(19) Deutsches Patent- und Markenamt

(10) **DE 10 2020 112 811 B3** 2021.10.21

(12) # Patentschrift

(21) Aktenzeichen: **10 2020 112 811.8**
(22) Anmeldetag: **12.05.2020**
(43) Offenlegungstag: **–**
(45) Veröffentlichungstag der Patenterteilung: **21.10.2021**

(51) Int Cl.: ***H04L 9/32*** (2006.01)
G05B 9/02 (2006.01)
G05B 23/02 (2006.01)

Innerhalb von neun Monaten nach Veröffentlichung der Patenterteilung kann nach § 59 Patentgesetz gegen das Patent Einspruch erhoben werden. Der Einspruch ist schriftlich zu erklären und zu begründen. Innerhalb der Einspruchsfrist ist eine Einspruchsgebühr in Höhe von 200 Euro zu entrichten (§ 6 Patentkostengesetz in Verbindung mit der Anlage zu § 2 Abs. 1 Patentkostengesetz).

(73) Patentinhaber:
ebm-papst Mulfingen GmbH & Co. KG, 74673 Mulfingen, DE

(74) Vertreter:
Rüger Abel Patentanwälte PartGmbB, 73728 Esslingen, DE

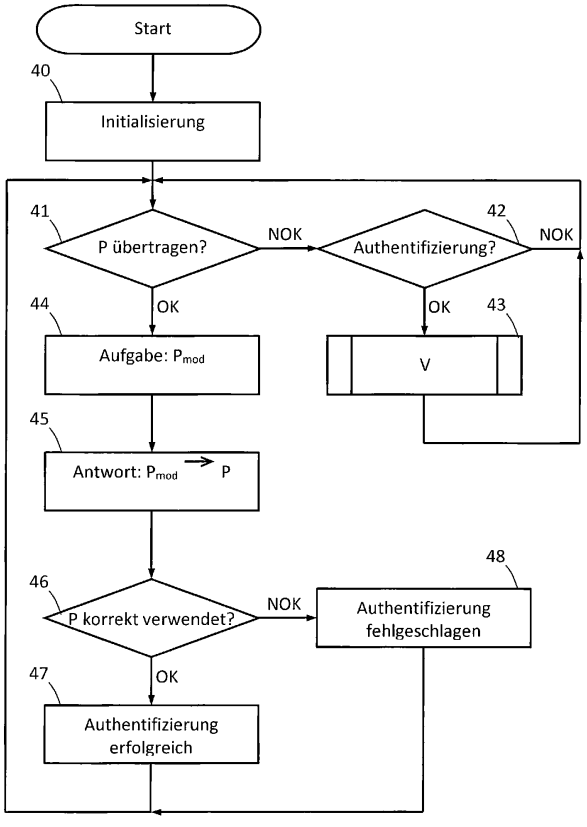
(72) Erfinder:
Humm, Markus, 74679 Weißbach, DE

(56) Ermittelter Stand der Technik:

DE	**101 08 233**	**A1**
DE	**103 44 088**	**A1**
DE	**103 52 071**	**A1**
DE	**195 45 645**	**A1**
DE	**10 2012 109 227**	**A1**

(54) Bezeichnung: **Verfahren und Anlage zur Authentifizierung wenigstens eines Aggregats**

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren zur Authentifizierung eines Aggregats (12) einer Anlage (10). Die Anlage (10) weist eine zentrale Steuerung (11) auf, die mit einem oder mehreren Aggregaten (12) in Kommunikationsverbindung steht. Zur Prüfung der Authentizität eines Aggregats (12) steht wenigstens ein Aufgabe-Antwort-Algorithmus zur Verfügung. Wenn mehrere Aufgabe-Antwort-Algorithmen zur Verfügung stehen, beruht wenigstens ein Aufgabe-Antwort-Algorithmus auf der Verwendung eines Betriebsparameters. Bei dem Betriebsparameter kann es sich beispielsweise um einen von der zentralen Steuerung (11) zu übertragenden Steuer- oder Regelparameter (P) handeln oder um einen in aktuellen Betriebszustand des Aggregats (12) beschreibenden Istwert. Dabei kann die Aufgabe oder die Antwort auf dem Betriebsparameter beruhen. Bei einer bevorzugten Ausführungsform wird ein in dem ausgewählten Aggregat (12) einzustellender Steuer- oder Regelparameter (P), beispielsweise ein Sollwert, modifiziert und als modifizierter Parameter (P_{mod}) an das ausgewählte Aggregat (12) übertragen. Anschließend wird überprüft, ob das ausgewählte Aggregat (12) in der Lage ist, den modifizierten Parameter (P_{mod}) korrekt in den Steuer- oder Regelparameter (P) umzurechnen und daraufhin den Betrieb unter Verwendung des ermittelten Steuer- oder Regelparameters (P) anzupassen. Ist dies der Fall, ist die Authentifizierung des Aggregats (12) erfolgreich.



Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zur Authentifizierung wenigstens eines Aggregats einer Anlage, wobei die Anlage zusätzlich zu dem wenigstens einen Aggregat außerdem eine zentrale Steuerung aufweist, die mit dem wenigstens einen Aggregat kommunikationsverbunden ist. Das Aggregat kann beispielsweise dazu eingerichtet sein, eine Fluidströmung zu erzeugen. Bei dem wenigstens einen Aggregat kann es sich beispielsweise um einen Ventilator oder eine Pumpe handeln. Die Anlage kann auch Aggregate unterschiedlichen Typs aufweisen, beispielsweise wenigstens eine Pumpe und wenigstens einen Ventilator.

[0002] Für den Betrieb solcher Anlagen ist es wichtig, dass die einzelnen Komponenten korrekt zusammenarbeiten. Wenn die zentrale Steuerung mit dem wenigstens einen Aggregat kommuniziert, muss sichergestellt werden, dass die übermittelten Daten vom jeweiligen Empfänger korrekt empfangen und interpretiert werden. Nur dann kann ein korrekter Betrieb der Anlage sichergestellt werden. Wenn beispielsweise Ventilatoren oder Pumpen dazu vorgesehen sind, gasförmige oder flüssige Kühlmedien zu fördern und eine Kühlströmung zu erzeugen, kann ein fehlerhafter Betrieb dazu führen, dass Einrichtungen nicht ausreichend gekühlt werden und einem erhöhten Verschleiß unterworfen sind bzw. ausfallen. Es ist daher wichtig, dass die Kompatibilität der zentralen Steuerung und der Aggregate sichergestellt ist. Die vorliegende Erfindung verwendet deshalb eine Methode zur Authentifizierung basierend auf einer Kommunikation zwischen der zentralen Steuerung und dem wenigstens einen Aggregat.

[0003] Aus dem Stand der Technik sind Authentifizierungsmethoden bekannt.

[0004] EP 0 995 288 B1 betrifft ein Verfahren zur gegenseitigen Authentifizierung zwischen einer Mobilkomponente und einem Netz. Dabei wird auf das sogenannte „Challenge-Response-Verfahren“ zurückgegriffen. Um Zeitverzögerungen zu vermeiden, wird die vom Netz gestellte erste Aufgabe von der Mobileinheit beantwortet und dabei gleichzeitig eine weitere Aufgabe an das Netz übermittelt, die dann wiederum vom Netz beantwortet werden kann.

[0005] Ein Authentifizierungsverfahren mittels des Challenge-Response-Verfahrens ist auch in EP 1 397 886 B1 beschrieben. Bei der beschrienen Anwendung wird eine Chipkarte gegenüber einem Terminal authentifiziert. Zur Erhöhung der Sicherheit wird eine Variabilität der Daten erzeugt, wobei der Datenaustausch während des Authentifikationsverfahrens von historischen Daten abhängt, nämlich einem vorhergehenden Authentifizierungsvorgang.

[0006] Beim dem Authentifizierungsverfahren gemäß DE 10 2017 212 809 B3 werden zwei separate Kommunikationsverbindung zwischen Datenverarbeitungseinrichtungen verwendet, wobei Nutzdaten über die erste Kommunikationsverbindung übertragen werden und Authentifizierungsanfragen über die zweite Kommunikationsverbindung. Zur Authentifizierung kann ein Challenge-Response-Verfahren eingesetzt werden, bei dem Nutzdaten in Blöcke unterteilt werden und auf Basis eines Blocks eine Anfrage zur Authentifizierung erzeugt wird.

[0007] EP 3 340 213 A1 beschreibt eine Sicherheitsfunktion zur Kennzeichnungen von Produkten. Die Markierung enthält eine sogenannte „Physical Unclonable Function (PUF)“, die manchmal auch als „Physical Random Function“ bezeichnet wird. Außerdem enthält die Markierung eine Darstellung einer digitalen Signatur oder eines Verweises darauf. Über die digitale Signatur wird ein Hash-Wert signiert, der aus der Anwendung einer vorherbestimmten Hash-Funktion auf Daten resultiert, die auf Basis der PUF eine Antwort auf eine Aufgabe in einem Authentifizierungsverfahren darstellen (Challenge-Response-Verfahren). Durch die PUF wird bereits eine gewisse Sicherheit erreicht. Um die Echtheit des gekennzeichneten Objekts zur verifizieren, wird eine Aufgabe an die PUF gestellt und aus der Antwort unter Verwendung der Hash-Funktion ein Hash-Wert erzeugt. Dieser Hash-Wert wird dann mit dem in der digitalen Signatur enthaltenen Hash-Wert verglichen. Ein ähnliches Verfahren ist auch in EP 3 565 179 A1 beschrieben.

[0008] Ein Verfahren zur Authentifizierung von Brennstoffkartuschen ist aus WO 2008/021101 A1 bekannt. Über eine Einrichtung, an die die Brennstoffkartusche angeschlossen wird, wird zunächst die Brennstoffkartusche authentifiziert, bevor es ermöglicht wird, Brennstoff von der Brennstoffkartusche in das System einzuleiten. Hierzu kann beispielsweise das Challenge-Response-Verfahren zur Authentifizierung verwendet werden.

[0009] Bei den Verfahren nach WO 2015/030818 A1 geht es um die Authentifizierung einer Tonerkartusche in einem Drucker. Zur Authentifizierung wird das Zeitverhalten berücksichtigt. Der Drucker stellt eine Aufgabe an die Tonerkartusche und überwacht nicht nur die Korrektheit der Antwort, sondern auch den Zeitpunkt der Antwort im Hinblick auf das Erfüllen eines vorgegebenen Zeitfensters, in dem die Antwort erwartet wird. Wenn zumindest eine der beiden Anforderungen nicht erfüllt ist, ist die Authentifizierung fehlgeschlagen.

[0010] US 2004/0223011 A1 und WO 2004/102310 A2 betreffen das Authentifizieren einer Verbrauchseinheit in einem Gerät, beispielsweise einer Kartusche in einem Drucker. Die

Verbrauchseinheit hat einen Authentifizierungscode. Dieser wird mit einem Prüfcode verglichen, um die Authentizität der Versorgungseinheit festzustellen. Dabei kann ein HMAC-Algorithmus (Hash-Massage Authentication Code) verwendet werden.

[0011] Ein weiteres Authentifizierungssystem bzw. Verfahren ist in WO 2013/048430 A1 beschrieben. Es geht darum, eine nachfüllbare Einheit (Tonerkartusche) in einem Gerät (Drucker) zu authentifizieren. Hierzu werden analoge Seriennummern verwendet, die die austauschbaren Einheiten eindeutig kennzeichnen. Die analoge Seriennummer enthält einen besonderen physikalischen Parameter des Chips auf dem sie gespeichert ist. Dieser physikalische Parameter wird digital codiert. Beim Betrieb wird der physikalische Parameter gemessen und mit dem gespeicherten Wert verglichen, um die Einheit zu authentifizieren.

[0012] Aus EP 3 297 834 B1 ist das Authentifizieren eines austauschbaren Gegenstands (Druckerkartusche in einem Drucker) bekannt. Dabei wird überprüft, wie viele und welche Authentifizierungswerte bereits vom austauschbaren Gegenstand an das System übermittelt wurden. Ist eine maximale Anzahl erreicht, werden keine weiteren abgespeicherten Authentifizierungswerte verwendet, sondern nur auf die zuvor bereits übermittelten Authentifizierungswerte zurückgegriffen. Eine ähnliche Vorgehensweise ist auch in EP 3 338 143 B1 beschrieben.

[0013] WO 2013/062528 A1 beschreibt das Authentifizieren einer austauschbaren Versorgungseinheit für einen Drucker. Hierzu kann ein Aufgabencode im Drucker erzeugt und an die austauschbare Versorgungseinheit übermittelt werden. Diese erzeugt eine Antwort. Die Antwort kann zusätzliche Informationen aufweisen, wie etwa das Modell der austauschbaren Versorgungseinheit, eine Lebensdauerangabe, eine Seriennummer oder ein Herstellungsdatum. Basierend auf der Antwort kann der Drucker die Authentizität der austauschbaren Versorgungseinheit prüfen.

[0014] Aus EP 2 605 175 A2 ist bekannt, eine austauschbare Einheit (Field Replaceable Unit) zu prüfen. Die austauschbare Einheit weist eine Kennzeichnung auf, die mit einer in einem Sicherheitsmodul gespeicherten Kennzeichnung verglichen wird. Die Kennzeichnung kann die Topologie eines Schlüsselchips beinhalten.

[0015] Bei dem aus US 2005/0050325 A1 bekannten Authentifizierungssystem erzeugt eine Authentifizierungseinrichtung eines ersten Geräts ein Signal, das an ein weiteres Gerät gesendet wird. Dieses antwortet wiederum mit einem Signal. Die beiden Signale werden miteinander verglichen. Durch den Vergleich der Signale kann die Identität des am ersten Gerät angeschlossenen weiteren Geräts geprüft werden.

[0016] Ein Verfahren zur kontaktlosen Authentifizierung einer Smartcard ist aus US 2010/0224682 A1 bekannt. Ein Lesegerät misst eine Impulsantwort, die mit der Smartcard verknüpft ist. Die Impulsantwort wird mit Referenzdaten verglichen. Optional kann das Lesegerät außerdem wenigstens eine Aufgabe an die Smartcard übermitteln und deren Antwort verifizieren.

[0017] WO 2006/052111 A1 betrifft ein Verfahren zur Übertragungsverschlüsselung zwischen Knoten. Dabei geht es im Kern um die Verwaltung der verwendeten Schlüssel. Es wird vorgeschlagen, eine unverzweigte Kette mit Schlüsseln zu erzeugen und die Schlüssel entsprechend der unverzweigten Struktur der Kette auf die Knoten zu verteilen.

[0018] Das Authentifikationsverfahren aus EP 3 511 854 A1 verwendet einen zweiten Schaltkreis zur Authentifizierung eines ersten Schaltkreises. In jedem Schaltkreis wird eine Signatur unter Berücksichtigung der jeweiligen elektrischen Knoten erzeugt.

[0019] DE 10 2012 109 227 A1 beschreibt eine Anordnung mit wenigstens einem Feldgerät, das mit einer Leitwarte kommunikationsverbunden ist. Zusätzlich ist eine mobile Rechnereinheit vorhanden, die drahtlos mit dem Feldgerät und der Leitwarte kommunizieren kann. Die Datenkommunikation zwischen der Leitwarte und dem Feldgerät kann zusätzlich über die mobile Rechnereinheit übertragen werden, so dass durch diese Redundanz ein Abgleich stattfinden kann. Somit lassen sich Übertragungsfehler erkennen. Die Signalübertragung kann verschlüsselt erfolgen.

[0020] Eine Funktionsprüfvorrichtung für ein Feldgerät und ein entsprechendes Verfahren sind aus DE 103 44 088 A1 bekannt. Dazu können beispielsweise regelmäßig Stellsignale an Feldgeräte übertragen werden, um deren korrekte Funktion zu prüfen und zu überwachen.

[0021] DE 103 52 071 A1 beschreibt ein Verfahren zur Erkennung von unberechtigt ausgetauschten Komponenten. Eine verschlüsselte Nachricht wird an eine zu prüfende Komponente übermittelt. Die Nachricht enthält einen Wert, der mittels eines Zufallsgenerators oder eines zufällig anliegenden Sensorsignals erzeugt wird. Die Nachricht wird in der zu prüfenden Komponente gelesen und über eine vorgegebene Zuordnung eine Kennung ermittelt und zurück übertragen. Die Zuordnung ist dem Steuergerät bekannt und es kann dann geprüft werden, ob die korrekte Kennung von der zu prüfenden Komponente als Antwort auf die verschlüsselte Nachricht übermittelt wurde.

[0022] Ausgehend vom Stand der Technik kann es als Aufgabe der vorliegenden Erfindung angesehen werden, eine einfache Möglichkeit der Authentifizierung zu schaffen.

[0023] Diese Aufgabe wird durch ein Verfahren mit den Merkmalen des Patentanspruches 1 sowie eine Anlage mit den Merkmalen des Patentanspruches **11** gelöst.

[0024] Bei der Erfindung geht es um die Authentifizierung wenigstens eines Aggregats, das Bestandteil einer Anlage ist. Das wenigstens eine Aggregat kann ein Kühlaggregat sein. Vorzugsweise sind mehrere Aggregate vorhanden, die mit einer gemeinsamen zentralen Steuerung kommunikationsverbunden sind. Die Kommunikationsverbindung kann drahtlos und/oder drahtgebunden erfolgen. Vorzugsweise sind die zentrale Steuerung und das wenigstens eine Aggregat über ein Bussystem kommunikationsverbunden.

[0025] Das Authentifizierungsverfahren wird beispielsweise gestartet, wenn eine Prüfbedingung zur Überprüfung der Authentizität eines Aggregats erfüllt ist. Die Prüfbedingung kann beispielweise das Erreichen eines zufällig ausgewählten Zeitpunkts sein. Die Prüfbedingung kann auch erfüllt sein, wenn eine Kommunikation zur Steuerung oder Regelung zwischen der zentralen Steuerung und dem Aggregat, das authentifiziert werden soll, ohnehin erforderlich ist oder entsprechend den Vorgaben eines verwendeten Kommunikationsprotokolls stattfindet.

[0026] Es wird zunächst ein zu authentifizierendes Aggregat ausgewählt. Im Anschluss daran wird ein Betriebsparameter erfasst oder ermittelt, der dann verwendet wird, um die Authentizität zu prüfen. Dazu wird ein Aufgabe-Antwort-Algorithmus eingesetzt, bei dem basierend auf dem Betriebsparameter die Aufgabe und/oder die Antwort generiert wird.

[0027] Bei einem Ausführungsbeispiel des Verfahrens kann die zentrale Steuerung einen Istwert des ausgewählten Aggregats abfragen, wie beispielsweise eine Isttemperatur und/oder eine Istdrehzahl eines Motors des Aggregats und/oder einen Iststrom eines Elektromotors des Aggregats, usw. Als Betriebsparameter kann wenigstens ein beliebiger Sensorwert und/oder Zählerstand verwendet werden, der den aktuellen Betriebszustand des Aggregats charakterisiert, beispielsweise auch der Stand eines Betriebsstundenzählers des ausgewählten Aggregats.

[0028] Die Anfrage der zentralen Steuerung zur Übermittlung des Betriebsparameters und/oder das Auslesen des Betriebsparameters kann bereits als Aufgabe bei dem ausgewählten Aggregat verstanden werden. Alternativ dazu ist es auch möglich, dass die zentrale Steuerung eine Nachricht an das ausgewählte Aggregat übermittelt, die eine Aufgabe zur Authentifizierung darstellt.

[0029] Das ausgewählte Aggregat kann daraufhin eine vorgegebene Rechenoperation basierend auf dem Betriebsparameter ausführen. Die Rechenoperation kann durch wenigstens eine oder mehrere mathematische und/oder logische Operationen gebildet sein. Die Rechenoperation ist sowohl dem Aggregat, als auch der zentralen Steuerung bekannt. Das Ergebnis der Rechenoperation wird als Antwort auf die Aufgabe für die zentrale Steuerung bereitgestellt. Die zentrale Steuerung kann die Antwort aus einem Register des ausgewählten Aggregats auslesen oder das ausgewählte Aggregat kann die Antwort an die zentrale Steuerung übertragen.

[0030] In der zentralen Steuerung kann dieselbe Rechenoperation auf den bereits bekannten Betriebsparameter angewandt werden und überprüft werden, ob das Ergebnis mit der Antwort des ausgewählten Aggregats übereinstimmt. Ist die Antwort des ausgewählten Aggregats auf die empfangene Aufgabe korrekt, wird die Authentizität des ausgewählten Aggregats festgestellt. Andernfalls war die Authentizitätsprüfung des ausgewählten Aggregats nicht erfolgreich und es können Maßnahmen eingeleitet werden, beispielsweise das Stillsetzen des Aggregats.

[0031] Wenn in dieser Anmeldung von einer Rechenoperation gesprochen wird, ist darunter wenigstens eine mathematische Operation und/oder wenigstens eine logische Operation zu verstehen, die einen Wert verschlüsselt, wobei der Wert dabei mit wenigstens einem weiteren Wert verknüpft werden kann. Die Werte sind vorzugsweise binäre Zahlen beliebiger Länge, beispielsweise mindestens 8 bit. Hierbei können sämtliche in der Kryptologie verwendeten Rechenoperationen eingesetzt werden. In einem sehr einfachen Beispiel können beispielsweise zwei binäre Werte bitweise unter Verwendung einer XOR-Operation (logische exklusive ODER-Verknüpfung) miteinander kombiniert werden, um die Aufgabe und/oder die Antwort zu ermitteln.

[0032] Bei der vorstehenden Variante beruht die Antwort des ausgewählten Aggregats auf dem Betriebsparameter, also beispielsweise einem Istwert des Betriebs des ausgewählten Aggregats. Da es zwischen dem Erfassen des Istwertes durch die zentrale Steuerung und dem Übermitteln oder Auslesen der Antwort zu einer Zeitverzögerung kommen kann, in der sich der Betriebsparameter ändern kann, kann es notwendig sein, das Aufgabe-Antwort-Verfahren mehrfach durchzuführen, um die Authentizität des ausgewählten Aggregats bestätigen oder verneinen zu können. Beispielsweise kann das Aufgabe-Antwort-Verfahren mehrfach (ungerade Anzahl) ausgeführt und anschließend eine Mehrheitsentscheidung getroffen

werden, um die Authentizität des ausgewählten Aggregats zu bestätigen oder abzulehnen.

[0033] Bei einem zusätzlichen oder alternativen Aufgabe-Antwort-Algorithmus des erfindungsgemäßen Verfahrens kann der Betriebsparameter ein Steuerparameter oder Regelparameter für das ausgewählte Aggregat sein. Beispielsweise kann als Steuerparameter oder Regelparameter ein Sollwert und/oder ein Grenzwert und/oder ein in einer Steuerfunktion oder Regelfunktion des Aggregats zu verwendender Parameter an das ausgewählte Aggregat übermittelt werden. Bei dieser Variante wird der Betriebsparameter analog zu der vorstehend beschriebenen Variante durch eine der zentralen Steuerung und dem Aggregat bekannte Rechenoperation verändert. Er kann dabei mit einem oder mehreren sowohl in der zentralen Steuerung als auch im ausgewählten Aggregat bekannten Werten verknüpft werden. Durch diese mathematische und/oder logische Rechenoperation wird eine Aufgabe erzeugt, die von der zentralen Steuerung an das ausgewählte Aggregat übermittelt wird. Als Antwort auf die empfangene Aufgabe berechnet das ausgewählte Aggregat den in der Aufgabe enthaltenen Betriebsparameter und verwendet diesen Betriebsparameter anschließend für den weiteren Betrieb.

[0034] Die zentrale Steuerung kann dann überprüfen, ob der in der Aufgabe enthaltene Betriebsparameter korrekt im ausgewählten Aggregat verwendet wird. Hierzu können beispielsweise ein oder mehrere Istwerte abgefragt oder ausgelesen werden, die den aktuellen Betrieb des ausgewählten Aggregats charakterisieren. Das decodieren der Aufgabe das Verwenden des ermittelten Betriebsparameters für den weiteren Betrieb des ausgewählten Aggregats stellt in diesem Fall die Antwort auf die empfangene Aufgabe dar. Wurde die Aufgabe vom ausgewählten Aggregat korrekt umgesetzt, wird die Authentizität bestätigt und andernfalls abgelehnt.

[0035] Bei allen erfindungsgemäßen Varianten der Verfahrens ist zumindest ein Aufgabe-Antwort-Algorithmus auswählbar und einsetzbar, bei dem ein Betriebsparameter (zum Beispiel Sollwert, Istwert, Steuerparameter, Regelparameter) zur Erzeugung der Aufgabe und/oder zur Erzeugung der Antwort auf die Aufgabe verwendet wird. Das Übermitteln des Betriebsparameters zwischen der zentralen Steuerung und dem ausgewählten Aggregat ist ohnehin während des Betriebs der Anlage erforderlich oder vorteilhaft, beispielsweise um die zentrale Steuerung über aktuelle Betriebszustände der Aggregate zu informieren oder um durch die zentrale Steuerung den Betrieb eines Aggregats anzupassen, beispielweise an veränderte Umgebungsbedingungen. Diese Kommunikation kann gleichzeitig zur Authentifizierung verwendet werden. Die für die Authentifizierung erforderliche zusätzliche Kommunikation zwischen der zentralen Steuerung und dem wenigstens einen Aggregat kann reduziert und die erforderliche Bandbreite minimiert werden. Das zur Kommunikation verwendete Kommunikationssystem wird weniger stark belastet. Das Authentifizieren der vorhandenen Aggregate erfolgt somit äußerst effizient.

[0036] Vorzugsweise werden alle von der zentralen Steuerung an alle vorhandenen Aggregate der Anlage übermittelten Sollwerte durch wenigstens eine mathematische und/oder logische Rechenoperation in eine Aufgabe umgewandelt und übertragen. Sollwerte werden bei dieser Ausgestaltung des Verfahrens nicht unverschlüsselt kommuniziert. Alternativ dazu können Betriebsparameter nur dann verschlüsselt in Form einer Aufgabe übermittelt werden, wenn eine zusätzliche Prüfbedingung erfüllt ist, die eine Prüfung der Authentizität erfordert.

[0037] Wie erläutert ist es vorteilhaft, wenn das ausgewählte Aggregat den Betriebsparameter aus der empfangenen Aufgabe ermittelt und für den weiteren Betrieb verwendet. Dies stellt eine sehr effiziente Möglichkeit der Authentifizierung dar, da das Übertragen eines solchen Betriebsparameters für die Steuerung oder Regelung des ausgewählten Aggregats ohnehin notwendig ist. Der Betriebsparameter kann beispielsweise ein Sollwert sein, wie etwa die Solldrehzahl eines Elektromotors des ausgewählten Aggregats oder ein Sollstrom eines Elektromotors des Aggregats oder ähnliches.

[0038] Das wenigstens eine Aggregat kann ein Kühlaggregat sein. Das wenigstens eine Aggregat kann zur Erzeugung einer Fluidströmung eingerichtet sein, beispielsweise einer Luftströmung oder einer Kühlmittelströmung. Bei einem Ausführungsbeispiel ist zumindest eines der Aggregate ein Ventilator und/oder eine Pumpe. Die Aggregate einer Anlage können vom selben Typ oder unterschiedlichen Typs sein. Beispielsweise kann eine Anlage ausschließlich durch Ventilatoren oder durch Pumpen gebildete Aggregate aufweisen oder Pumpen und Ventilatoren enthalten.

[0039] Das Überprüfen der Authentizität jedes Aggregats kann einmalig erfolgen, beispielsweise bei der Inbetriebnahme. Zusätzlich oder alternativ kann eine Authentizitätsprüfung eines Aggregats in regelmäßigen oder unregelmäßigen Zeitabständen bzw. immer dann wiederholt werden, wenn eine Prüfbedingung erfüllt ist.

[0040] Die auf dem Betriebsparameter basierte Aufgabe und/oder Antwort kann unter Verwendung eines weiteren Wertes ermittelt werden, der sowohl der zentralen Steuerung als auch dem ausgewählten Aggregat bekannt ist, beispielsweise einem einmalig erzeugten und während des weiteren Betriebs unveränderlichen Wert. Zum Beispiel kann die zentrale

Steuerung bei der Initialisierung jedes Aggregats einen Initialisierungswert vorgeben und an das jeweilige Aggregat übermitteln. Basierend auf dem Initialisierungswert und einer sowohl der zentralen Steuerung als auch dem Aggregat bekannten Rechenoperation kann dann die Aufgabe in der zentralen Steuerung oder die Antwort im ausgewählten Aggregat berechnet werden. Im Anschluss daran kann auf Basis dieser Rechenoperation die Aufgabe im ausgewählten Aggregat gelöst bzw. die Antwort in der zentralen Steuerung geprüft werden.

[0041] Zusätzlich oder alternativ zu dem Initialisierungswert können auch andere Zahlen oder Werte zur Bildung der Aufgabe und/oder der Antwort verwendet werden, z.B. wenigstens einer der folgenden Werte:

- eine von der zentralen Steuerung an das ausgewählte Aggregat übermittelt Zufallszahl;
- eine Seriennummer des ausgewählten Aggregats oder ein Teil davon;
- ein im ausgewählten Aggregat gespeicherter unveränderlicher Registerwert (kann auch als Salt-Wert bezeichnet werden), der auch der zentralen Steuerung bekannt ist.

[0042] Die Anzahl der verwendeten Werte oder Zahlen und die Rechenoperation um einen Wert zu verändern oder mehrere Werte miteinander zu verknüpfen kann beliebig gewählt werden.

[0043] Zur Authentifizierung wird eine Gruppe mehrerer unterschiedlicher Aufgabe-Antwort-Algorithmen bereitgestellt. Ein erster Algorithmus entspricht dabei dem auf dem Betriebsparameter basierten Aufgabe-Antwort-Algorithmus, wie er vorstehend erläutert wurde. Bei diesem ersten Algorithmus beruht die Aufgabe und/oder die Antwort auf einem Betriebsparameter für das ausgewählte Aggregat oder von dem ausgewählten Aggregat. Die Gruppe weist zusätzlich zu dem ersten Algorithmus wenigstens einen weiteren Algorithmus auf. Vor oder nach dem Auswählen eines zu authentifizierenden Aggregats wird einer oder werden mehrere der bereitgestellten Algorithmen ausgewählt, um die Authentifizierung durchzuführen. Dadurch kann die Sicherheit bei der Authentifizierung weiter verbessert werden.

[0044] Ein weiterer Algorithmus aus der Gruppe von Aufgabe-Antwort-Algorithmen kann beispielsweise auf einem Zufallswert basieren, den die zentrale Steuerung ermittelt und dem ausgewählten Aggregat bereitstellt, beispielsweise an das ausgewählte Aggregat übermittelt. Bei einer bevorzugten Ausführungsform weist das ausgewählte Aggregat ein definiertes Register auf, in dem die zentrale Steuerung den Zufallswert einträgt. Das Bereitstellen des Zufallswertes bildet die Aufgabe. Das ausgewählte Aggregat ermittelt basierend auf dem Zufallswert und wenigstens einem weiteren Wert, insbesondere dem Initialisierungswert, eine Antwort, die der zentralen Steuerung bereitgestellt wird. Vorzugsweise wird die Antwort in ein definiertes Register des ausgewählten Aggregats geschrieben und steht dort für den Zugriff durch die zentrale Steuerung bereit. Die zentrale Steuerung kann die Antwort auslesen. Die Antwort kann in der zentralen Steuerung dadurch geprüft werden, dass dieselbe Rechenoperation basierend auf dem Zufallswert und dem wenigstens einen weiteren Wert (z.B. Initialisierungswert) ausgeführt und das Ergebnis mit der Antwort verglichen wird.

[0045] Es ist dabei vorteilhaft, den wenigstens einen weiteren Wert und/oder die zur Berechnung verwendete Rechenoperation in dem wenigstens einen Aggregat bzw. in der zentralen Steuerung vor dem Einbau in die Anlage abzuspeichern. Dadurch kann vermieden werden, dass nachträglich eingebaute und inkompatible Aggregate im Rahmen einer Initialisierung eingebunden werden können.

[0046] Vorteilhafte Ausgestaltungen der Erfindung ergeben sich aus den abhängigen Patentansprüchen, der Beschreibung und den Zeichnungen. Nachfolgend werden bevorzugte Ausführungsbeispiele der Erfindung anhand der beigefügten Zeichnungen erläutert. In den Zeichnungen zeigen:

Fig. 1 eine schematische Darstellung eines Ausführungsbeispiels einer Anlage mit einer zentralen Steuerung und mehreren damit kommunikationsverbundenen Aggregaten,

Fig. 2 ein Blockschaltbild eines Ausführungsbeispiels eines Aggregats aus **Fig. 1**,

Fig. 3 ein Blockschaltbild eines Ausführungsbeispiels eines Registers einer Aggregatsteuerung eines Aggregats aus den **Fig. 1** oder **Fig. 2** und

Fig. 4 bis **Fig. 6** Flussdiagramme unterschiedlicher Ausführungsbeispiele von Verfahren zur Authentifizierung eines Aggregats.

[0047] In **Fig. 1** ist stark schematisiert in Form eines Blockschaltbilds eine Anlage **10** veranschaulicht, die eine zentrale Steuerung **11** sowie mehrere Aggregate **12** aufweist. Die Aggregate **12** und die zentrale Steuerung **11** sind mittels eines Kommunikationssystems **13** kommunikationsverbunden. Das Kommunikationssystem **13** kann dazu eine drahtgebundene oder/oder drahtlose Kommunikationsverbindung herstellen. Beim Ausführungsbeispiel ist das Kommunikationssystem **13** ein Bussystem **14**, das eine drahtgebundene Kommunikationsverbindung zwischen der zentralen Steuerung **11** und den Aggregaten **12** ermöglicht. Das Bussystem **14** beruht beispielsgemäß auf einer Master-Slave-Architektur bzw. Client-Server-Architektur. Die zentrale Steuerung **11** stellt dabei den Master **M** dar. Die Aggregate **12** bilden jeweils einen Slave $\mathbf{S_x}$. Das Bussystem kann ir-

gendeiner bekannten Architektur oder irgendeinem bekannten Standard entsprechen, beispielsweise einem Feldbus-Standard, wie etwa PROFIBUS oder MODBUS.

[0048] Der Index „x“ charakterisiert eine Nummer des Aggregats **12**. Die Anzahl n der Aggregate **12** kann variieren und jedes Aggregat **12** bildet beispielsgemäß einen Slave $\mathbf{S_x}$ mit x = 1 bis n. Der Index „x“ beschreibt beispielhaft, dass der mit dem Index „x“ versehene Parameter oder Wert zu dem SLAVE $\mathbf{S_x}$ gehört.

[0049] Bei den Aggregaten **12** der Anlage **10** handelt es sich beispielsgemäß um Ventilatoren **15**. Eine beispielhafte blockschaltbildähnliche Darstellung eines Ventilators **15** ist in **Fig. 2** veranschaulicht. Zusätzlich oder alternativ kann wenigstens ein Aggregat **12** oder es können mehrere oder alle Aggregate **12** auch durch andere steuerbare Aggregate, insbesondere ein Fluidströmung verursachende Aggregate gebildet sein, beispielsweise durch eine Pumpe.

[0050] Der Ventilator **15** weist eine Aggregatsteuerung **16** auf. Die Aggregatsteuerung **16** ist zur Steuerung oder Regelung eines Elektromotors **17** des Ventilators **15** eingerichtet. Über den Elektromotor **17** kann eine Rotoreinheit **18** des Ventilators **15** zur Erzeugung einer Gasströmung, insbesondere Luftströmung, drehend angetrieben werden. Mittels wenigstens eines Sensors **19** des Ventilators **15** kann ein Betriebszustand des Elektromotors **17** und/oder der Rotoreinheit **18** erfasst und ein entsprechendes Sensorsignal $\mathbf{O_x}$ an die Aggregatsteuerung **16** übermittelt werden. Basierend auf dem wenigstens einen Sensorsignal $\mathbf{O_x}$ kann eine geschlossene Regelschleife implementiert werden.

[0051] Der Ventilator **15** weist eine Schnittstelle **20** auf, mittels der die Verbindung zum Bussystem **14** hergestellt ist. Die Schnittstelle **20** kann Bestandteil der Aggregatsteuerung **16** sein.

[0052] Die Aggregatsteuerung **16** weist außerdem einen Speicher **21** auf, in den Werte temporär und/oder dauerhaft gespeichert werden können. Mehrere Register des Speichers **21** sind schematisch in **Fig. 3** veranschaulicht. Ein Teil der Register kann über Daten oder Werte, die an der Schnittstelle **20** empfangen werden, beschrieben werden. Teile des Registers können mittels der Aggregatsteuerung **16** beschrieben werden und für den Zugriff über das Kommunikationssystem **13** bzw. des Bussystem **14** von extern bereitgestellt werden, insbesondere für den Zugriff durch die zentrale Steuerung **11** (Master **M**).

[0053] Die Anlage **10** und insbesondere die zentrale Steuerung **11** und die Aggregate **12** sind zur Durchführung einer Authentifizierung eingerichtet. Dadurch kann festgestellt werden, ob innerhalb der Anlage **10** ein oder mehrere Aggregate **12** hinzugefügt oder ausgetauscht wurden, die inkompatibel sein können.

[0054] Ein Ausführungsbeispiel eines Verfahrens ist in **Fig. 4** veranschaulicht. Beispielsgemäß wird nach dem Start in einem Schritt **30** bei der ersten Inbetriebnahme der Anlage **10** und/oder eines in die Anlage **10** integrierten Aggregats **12** durch die zentrale Steuerung **11** eine Initialisierung vorgenommen. Dabei wird durch die zentrale Steuerung **11** bei der Inbetriebnahme der Anlage **10** jedem Aggregat **12** ein Initialisierungswert $\mathbf{Init_x}$ zugewiesen und in einem Register des Speichers **21** abgelegt (**Fig. 3**).

[0055] Wenn lediglich ein oder mehrere neue Aggregate **12** in die Anlage **10** integriert werden sollen, kann die zentrale Steuerung **11** entweder allen Aggregaten **12** jeweils einen neuen Initialisierungswert $\mathbf{Init_x}$ vorgeben oder lediglich die neu hinzugefügten Aggregate initialisieren.

[0056] Der Initialisierungswert $\mathbf{Init_x}$ kann beispielsweise eine beliebige Zufallszahl sein. Die Initialisierungswerte der Aggregate **12** sind alle verschieden voneinander. Im Betrieb der Anlage im Anschluss an die Initialisierung ist der Initialisierungswert $\mathbf{Init_x}$ jedes Aggregats **12** (Slave $\mathbf{S_x}$) unveränderlich.

[0057] Zusätzlich oder alternativ zu dieser Vergabe des Initialisierungswerts $\mathbf{Init_x}$ kann ein Register des Speichers **21** die Seriennummer $\mathbf{N_x}$ des jeweiligen Aggregats **12** und/oder einen unveränderlichen Registerwert $\mathbf{F_x}$ aufweisen. Die Seriennummer $\mathbf{N_x}$ und/oder der unveränderliche Registerwert $\mathbf{F_x}$ können bereits vor dem Einbau des Aggregats **12** in die Anlage **10** im Speicher **21** abgespeichert werden. Die Seriennummer $\mathbf{N_x}$ kann im Rahmen der Initialisierung durch die zentrale Steuerung **11** abgefragt werden. Zusätzlich oder alternativ kann der unveränderliche Registerwert $\mathbf{F_x}$ in einem Register abgelegt werden, das der zentralen Steuereinheit **11** bekannt ist und dort zum Auslesen im Rahmen der Initialisierung bereitgestellt werden.

[0058] Der unveränderliche Registerwert $\mathbf{F_x}$ der Aggregate **12** einer Anlage **10** kann alternativ vorzugsweise vor der Inbetriebnahme in der zentralen Steuerung **11** abgespeichert werden. Dadurch kann ein Übertragen des unveränderlichen Registerwerts $\mathbf{F_x}$ über das Kommunikationssystem **13** vermieden werden, beispielsweise bei der Initialisierung. Das Vergeben eine Initialisierungswertes $\mathbf{Init_x}$ und/oder das Austauschen von Werten zwischen der zentralen Steuerung **11** und dem wenigstens einen Aggregat **12** während der Initialisierung als Basis für eine nachfolgende Authentizitätsprüfung ist optional und nicht zwingend erforderlich.

[0059] In der zentralen Steuerung **11** sowie der Aggregatsteuerung **16** kann außerdem eine Rechen-

operation **C** vorgegeben sein. Die Rechenoperation **C** kann aus einer oder mehreren mathematischen und/oder logischen Operationen gebildet werden. Die Rechenoperation **C** ist im Prinzip beliebig wählbar. Bei einigen Ausführungsbeispielen wird die Rechenoperation **C** derart gewählt, dass wenigstens ein Wert, der mittels der Rechenoperation **C** verschlüsselt wird, aus dem Ergebnis der Rechenoperation **C** wieder berechnet werden kann, wenn die Rechenoperation **C** bekannt ist. Bei der Rechenoperation **C** können in der Kryptologie verwendete Operationen eingesetzt werden.

[0060] Nach dem Schritt **30** wird in einem Schritt **31** abgefragt, ob eine Authentifizierung erfolgen soll. Hierfür können eine oder mehrere Prüfbedingungen vorgegeben werden. Wenn keine der Prüfbedingungen erfüllt ist (Verzweigung NOK aus Schritt **31**), wird die Anlage **10** im Schritt **32** in Betrieb genommen oder weiterbetrieben. Wenn eine der Prüfbedingungen erfüllt ist (Verzweigung OK aus dem Schritt **31**) wird das Verfahren im Schritt **33** fortgesetzt. Jede der Prüfbedingungen im Schritt **31** kann zeitabhängig und/oder ereignisabhängig sein und während des Betriebs der Anlage (Schritt **32**) wiederholt geprüft werden (Schleife der Schritte **31**, **32**).

[0061] Eine Prüfbedingung kann beispielsweise sein, dass die Anlage **10** oder wenigstens ein Aggregat **12** im Schritt **30** initialisiert werden soll. Eine andere Prüfbedingung kann beispielsweise sein, dass ein Betriebsparameter von der zentralen Steuerung **11** an ein ausgewähltes Aggregat **12** übermittelt wird, der für den nachfolgenden Betrieb des ausgewählten Aggregats verwendet werden soll. Noch eine andere Prüfbedingung kann sein, dass ein aktueller Betriebsparameter (zum Beispiel ein Istwert) eines ausgewählten Aggregats an die zentrale Steuerung **11** übermittelt wird oder von der zentralen Steuerung **11** angefordert oder eingelesen wird. Eine weitere Prüfbedingung kann eine Zufallsbedingung sein, die durch einen Zufallsgenerator der zentralen Steuerung **11** ausgelöst wird. Nach dem Zufallsprinzip können eine oder mehrere Aggregate **12** zur Prüfung deren Authentizität ausgewählt werden.

[0062] Zu Beginn der Authentifizierung wird eine Aufgabe von der zentralen Steuerung **11** an das zur authentifizierenden ausgewählten Aggregat **12** übermittelt (Schritt **33**). Dabei kann der zentralen Steuerung **11** eine Gruppe **G** mehrerer Aufgabe-Antwort-Algorithmen bereitgestellt werden, aus denen die zentrale Steuerung **11** einen Algorithmus oder mehrere Algorithmen für die Authentifizierung auswählt. Die Aufgabe des wenigstens einen Aufgabe-Antwort-Algorithmus wird anschließend an das ausgewählte Aggregat **12** übermittelt.

[0063] Die Gruppe **G** enthält zumindest einen Aufgabe-Antwort-Algorithmus zur Verfügung, bei dem die Aufgabe und/oder die Antwort auf einem Betriebsparameter des ausgewählten Aggregats **12** basiert. Beispielsweise kann ein Steuerparameter oder Regelparameter P, insbesondere ein Sollwert, mittels der Rechenoperation **C** modifiziert und als modifizierter Parameter Pmod an das ausgewählte Aggregat **12** übermittelt werden, wobei diese Übermittlung die Aufgabe darstellt. Das ausgewählte Aggregat **12** muss als Antwort auf diese Aufgabe den weiteren Betrieb unter Verwendung des Steuer- oder Regelparameters P anpassen. Dies ist nur dann möglich, wenn das ausgewählte Aggregat **12** die Rechenoperation **C** kennt und aus dem modifizierten Parameter Pmod den Steuer- oder Regelparameter P, insbesondere einen Sollwert, ermitteln und für die Steuerung oder Regelung verwenden kann.

[0064] Der Betriebsparameter kann bei einem Aufgabe-Antwort-Algorithmus ein beliebiger aktueller Istwert sein, der den aktuellen Betrieb oder Zustand des Aggregats **12** charakterisiert und von der zentralen Steuerung **11** ausgelesen oder abgefragt wird (Aufgabe). Anschließend kann als Antwort das verschlüsselte Übermitteln **11** des bereits ausgelesenen oder abgefragten Betriebsparameters vom ausgewählten Aggregat **12** an die zentrale Steuerung **11** erfolgen.

[0065] Nachdem das ausgewählte Aggregat **12** die Aufgabe von der zentralen Steuerung **11** empfangen hat, erzeugt das ausgewählte Aggregat **12** eine Antwort (Schritt **34**). Die Antwort ist an die gestellte Aufgabe angepasst. In einem darauffolgenden Schritt **35** wird durch die zentrale Steuerung **11** überprüft, ob die Antwort korrekt ist. Dies kann bei einem Ausführungsbeispiel des Aufgabe-Antwort-Algorithmus dadurch geschehen, das der Betrieb des ausgewählten Aggregats **12** nach den Stellen der Aufgabe im Schritt **33** durch die zentrale Steuerung **11** überwacht wird, so dass geprüft werden kann, ob der übermittelte Steuer- oder Regelparameter P beim weiteren Betrieb verwendet wird. Bei einem anderen Ausführungsbeispiel des Aufgabe-Antwort-Algorithmus kann als Antwort ein mittels einer Rechenoperation verschlüsselter Betriebsparameter an die zentrale Steuerung übermittelt oder zum Auslesen in einem Register des Speichers **21** abgespeichert werden.

[0066] Ist die Antwort korrekt (Verzweigung OK aus Schritt **35**) wird die Authentizität des ausgewählten Aggregats **12** im Schritt **36** bestätigt. Ist dies nicht der Fall (Verzweigung NOK aus Schritt **35**) wird in einem Schritt **37** die fehlende Authentizität des ausgewählten Aggregats festgestellt. Optional kann im Schritt **37** das nicht authentifizierte Aggregat **12** stillgesetzt werden und/oder eine entsprechende Mitteilung über eine Schnittstelle der Anlage **10** ausgegeben werden, um den Austausch des nicht authentifizierten Aggregats **12** zu veranlassen.

[0067] Das Stillsetzen des nicht authentifizierten Aggregats **12** im Schritt **37** kann beispielsweise dadurch erfolgen, dass eine entsprechende steuerungstechnische oder regelungstechnische Vorgabe von der zentralen Steuerung **11** an das Aggregat **12** übertragen wird, beispielsweise ein Sollwert gleich Null. Selbstverständlich erfolgt der Befehl zum Stillsetzen derart, dass die Anforderung vom nicht authentifizierten Aggregat **12** umgesetzt werden kann, insbesondere unverschlüsselt ohne Verwendung der Rechenoperation **C**.

[0068] In dem Schritt **33** des Verfahrens kann die Aufgabe auch darin bestehen, dass die zentrale Steuerung **11** einen Betriebsparameter des ausgewählten Aggregats **12** erfasst. Beispielsweise kann ein Istwert des ausgewählten Aggregats **12** ermittelt werden. Bei dem vom Ventilator **15** gebildeten Aggregat **12** kann beispielsweise ein Motorstrom oder die Drehzahl des Elektromotors **17** durch einen Sensor **19** erfasst und das Sensorsignal $\mathbf{O_x}$ als Sensorwert $\mathbf{OV_x}$, beispielsweise binärer Sensorwert, in einem Register des Speichers **21** zum Auslesen bereitgestellt werden. Der Sensorwert $\mathbf{OV_x}$ kann dann durch die zentrale Steuerung **11** ausgelesen werden. Dieses Auslesen kann gleichzeitig eine Aufgabe für das ausgewählte Aggregat **12** darstellen (Schritt **33**).

[0069] Als Antwort auf diese Aufgabe kann das ausgewählte Aggregat **12** bzw. die Aggregatsteuerung **16** den im Register des Speichers **21** gespeicherten Sensorwert $\mathbf{OV_x}$ über die Rechenoperation **C** verschlüsseln und beispielsweise mit einem oder mehreren anderen Werten verknüpfen, wie etwa mit der Seriennummer $\mathbf{N_x}$ oder einem Teil davon, dem unveränderlichen Registerwert $\mathbf{F_x}$ und /oder dem Initialisierungswert $\mathbf{Init_x}$. Der auf diese Weise verschlüsselte Sensorwert $\mathbf{OV_x}$ kann als Ausgangsregisterwert $\mathbf{Rout_x}$ in einem Ausgangsregister des Speichers **21** für das Auslesen durch die zentrale Steuerung **11** bereitgestellt werden oder alternativ auch an die zentrale Steuerung **11** übermittelt werden. Der berechnete und bereitgestellte Ausgangsregisterwert $\mathbf{Rout_x}$ bildet die Antwort (Schritt **34**).

[0070] Die zentrale Steuerung **11** kann die Antwort basierend auf den bekannten Werten und/oder der Rechenoperation **C** verwenden, um den Sensorwert $\mathbf{O_x}$ wieder zu ermitteln und das Ergebnis mit dem erfassten Sensorwert zu vergleichen (Schritt **35**). Stimmen die Werte überein, war die Antwort korrekt und die Authentizität bestätigt (Schritt **36**). Andernfalls wird die Authentizität verneint (Schritt **37**).

[0071] Bei diesen beispielhaften Aufgabe-Lösungs-Algorithmen werden Betriebsparameter, beispielsweise Sollwerte, Grenzwerte oder andere Steuer- oder Regelparameter oder Istwerte verwendet, um die Aufgabe und/oder die Lösung des Aufgabe-Lösungs-Algorithmus zu bilden. Da solche Betriebsparameter während des Betriebs der Anlage **10** zumindest von Zeit zu Zeit ohnehin übermittelt werden müssen, stellt dieses Verfahren eine besonders effiziente Möglichkeit der Authentifizierung dar. Die Kommunikation über das Kommunikationssystem **13** wird nicht oder nur geringfügig erhöht.

[0072] In den **Fig. 5** und **Fig. 6** ist ein weiteres Ausführungsbeispiel eines Verfahrens zur Authentifizierung veranschaulicht. Nach dem Start kann im Rahmen einer Initialisierung jedem Aggregat **12** der Anlage **10** ein Initialisierungswert $\mathbf{Init_x}$ übermittelt werden (Schritt **40**). Analog zum Schritt **30** aus **Fig. 4** können zusätzlich oder alternativ zu dieser Initialisierung auch bereits vor dem Einbau in die Anlage **10** vorgegebene Werte $\mathbf{N_x}$ oder $\mathbf{F_x}$ für das weitere Verfahren verwendet werden. Der Austausch von Werten im Rahmen der Initialisierung im Schritt **40** für eine spätere Authentifizierung ist optional. Für den Schritt **40** gelten die Erläuterungen zum Schritt **30** gemäß dem Verfahren aus **Fig. 4** entsprechend.

[0073] Im Anschluss an den Schritt **40** wird in einem Schritt **41** überprüft, ob ein Steuer- oder Regelparameter P von der zentralen Steuerung **11** an eines der Aggregate **12** übertragen werden soll. Es erfolgt im Schritt **41** daher eine Prüfung, ob eine Prüfbedingung erfüllt ist, die das Überprüfen der Authentizität eines ausgewählten Aggregats **12** auslöst.

[0074] Ist dies nicht der Fall (Verzweigung NOK aus Schritt **41**) wird in einem Schritt **42** geprüft, ob eine andere Prüfbedingung erfüllt ist, beispielsweise eine Zufallsbedingung in der zentralen Steuerung **11**. Ist dies der Fall (Verzweigung OK aus Schritt **42**) wird eine Verfahrensroutine **V** gemäß **Fig. 6** aufgerufen (Schritt **43**). Andernfalls (Verzweigung NOK aus Schritt **42**) kehrt das Verfahren zum Schritt **41** zurück.

[0075] Wenn ein Steuer- oder Regelparameter P übertragen werden soll (Verzweigung OK aus Schritt **41**), wird in einem Schritt **44** unter Verwendung der Rechenoperation **C**, dem Steuer- oder Regelparameter P und optional wenigstens einem der Werte $\mathbf{Init_x}$, $\mathbf{N_x}$, $\mathbf{F_x}$ der modifizierte Parameter Pmod erzeugt und an das ausgewählte Aggregat **12** übermittelt.

[0076] Das ausgewählte Aggregat **12** empfängt den modifizierten Parameter Pmod und kann als Antwort darauf, sofern die Rechenoperation **C** und die optional verwendeten Werte $\mathbf{Init_x}$, $\mathbf{N_x}$, $\mathbf{F_x}$ bekannt sind, den Steuer- oder Regelparameter P ermitteln und die Steuerung oder Regelung auf Basis des Steuer- oder Regelparameters P anpassen (Schritt **45**).

[0077] Im Schritt **46** wird überprüft, ob das ausgewählte Aggregat **12** basierend auf dem modifizierten Parameter Pmod in der Lage war, den verschlüsselt übertragenen Steuer- oder Regelparameter P aus dem modifizierten Parameter Pmod zu ermitteln

und basierend darauf den Betrieb des ausgewählten Aggregats **12** anzupassen. Wenn beispielsweise der übertragene Steuer- oder Regelparameter P ein Sollwert ist, kann die zentrale Steuerung **11** prüfen, ob der zugehörige Istwert im Rahmen der vorgegebenen Toleranz mit dem übermittelten Sollwert übereinstimmt oder sich daran annähert. Das Anpassen des Betriebs basierend auf dem empfangenen Steuer- oder Regelparameter P stellt die Antwort des ausgewählten Aggregats **12** dar.

[0078] Ist die Antwort korrekt und wurde der Betrieb korrekt angepasst (Verzweigung OK aus dem Schritt **46**) wird in einem Schritt **47** die Authentizität des ausgewählten Aggregats **12** bestätigt. Andernfalls wird in einem Schritt **48** die Authentizität des ausgewählten Aggregats **12** verneint und optional das nicht authentifizierte Aggregat **12** stillgesetzt. Nach dem Schritt **47** oder dem Schritt **48** wird das Verfahren wieder im Schritt **41** fortgeführt.

[0079] In Bezug auf die Schritte **44** und **45** wird auch auf die Erläuterungen zu den Schritten **33** und **34** des Verfahrens nach **Fig. 4** Bezug genommen.

[0080] Wenn eine Übertragung eines Betriebsparameter im Schritt **41** nicht erforderlich ist, jedoch eine andere Prüfbedingung zur Überprüfung der Authentizität eines der Aggregate **12** erfüllt ist (Verzweigung OK aus dem Schritt **42**), wird die Verfahrensroutine **V** im Schritt **43** aufgerufen. Ein Ausführungsbeispiel der Verfahrensroutine **V** ist in **Fig. 6** gezeigt.

[0081] Nach dem Start der Verfahrensroutine **V** wird in einem Schritt **50** ein Zufallswert, beispielsweise eine Zufallszahl erzeugt und als Eingangsregisterwert $\mathbf{Rin_x}$ in ein Eingangsregister des Speichers **21** eingetragen. Das Schreiben des Eingangsregisterwerts $\mathbf{Rin_x}$ in das Eingangsregister stellt die Aufgabe an das ausgewählte Aggregat **12** dar.

[0082] In einem darauffolgenden Schritt **51** erzeugt das ausgewählte Aggregat **12** eine Antwort basierend auf der im Eingangsregister $\mathbf{Rin_x}$ eingetragenen Zufallszahl. Dazu wird der Eingangsregisterwert $\mathbf{Rin_x}$ durch die Rechenoperation **C** verschlüsselt, wobei die Rechenoperation **C** den Eingangsregisterwert $\mathbf{Rin_x}$ optional zusätzlich mit einem oder mehreren weiteren Werten verknüpft werden kann. Das Ergebnis der Rechenoperation **C** ist der Ausgangsregisterwert $\mathbf{Rout_x}$, der als Antwort durch das ausgewählte Aggregat **12** für die zentrale Steuereinheit **11** bereitgestellt wird. Beispielsgemäß wird die Antwort in dem Ausgangsregister für den Zugriff durch die zentrale Steuerung **11** bereitgestellt.

[0083] Die zentrale Steuerung **11** kennt die Rechenoperation **C** und den wenigstens einen weiteren Wert, mit dem die übermittelte Zufallszahl verknüpft wurde, beispielsweise die Seriennummer $\mathbf{N_x}$ und/oder unveränderlichen Registerwert $\mathbf{F_x}$ und/oder den Initialisierungswert $\mathbf{Init_x}$. Im Schritt **52** prüft die zentrale Steuerung **11**, ob der Eingangsregisterwert $\mathbf{Rin_x}$ korrekt modifiziert bzw. verknüpft wurde. Ist dies der Fall (Verzweigung OK aus dem Schritt **52**) wird in einem Schritt **53** die Authentizität des ausgewählten Aggregats **12** bestätigt. Andernfalls (Verzweigung NOK aus Schritt **52**) wird die Authentizität des ausgewählten Aggregats **12** verneint und es können Maßnahmen ergriffen werden, beispielsweise das ausgewählte Aggregat **12** stillgesetzt (Schritt **54**).

[0084] Nach dem Schritt **53** oder dem Schritt **54** wird in das Verfahren zur Authentifizierung gemäß **Fig. 5** zurückgesprungen und das Verfahren wird dort nach Abschluss der Verfahrensroutine **V** im Schritt **41** fortgesetzt.

[0085] Zusätzlich oder alternativ zu den bereits erläuterten Werten kann im Schritt **51** zur Berechnung der Antwort auch ein Betriebsparameter, insbesondere ein Istwert des Betriebs des Aggregats **12** verwendet werden, wie etwa eine Isttemperatur, eine Istdrehzahl, ein Iststrom, eine aktuelle Zahl der Betriebsstunden des Aggregats **12**, usw. Den entsprechenden Betriebsparameter kann die zentrale Steuerung **11** aus einem Register des Speichers **21** auslesen und bei der Prüfung im Schritt **52** berücksichtigen.

[0086] Es ist zu beachten, dass insbesondere bei der Verwendung von aktuellen Istwerten eines Aggregats **12** bei der Authentifizierung in Einzelfällen Abweichungen auftreten können. Die Abweichungen können dadurch bedingt sein, dass sich ein Istwert zwischen der Abfrage durch die zentrale Steuerung **11** und dem Erzeugen der Antwort durch das Aggregat **12** verändert. Bei einer solchen Authentifizierung kann es erforderlich sein, den Authentifizierungsprozess mehrfach zu wiederholen, um dann zu entscheiden, ob die Authentizität bejaht oder verneint werden kann. Beispielsweise kann hier eine Mehrheitsentscheidung getroffen werden.

[0087] Die Erfindung betrifft ein Verfahren zur Authentifizierung eines Aggregats **12** einer Anlage **10**. Die Anlage **10** weist eine zentrale Steuerung **11** auf, die mit einem oder mehreren Aggregaten **12** in Kommunikationsverbindung steht. Zur Prüfung der Authentizität eines Aggregats **12** steht wenigstens ein Aufgabe-Antwort-Algorithmus zur Verfügung. Wenn mehrere Aufgabe-Antwort-Algorithmen zur Verfügung stehen, beruht wenigstens ein Aufgabe-Antwort-Algorithmus auf der Verwendung eines Betriebsparameters. Bei dem Betriebsparameter kann es sich beispielsweise um einen von der zentralen Steuerung **11** an das Aggregat **12** zu übertragenden Steuer- oder Regelparameter P handeln oder um einen in aktuellen Betriebszustand des Aggregats **12** beschreibenden Istwert. Dabei kann die Aufga-

be oder die Antwort auf dem Betriebsparameter beruhen. Bei einer bevorzugten Ausführungsform wird ein in dem ausgewählten Aggregat **12** einzustellender Steuer- oder Regelparameter P, beispielsweise ein Sollwert, modifiziert und als modifizierter Parameter Pmod an das ausgewählte Aggregat **12** übertragen. Anschließend wird überprüft, ob das ausgewählte Aggregat **12** in der Lage ist, den modifizierten Parameter Pmod korrekt in den Steuer- oder Regelparameter P umzurechnen und daraufhin den Betrieb unter Verwendung des ermittelten Steuer- oder Regelparameters P anzupassen. Ist dies der Fall, ist die Authentifizierung des Aggregats **12** erfolgreich.

Bezugszeichenliste

10	Anlage
11	zentrale Steuerung
12	Aggregat
13	Kommunikationssystem
14	Bussystem
15	Ventilator
16	Aggregatsteuerung
17	Elektromotor
18	Rotoreinheit
19	Sensor
20	Schnittstelle
21	Speicher
30	Schritt eines ersten Verfahrens
31	Schritt eines ersten Verfahrens
32	Schritt eines ersten Verfahrens
33	Schritt eines ersten Verfahrens
34	Schritt eines ersten Verfahrens
35	Schritt eines ersten Verfahrens
36	Schritt eines ersten Verfahrens
37	Schritt eines ersten Verfahrens
39	Schritt eines zweiten Verfahrens
40	Schritt eines zweiten Verfahrens
41	Schritt eines zweiten Verfahrens
42	Schritt eines zweiten Verfahrens
43	Schritt eines zweiten Verfahrens
44	Schritt eines zweiten Verfahrens
45	Schritt eines zweiten Verfahrens
46	Schritt eines zweiten Verfahrens
47	Schritt eines zweiten Verfahrens
48	Schritt eines zweiten Verfahrens
50	Schritt einer Verfahrensroutine
51	Schritt einer Verfahrensroutine
52	Schritt einer Verfahrensroutine
53	Schritt einer Verfahrensroutine
54	Schritt einer Verfahrensroutine
C	Rechenoperation
F_x	unveränderlicher Registerwert
G	Gruppe
$Init_x$	Initialisierungswert
M	Master
N_x	Seriennummer
O_x	Sensorsignal
OV_x	Sensorwert
Rin_x	Eingangsregisterwert
$Rout_x$	Ausgangsregisterwert $Rout_x$
S_x	Slave
V	Verfahrensroutine

Patentansprüche

1. Verfahren zur Authentifizierung wenigstens eines Aggregats (12) einer Anlage (10), die außerdem eine zentrale Steuerung (11) aufweist, die mit dem wenigstens einen Aggregat (12) kommunikationsverbunden ist, wobei das Verfahren folgende Schritte umfasst:
- Auswählen eines der Aggregate (12), das authentifiziert werden soll, wenn eine Prüfbedingung erfüllt ist,
- Erfassen eines Betriebsparameters (O_x) des ausgewählten Aggregats (12) oder Ermitteln eines Betriebsparameters (P) für das ausgewählte Aggregat (12),
- Erzeugen einer Aufgabe und Erzeugen einer Antwort auf die empfangene Aufgabe durch das ausgewählte Aggregat (12), wobei die Aufgabe und/oder die Antwort auf dem Betriebsparameter (P, O_x) basiert,
- Bereitstellen einer Gruppe (G) mit zwei oder mehr Aufgabe-Antwort-Algorithmen, die den auf dem Betriebsparameter (P, O_x) basierten Aufgabe-Antwort-Algorithmus aufweist, wobei vor oder nach dem Auswählen eines der Aggregate (12) zur Authentifizierung zumindest ein Aufgabe-Antwort-Algorithmus aus der Gruppe (G) ausgewählt wird, um die Authentifizierung durchzuführen,
- Übertragen der Aufgabe des ausgewählten Aufgabe-Antwort-Algorithmus an das ausgewählte Aggregat (12),
- Überprüfen durch die zentrale Steuerung (11), ob die Antwort des ausgewählten Aggregats (12) nach dem Empfang der Aufgabe korrekt ist,

- Bestätigen der Authentizität des ausgewählten Aggregats (12), wenn die Antwort des ausgewählten Aggregats (12) korrekt ist.

2. Verfahren nach Anspruch 1, wobei das ausgewählte Aggregat (12) den Betriebsparameter (P) aus der empfangenen Aufgabe (P_{mod}) ermittelt und für den weiteren Betrieb verwendet.

3. Verfahren nach Anspruch 1 oder 2, wobei der Betriebsparameter (P) ein Sollwert ist, der in Form der Aufgabe (P_{mod}) an das ausgewählte Aggregat (12) übermittelt wird.

4. Verfahren nach Anspruch 3, wobei das ausgewählte Aggregat (12) den Sollwert aus der empfangenen Aufgabe (P_{mod}) ermittelt und den Betrieb des Aggregats (12) basierend auf dem ermittelten Sollwert steuert oder regelt.

5. Verfahren nach Anspruch 3 oder 4, wobei Sollwerte ausschließlich als Aufgabe (P_{mod}) an alle Aggregate (12) der Anlage (10) übertragen werden.

6. Verfahren nach einem der vorhergehenden Ansprüche 2 bis 5, wobei die zentrale Steuerung (11) den Betrieb des ausgewählten Aggregats (12) überwacht um festzustellen, ob der Betrieb des Aggregats (12) korrekt an den in der Aufgabe (P_{mod}) enthaltenen Betriebsparameter (P) angepasst wurde.

7. Verfahren nach einem der vorhergehenden Ansprüche, wobei das ausgewählte Aggregat (12) dazu eingerichtet ist, auf die empfangene Aufgabe eine Antwort zu ermitteln und der zentralen Steuerung (11) bereitzustellen.

8. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Aufgabe basierend auf dem Betriebsparameter (P, O_x) und einem Initialisierungswert ($Init_x$) des ausgewählten Aggregats (12) gebildet ist, der bei der Initialisierung festgelegt wird.

9. Verfahren nach Anspruch 8, wobei ein weiterer Aufgabe-Antwort-Algorithmus auf einem Zufallswert basiert, der dem ausgewählten Aggregat (12) von der zentralen Steuerung (11) bereitgestellt wird, und wobei das ausgewählte Aggregat (12) eine Antwort basierend auf dem Zufallswert und dem Initialisierungswert ($Init_x$) ermittelt und der zentralen Steuerung (11) bereitstellt.

10. Verfahren nach einem der Anspruch 8 oder 9, wobei ein weiterer Algorithmus auf einem Zufallswert basiert, der dem ausgewählten Aggregat (12) von der zentralen Steuerung (11) bereitgestellt wird und wobei das ausgewählte Aggregat (12) eine Antwort basierend auf dem Zufallswert und einem unveränderlichen Registerwert (F_x) ermittelt und der zentralen Steuerung (11) bereitstellt.

11. Anlage (10) aufweisend eine zentrale Steuerung (11) und wenigstens ein gesteuertes Aggregat (12), die miteinander kommunikationsverbunden sind, wobei die zentrale Steuerung (11) und das wenigstens eine Aggregat (12) dazu eingerichtet sind, das Verfahren nach einem der vorhergehenden Ansprüche durchzuführen.

Es folgen 4 Seiten Zeichnungen

Anhängende Zeichnungen

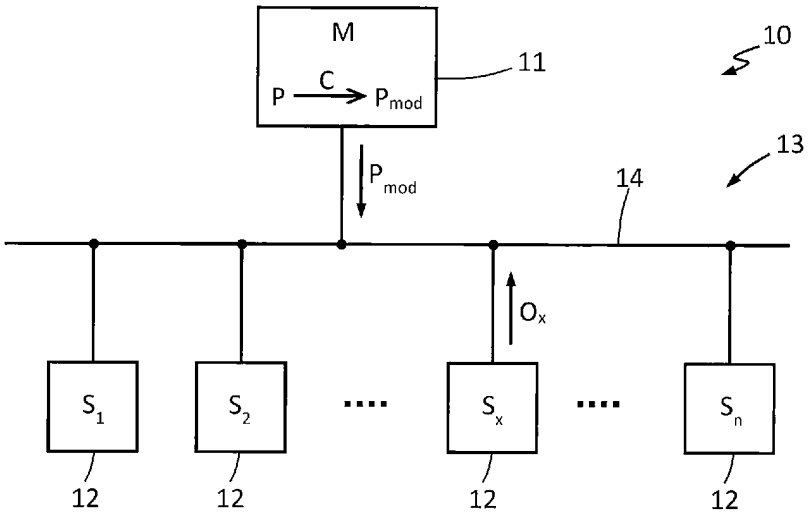


Fig. 1

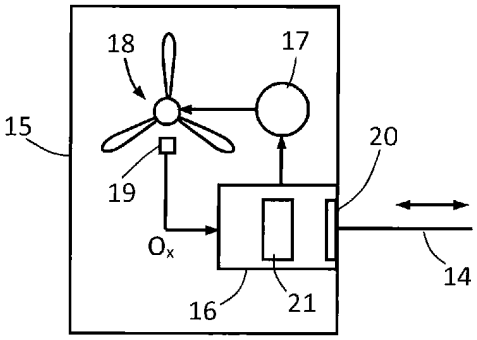


Fig. 2

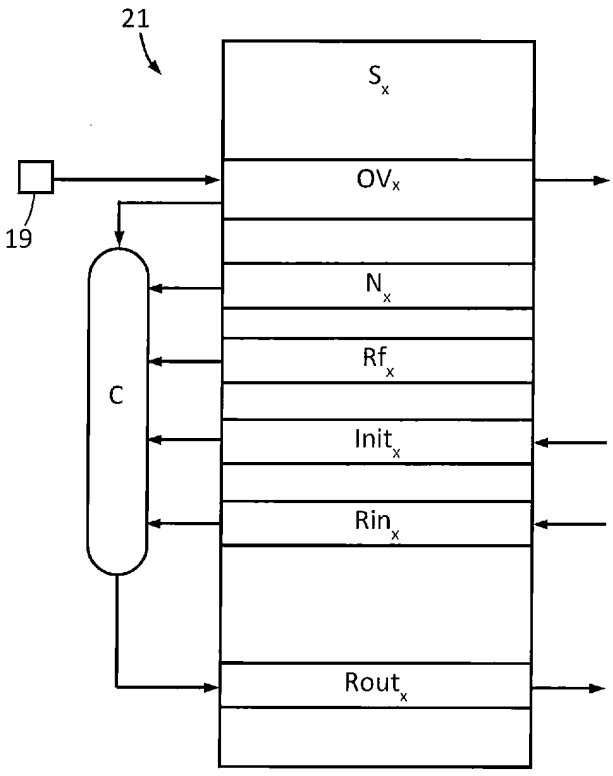


Fig. 3

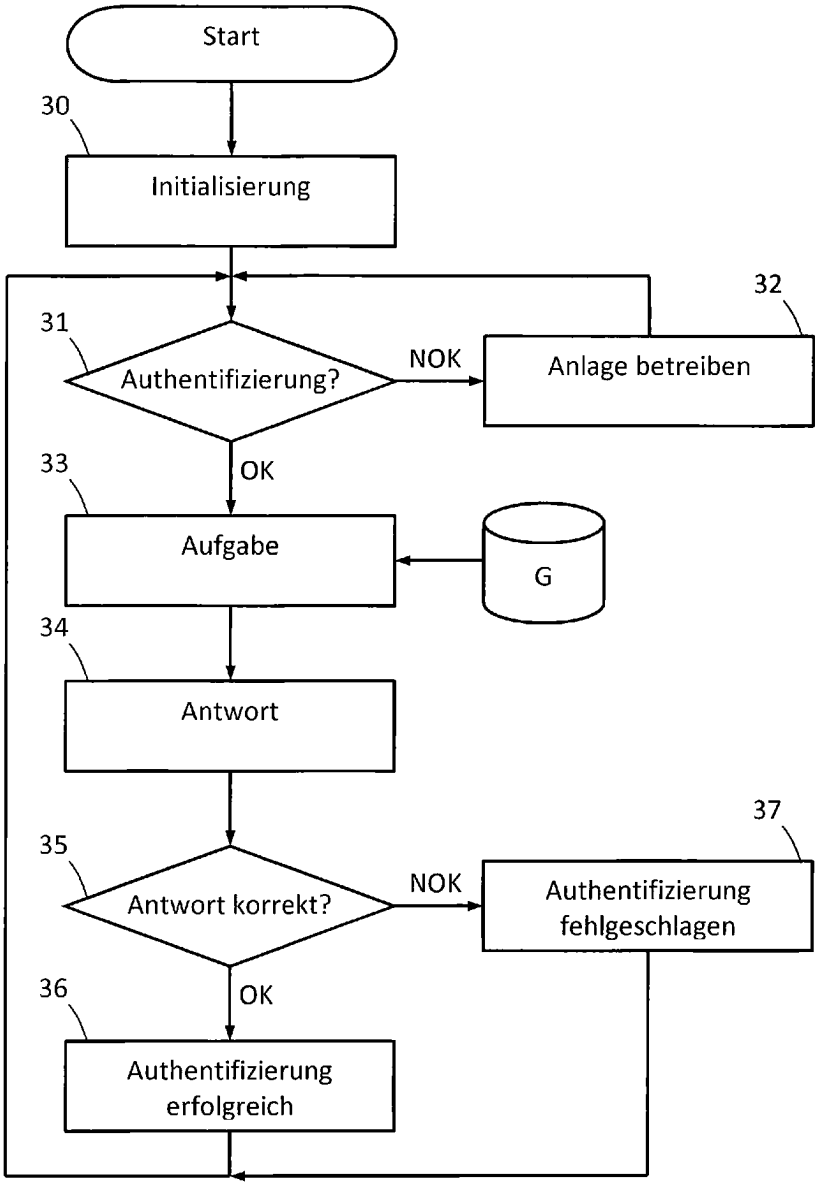

Start
30
Initialisierung
31
Authentifizierung?
NOK
32
Anlage betreiben
OK
33
Aufgabe
G
34
Antwort
35
Antwort korrekt?
NOK
37
Authentifizierung fehlgeschlagen
OK
36
Authentifizierung erfolgreich

Fig. 4

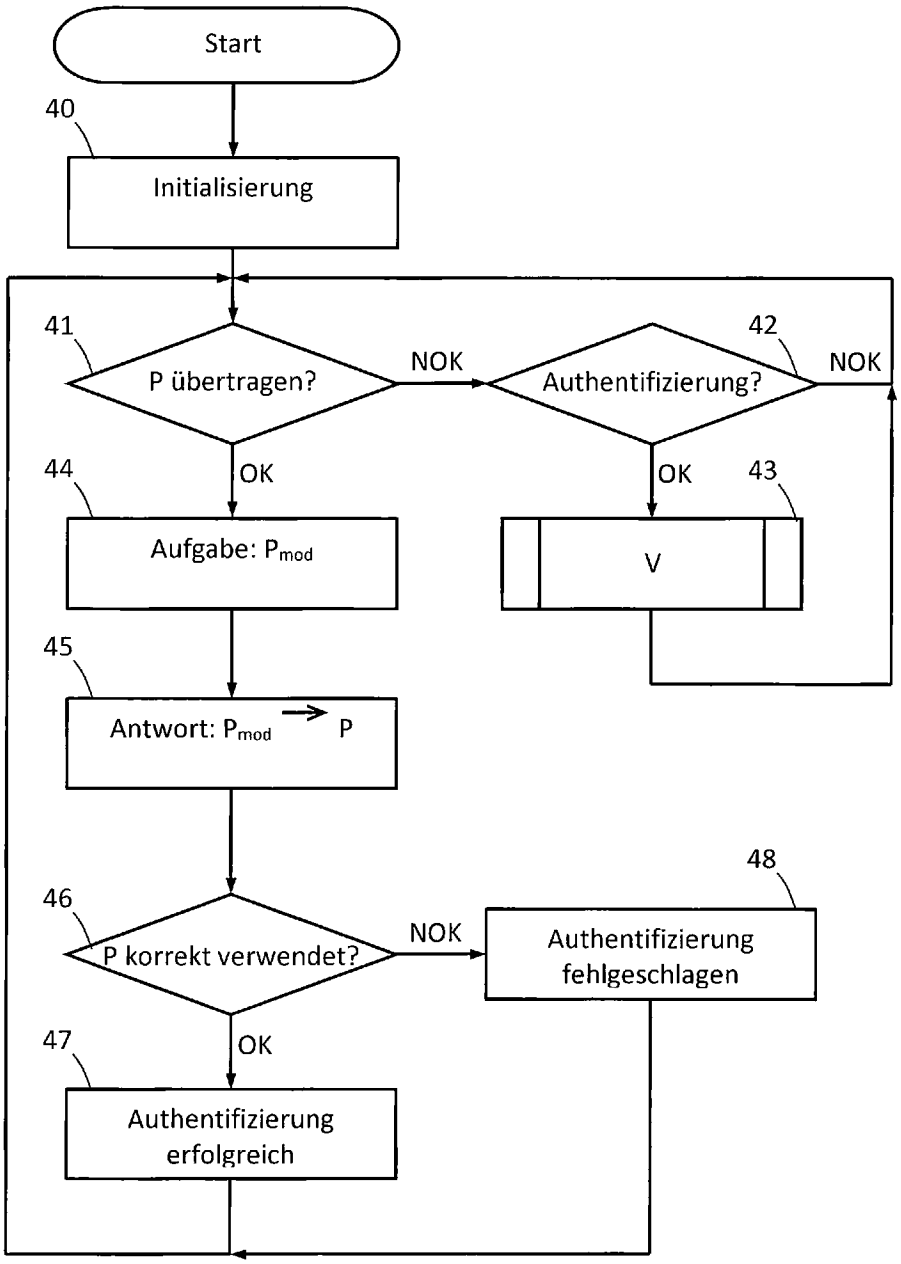

Start
40
Initialisierung
41
P übertragen?
NOK
42
Authentifizierung?
NOK
OK
OK
44
43
Aufgabe: P_{mod}
V
45
Antwort: P_{mod} P
48
46
P korrekt verwendet?
NOK
Authentifizierung fehlgeschlagen
OK
47
Authentifizierung erfolgreich

Fig. 5

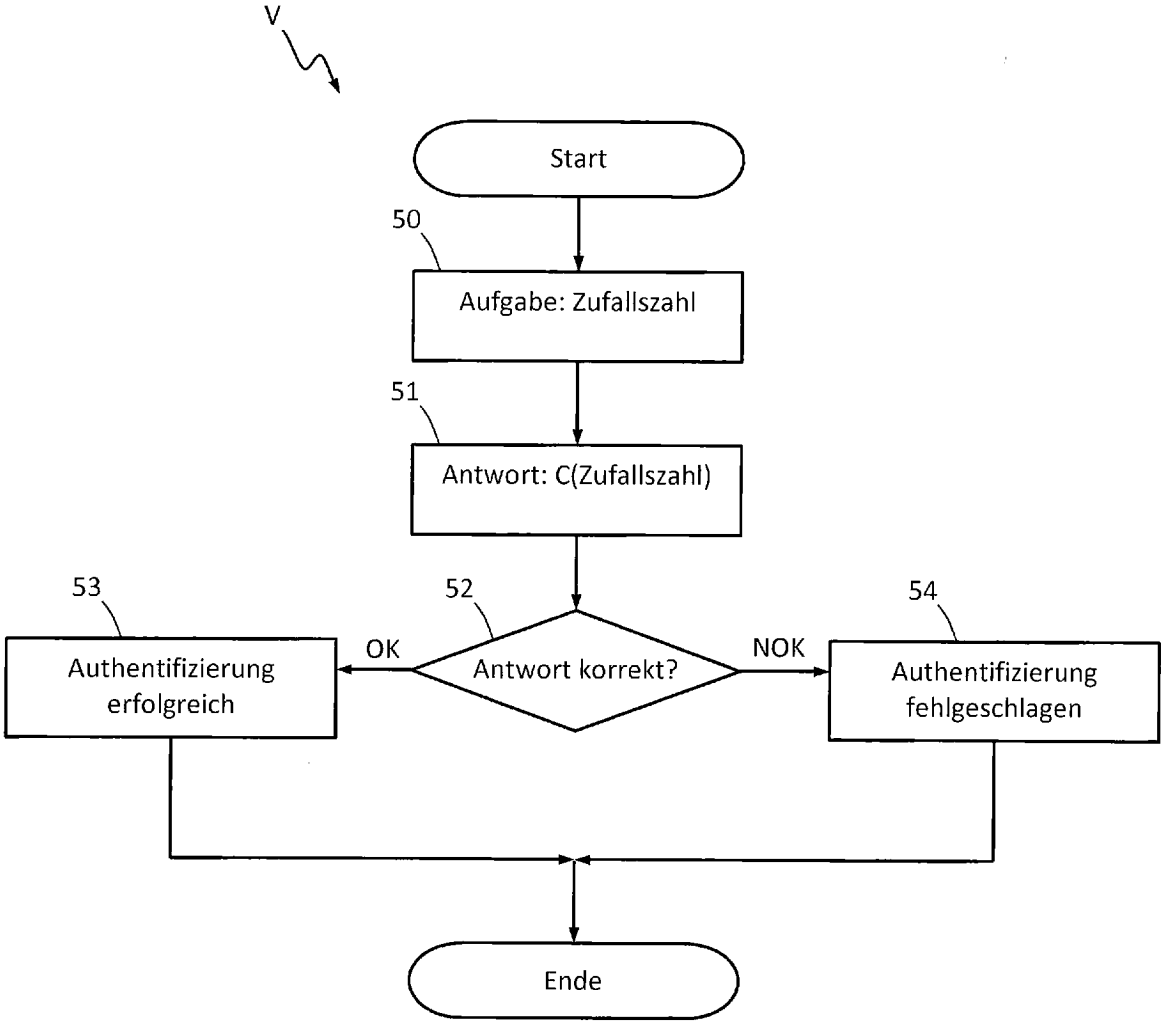


Fig. 6

