige Schlüsseldaten auf unterschiedlichen Bereichen eines beschreibbaren Speichers eines elektronischen Schlüssels (5) gespeichert sind. 20
 7. Zugangssystem (1) nach einem der Ansprüche 5 oder 6, **dadurch gekennzeichnet, dass** mehrere Logikfunktionen zu einer Logikbedingung zusammengefasst sind, wobei die Logikbedingung ein Kriterium für die Gültigkeit eines elektronischen Schlüssels (5) ist, und/oder durch die Logikbedingung Funktionen der Anlage vorgegeben sind. 25
 8. Zugangssystem (1) nach Anspruch 7, **dadurch gekennzeichnet, dass** in der Logikbedingung Logikfunktionen mit Klammern gruppiert sind. 30
 9. Zugangssystem (1) nach einem der Ansprüche 1 bis 8, **dadurch gekennzeichnet, dass** das an die Steuerung (2) ausgegebene Signal ein EIN-Signal zur Freigabe von Funktionen der Anlage (3) ist. 35
 10. Zugangssystem (1) nach einem der Ansprüche 1 bis 9, **dadurch gekennzeichnet, dass** mit einem an die Steuerung (2) gesendeten Signal eine Betriebsart der Anlage (3) ausgewählt wird. 40
 11. Zugangssystem (1) nach einem der Ansprüche 1 bis 10, **dadurch gekennzeichnet, dass** dieses eine fehlersichere Funktionalität im Sinne der Maschinensicherheit aufweist. 45
 12. Zugangssystem (1) nach einem der Ansprüche 1 bis 11, **dadurch gekennzeichnet, dass** in einem elektronischen Schlüssel (5) als Schlüsseldaten eine Berechtigung für eine Betriebsartenwahl der Anlage (3) gespeichert ist. 50
 13. Zugangssystem (1) nach Anspruch 12, **dadurch gekennzeichnet, dass** für eine Betriebsartenwahl die Zugangskontrolleinheit (4) über ein Bussystem (10) mit einem Bediengerät (11) verbunden ist, dass die Zugangskontrolleinheit (4) nach Lesen einer Berechtigung für eine Betriebsartenwahl in einem elektronischen Schlüssel (5) eine Anforderung an das Bediengerät (11) sendet, worauf das Bediengerät (11) eine ausgewählte Betriebsart an die Zugangskontrolleinheit (4) sendet, welche als Signal an die Steuerung (2) weitergegeben wird. 55
 14. Zugangssystem (1) nach Anspruch 13, **dadurch gekennzeichnet, dass** die Möglichkeit zur Betriebsartenwahl konfigurierbar ist.
 15. Verfahren zur Kontrolle eines Zugriffs auf eine von einer Steuerung (2) gesteuerten Anlage (3) mittels eines Zugangssystems (1) mit einer Zugangskontrolleinheit (4) und wenigstens einem elektronischen Schlüssel (5), wobei die Zugangskontrolleinheit (4) zum Lesen von in einem elektronischen Schlüssel (5) gespeicherten Schlüsseldaten ausgebildet ist, **dadurch gekennzeichnet, dass** in der Zugangskontrolleinheit (4) Kriterien vorgebar sind, anhand derer die Gültigkeit eines elektronischen Schlüssels anhand der von diesem gelesenen Schlüsseldaten festgestellt wird, und dass bei Erkennung eines gültigen elektronischen Schlüssels (5) die Zugangskontrolleinheit (4) wenigstens ein Signal an die Steuerung (2) sendet.

Fig. 1

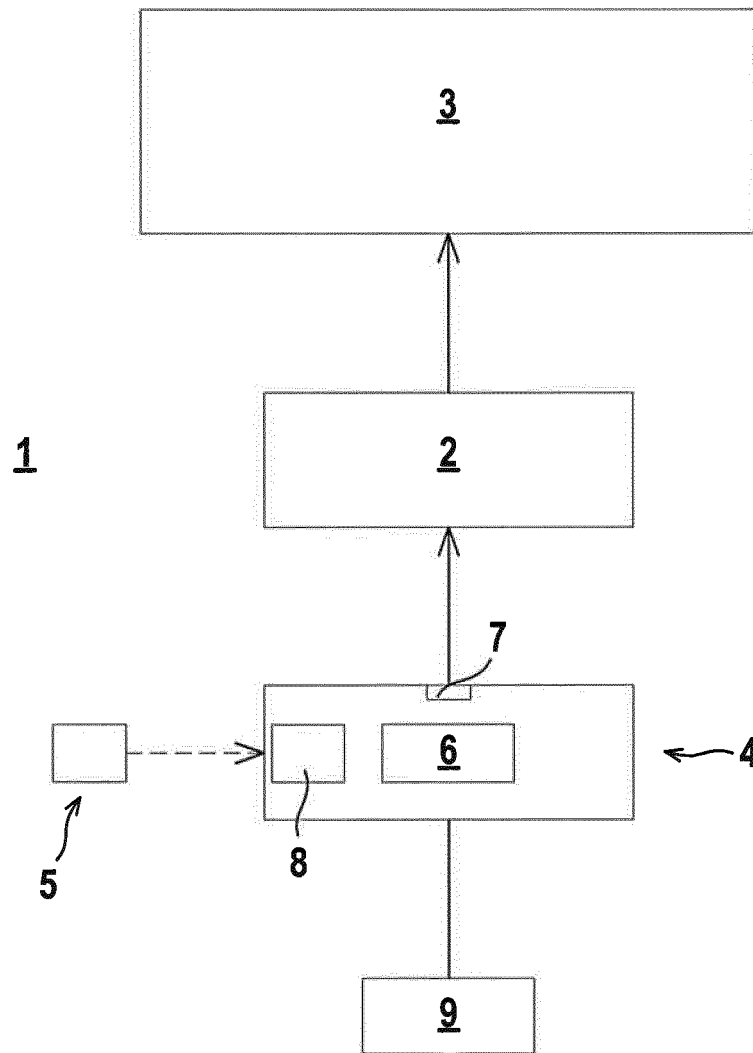


Fig. 2

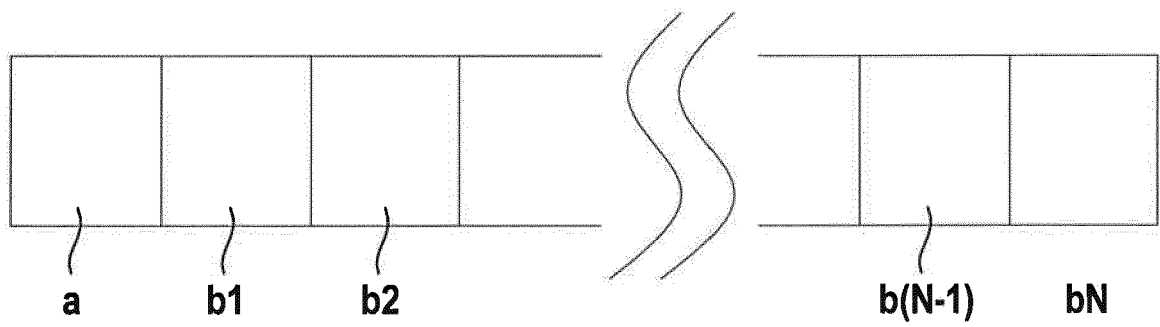
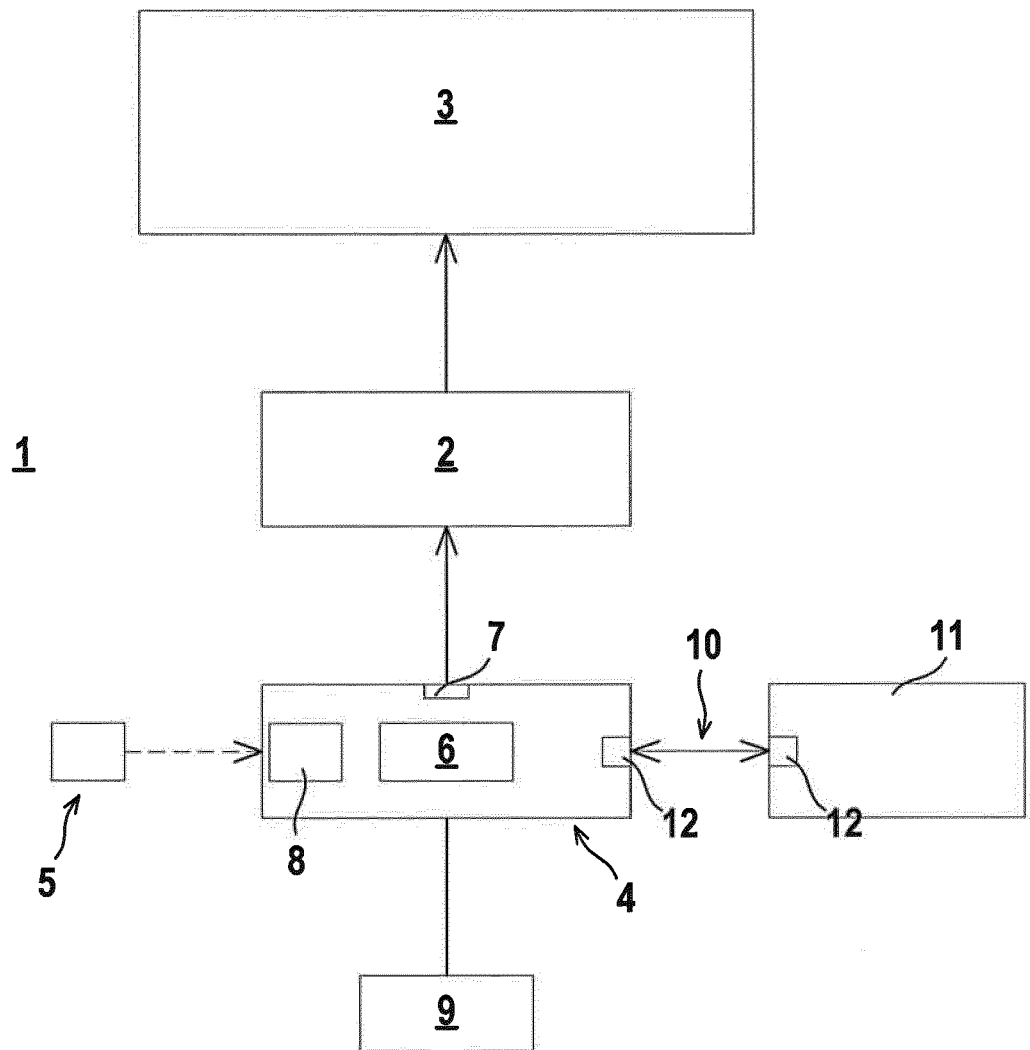


Fig. 3





EUROPÄISCHER RECHERCHENBERICHT

 Nummer der Anmeldung
EP 18 18 6555

5

10

15

20

25

30

35

40

45

50

55

EINSCHLÄGIGE DOKUMENTE			
Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (IPC)
X	EP 0 699 617 A1 (INVENTIO AG [CH]) 6. März 1996 (1996-03-06)	1-10,12,15	INV. G07C9/00
Y	* Zusammenfassung; Abbildung 1 * * Spalte 1, Zeile 53 - Spalte 2, Zeile 2 * * Spalte 2, Zeile 26 - Spalte 4, Zeile 27 *	13,14	
X	GB 2 352 057 A (ADDAPAC LTD [GB]) 17. Januar 2001 (2001-01-17) * Zusammenfassung; Abbildungen * * Seite 1, Absatz 3 * * Seite 3, Zeile 7 - Seite 4, Zeile 24 *	1-8,10-12,15	
X	US 2007/252675 A1 (LAMAR DAVID [US]) 1. November 2007 (2007-11-01) * Zusammenfassung; Abbildungen 1,2 * * Absätze [0031], [0032], [0035], [0038] *	1-9,11,15	
X	DE 101 52 349 A1 (SIEMENS AG [DE]) 15. Mai 2003 (2003-05-15) * Absatz [0006]; Abbildung 1 * * Absätze [0012], [0014], [0017], [0025], [0026] *	1,5-8,10-12,15	RECHERCHIERTE SACHGEBIETE (IPC)
Y	WO 2012/016847 A1 (KAERCHER GMBH & CO KG ALFRED [DE]; TROFF GILLES [DE]; STADELMANN FRANK) 9. Februar 2012 (2012-02-09) * Zusammenfassung; Ansprüche 1,12-15; Abbildungen *	13,14	G07C
A	EP 2 595 341 A1 (SAUTER SVEN [LI]) 22. Mai 2013 (2013-05-22) * Anspruch 1 *	3,4	
Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt			
Recherchenort Den Haag		Abschlußdatum der Recherche 1. Februar 2019	Prüfer Buron, Emmanuel
KATEGORIE DER GENANNTEN DOKUMENTE X : von besonderer Bedeutung allein betrachtet Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie A : technologischer Hintergrund O : mündliche Offenbarung P : Zwischenliteratur		T : der Erfindung zugrunde liegende Theorien oder Grundsätze E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist D : in der Anmeldung angeführtes Dokument L : aus anderen Gründen angeführtes Dokument & : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument	

EPO FORM 1503 03.82 (P04C03)

**ANHANG ZUM EUROPÄISCHEN RECHERCHENBERICHT
ÜBER DIE EUROPÄISCHE PATENTANMELDUNG NR.**

EP 18 18 6555

5 In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten europäischen Recherchenbericht angeführten Patentdokumente angegeben.
Die Angaben über die Familienmitglieder entsprechen dem Stand der Datei des Europäischen Patentamts am
Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

01-02-2019

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 0699617 A1	06-03-1996	AT 193273 T	15-06-2000
		CA 2156339 A1	01-03-1996
		CH 693065 A5	14-02-2003
		CN 1129667 A	28-08-1996
		DE 59508377 D1	29-06-2000
		EP 0699617 A1	06-03-1996
		ES 2148383 T3	16-10-2000
		FI 954023 A	02-03-1996
		HK 1011332 A1	27-10-2000
		JP H0881143 A	26-03-1996
		JP 2006111455 A	27-04-2006
		US 5689094 A	18-11-1997
		ZA 9506075 B	27-02-1996

GB 2352057 A	17-01-2001	KEINE	

US 2007252675 A1	01-11-2007	US 2006071753 A1	06-04-2006
		US 2007252675 A1	01-11-2007
		WO 2006036481 A2	06-04-2006

DE 10152349 A1	15-05-2003	DE 10152349 A1	15-05-2003
		EP 1444659 A2	11-08-2004
		US 2004246095 A1	09-12-2004
		WO 03038764 A2	08-05-2003

WO 2012016847 A1	09-02-2012	CN 103025223 A	03-04-2013
		DE 102010038420 A1	26-01-2012
		DE 202011110517 U1	05-06-2014
		DK 2598013 T3	31-07-2017
		EP 2598013 A1	05-06-2013
		RU 2013108174 A	10-09-2014
		US 2013141211 A1	06-06-2013
		WO 2012016847 A1	09-02-2012

EP 2595341 A1	22-05-2013	CH 705781 A1	31-05-2013
		DK 2595341 T3	03-11-2014
		EP 2595341 A1	22-05-2013

EPO FORM P0461

Für nähere Einzelheiten zu diesem Anhang : siehe Amtsblatt des Europäischen Patentamts, Nr.12/82

IN DER BESCHREIBUNG AUFGEFÜHRTE DOKUMENTE

Diese Liste der vom Anmelder aufgeführten Dokumente wurde ausschließlich zur Information des Lesers aufgenommen und ist nicht Bestandteil des europäischen Patentdokumentes. Sie wurde mit größter Sorgfalt zusammengestellt; das EPA übernimmt jedoch keinerlei Haftung für etwaige Fehler oder Auslassungen.

In der Beschreibung aufgeführte Patentdokumente

- DE 102015114717 A1 [0012] [0039] [0058]