

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

(19) Weltorganisation für geistiges Eigentum
Internationales Büro



(43) Internationales Veröffentlichungsdatum
5. April 2007 (05.04.2007)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2007/036178 A1

(51) Internationale Patentklassifikation:
G05B 19/042 (2006.01)

(21) Internationales Aktenzeichen: PCT/DE2005/001751

(22) Internationales Anmeldedatum:
29. September 2005 (29.09.2005)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme von
US): **SIEMENS AKTIENGESellschaft** [DE/DE];
Wittelsbacherplatz 2, 80333 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder (nur für US): **JURISCH, Andreas**
[DE/DE]; Eichenweg 11, 16727 Schwante (DE).

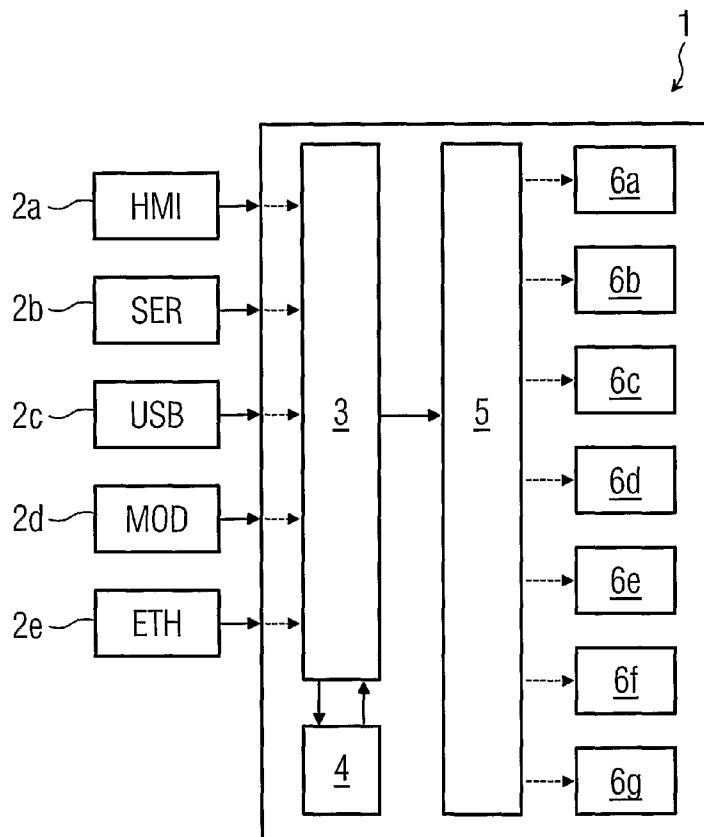
(74) Gemeinsamer Vertreter: **SIEMENS AKTIENGE-
SELLSCHAFT?**; Wittelsbacherplatz 2, 80333 München
(DE).

(81) Bestimmungsstaaten (soweit nicht anders angegeben, für
jede verfügbare nationale Schutzrechtsart): AE, AG, AL,
AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH,
CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES,
FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE,
KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY,
MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO,

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD FOR CARRYING OUT A PROTECTED FUNCTION OF AN ELECTRICAL FIELD DEVICE, AND AN
ELECTRICAL FIELD DEVICE

(54) Bezeichnung: VERFAHREN ZUM AUSFÜHREN EINER GESCHÜTZTEN FUNKTION EINES ELEKTRISCHEN FELD-
GERÄTES UND ELEKTRISCHES FELDGERÄT



(57) Abstract: In order to develop a method
for carrying out a protected function of an elec-
trical field device (1) in such a manner that a
high degree of security against unauthorized
accesses to the electrical field device (1) can be
ensured irrespective of the nature of the com-
munication link between a user and the elec-
trical field device, an identification device (3)
for the electrical field device (1) and a security
device (5) are used to check whether a stated
protected function of the electrical field device
(1) can be carried out, or should be refused.
The invention also relates to an appropriately
designed electrical field device.

(57) Zusammenfassung: Um ein Verfahren
zum Ausführen einer geschützten Funktion
eines elektrischen Feldgerätes (1) derart
auszugestalten, dass unabhängig von der Art
der Kommunikationsverbindung zwischen
einem Benutzer und dem elektrischen
Feldgerät eine hohe Sicherheit gegen
unbefugte Zugriffe auf das elektrische
Feldgerät (1) gewährleistet werden kann, wird
mit Hilfe einer Identifizierungseinrichtung
(3) des elektrischen Feldgerätes (1) und einer
Sicherheitseinrichtung (5) überprüft, ob eine
Ausführung einer angegebenen geschützten
Funktion

[Fortsetzung auf der nächsten Seite]

WO 2007/036178 A1



NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

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

Veröffentlicht:

— mit internationalem Recherchenbericht

(84) Bestimmungsstaaten (soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC,

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Beschreibung

Verfahren zum Ausführen einer geschützten Funktion eines elektrischen Feldgerätes und elektrisches Feldgerät

5

Elektrische Feldgeräte werden heutzutage in vielen Bereichen der Automatisierungstechnik eingesetzt. So können elektrische Feldgeräte beispielsweise zur Überwachung und Steuerung von chemischen und verfahrenstechnischen Prozessen, von industriellen Fertigungsprozessen oder auch von Prozessen zur Übertragung und/oder Verteilung elektrischer Energie in elektrischen Energieversorgungsnetzen verwendet werden. Normalerweise befinden sich die elektrischen Feldgeräte hierbei in der Nähe des zu automatisierenden Prozesses und nehmen dort den Prozess beschreibende Messwerte auf bzw. geben Befehle zur Steuerung von Prozesskomponenten ab.

So kann beispielsweise ein Feldgerät in einem elektrischen Energieversorgungsnetz Strom- und Spannungsmesswerte aufnehmen, die den momentanen Zustand des elektrischen Energieversorgungsnetzes angeben. Weiterhin kann das elektrische Feldgerät Steuerbefehle, wie beispielsweise einen Befehl zum Öffnen oder Schließen eines Leistungsschalters in dem elektrischen Energieversorgungsnetz, abgeben.

25

Normalerweise sind solche Feldgeräte vor unbefugtem Zugriff zu schützen. Dazu sind sie beispielsweise in entsprechend gesicherten Bereichen angeordnet, zu denen nur entsprechendes Personal Zugang hat. Solche gesicherten Bereiche können beispielsweise durch Türen oder Absperrungen geschützt sein; häufig findet auch eine Kameraüberwachung statt, um unerlaubten Fremdzugriff auf die Feldgeräte möglichst schnell erkennen bzw. verhindern zu können.

30

Zur Bedienung weisen elektrische Feldgeräte üblicherweise eine Eingabevorrichtung, wie beispielsweise ein Tastenfeld, und eine Anzeigevorrichtung, wie z. B. ein Display, auf. Über
5 die Eingabevorrichtung können alle Funktionen direkt am elektrischen Feldgerät aufgerufen werden. Für die Sicherheit des automatisierten Prozesses relevante Funktionen können hierbei üblicherweise nur nach Eingabe eines entsprechenden Passwortes ausgeführt werden. Innerhalb der letzten Jahre
10 wurden zur Vereinfachung der Bedienung von Feldgeräten Datenschnittstellen an diesen vorgesehen, mit denen eine Bedienung und/oder Beobachtung der Feldgeräte lokal oder aus der Ferne möglich ist. Üblich ist hierbei z. B. das Vorsehen einer seriellen Schnittstelle als Datenschnittstelle am elektrischen
15 Feldgerät, über die beispielsweise eine externe Datenverarbeitungseinrichtung, wie z.B. ein Parametrier-Laptop, angeschlossen werden kann, um Parameter-Einstellungen in dem elektrischen Feldgerät vorzunehmen.

20 Aufgrund dieser neuen Möglichkeit zur Bedienung von elektrischen Feldgeräten aus der Ferne ergeben sich jedoch stark veränderte Sicherheitsbedingungen. Während es bei älteren elektrischen Feldgeräten ohne die Möglichkeit einer Fernbedienung nämlich relativ einfach ist, den Zugriff auf das
25 Feldgerät wie oben beschrieben beispielsweise durch bauliche Maßnahmen und entsprechende Überwachungen zu verhindern, ist bei der Bedienung eines mit einer entsprechenden Datenschnittstelle versehenen Feldgerätes aus der Ferne die Gefahr eines unerlaubten Fremdzugriffs deutlich erhöht. Diese Gefahr
30 steigt durch die Einführung von netzwerkfähigen Ethernet-Schnittstellen als Datenschnittstellen an den Feldgeräten nochmals deutlich an, da die Feldgeräte nunmehr über große, nicht vollkommen absicherbare Netzwerke, wie beispielsweise ein Intranet oder sogar das Internet, angebunden sein können.

Aus der Systembeschreibung von SIPROTEC 4-Feldgeräten der Siemens AG, Ausgabe: 21.06.04, Bestellnr. E50417-H1100-C151-A6, gehen elektrische Feldgeräte hervor, die eine Eingabevorrichtung in Form eines Tastenfeldes und eine Anzeigevorrichtung in Form eines Displays aufweisen (vgl. z. B. S. 20 - 21 der Systembeschreibung). Über das Tastenfeld können sämtliche Funktionen des elektrischen Feldgerätes aufgerufen werden. Zum Aufrufen geschützter Funktionen muss über das Eingabefeld ein entsprechendes Passwort eingegeben werden (vgl. z. B. S. 12 der Systembeschreibung). Die Feldgeräte weisen ferner an ihrer Frontseite als Datenschnittstelle eine so genannte Bedienschnittstelle in Form einer seriellen Steckverbindung auf. An diese Bedienschnittstelle kann über ein seriellles Datenübertragungskabel ein externer Computer angeschlossen werden, auf dem eine Bedien-/Beobachtungs- und/oder Parametriersoftware abläuft. Mit Hilfe dieser Software können Einstellungen in dem Gerät vorgenommen und geändert sowie die Bedienung und Beobachtung des Gerätes durchgeführt werden.

Wie außerdem aus der erwähnten Systembeschreibung hervorgeht, können die Geräte auch mit einer Datenschnittstelle in Form einer Ethernet-Schnittstelle ausgestattet sein, die eine Netzwerkanbindung des Gerätes ermöglicht. Die Ansteuerung von geschützten Funktionen des elektrischen Feldgerätes ist standardmäßig über die Ethernet-Schnittstelle gesperrt, kann aber über den Benutzer des Feldgerätes auch zugelassen werden (vgl. S. 12 der Systembeschreibung).

Die Aufgabe der vorliegenden Erfindung besteht darin, ein Verfahren zum Ausführen einer geschützten Funktion eines elektrischen Feldgerätes sowie ein elektrisches Feldgerät anzugeben, wobei unabhängig von der Art der Kommunikationsver-

bindung mit dem elektrischen Feldgerät ein hoher Sicherheitsstandard gegen ungewollte Zugriffe gewährleistet wird.

5 Bezüglich des Verfahrens wird diese Aufgabe erfindungsgemäß durch ein Verfahren zum Ausführen einer geschützten Funktion eines elektrischen Feldgerätes gelöst, bei dem folgende Schritte durchgeführt werden: Von dem elektrischen Feldgerät werden Befehlsdaten empfangen, die einen Funktionsaufruf zum Ausführen einer geschützten Funktion des elektrischen Feldge-
10 räts angeben; von einer Identifizierungseinrichtung des elektrischen Feldgerätes werden den jeweiligen Absender der Befehlsdaten charakterisierende Absendercharakterisierungsdaten ermittelt und an die Befehlsdaten angefügt; von einer Si-
15 cherheitseinrichtung werden die um die Absendercharakterisierungsdaten erweiterten Befehlsdaten empfangen und daraufhin überprüft, ob sie eine Ausführung der von den Befehlsdaten angegebenen geschützten Funktion des elektrischen Feldgerätes erlauben, wobei bei bestehender Erlaubnis die Befehlsdaten an die geschützte Funktion übermittelt werden und diese
20 ausgeführt wird und bei fehlender Erlaubnis eine Ausführung der geschützten Funktion verweigert wird.

Der wesentliche Vorteil des erfindungsgemäßen Verfahrens besteht darin, dass eine Überprüfung der Autorisierung des Absenders unabhängig von der Art des Zugriffs auf das elektrische Feldgerät durchgeführt werden kann. Dies wird dadurch erreicht, dass das Feldgerät eine Identifizierungseinrichtung aufweist, die sämtliche Befehlsdaten - unabhängig von der Art und Weise, wie sie zum Feldgerät gelangt sind - einer Absender-
25 der-Identitätsermittlung unterzieht. Das bedeutet also, dass aus den schnittstellenspezifischen oder protokollspezifischen Befehlsdaten von der Datenschnittstelle unabhängige Absendercharakterisierungsdaten ermittelt werden. Im Zusammenspiel mit der Sicherheitseinrichtung des elektrischen Feldgerätes,
30

die anhand der von der Identifizierungseinrichtung getroffenen Absenderidentifizierung ein Ausführen der geschützten Funktion des elektrischen Feldgerätes entweder zulässt oder sperrt, kann eine hohe Sicherheit des Feldgerätes gegen unbefugten Zugriff auf seine geschützten Funktionen erreicht werden.

Eine vorteilhafte Ausführungsform des erfindungsgemäßen Verfahrens besteht darin, dass zur Ermittlung der Absendercharakterisierungsdaten von der Identifizierungseinrichtung den Befehlsdaten zugeordnete, den Absender bezeichnende absenderspezifische Daten an eine Identitätsdatenbank übergeben werden, von der Identitätsdatenbank den absenderspezifischen Daten entsprechende Absendercharakterisierungsdaten ermittelt werden und die ermittelten Absendercharakterisierungsdaten an die Identifizierungseinrichtung zurückgegeben werden.

Absenderspezifische Daten sind in diesem Zusammenhang solche Daten, die mit den Befehlsdaten an das elektrische Feldgerät übermittelt werden und die in irgendeiner Weise einen Rückschluss auf den Absender der Befehlsdaten zulassen. Auf diese Weise kann durch Abprüfung in der Identitätsdatenbank vorhandener Einträge in einfacher Weise der Absender der Befehlsdaten bestimmt werden. Ebenso kann der Benutzer des Feldgerätes auf einfache Weise Änderungen in der Identitätsdatenbank vornehmen, um so Informationen über neue Absender in die Datenbank aufzunehmen oder bestimmten Absendern einzelne geschützte Funktionen freizugeben oder zu sperren.

Eine vorteilhafte Weiterbildung sieht in diesem Zusammenhang vor, dass von der Identitätsdatenbank anhand der absenderspezifischen Daten einen Nutzertyp des Absenders angegebene Typdaten ermittelt und diese als Absendercharakterisierungsdaten an die Identifizierungseinrichtung zurückgegeben werden und

von der Sicherheitseinrichtung anhand dieser Typdaten die Erlaubnis des Absenders zur Ausführung der gesicherten Funktion überprüft wird.

- 5 Typdaten sind in diesem Zusammenhang solche Daten, die nicht den einzelnen, konkreten Absender angeben, sondern eine ihm zugeordnete Gruppe bzw. einen ihm zugeordneten Typ. Durch das Auslesen von Typdaten aus der Identitätsdatenbank muss also nicht der konkrete Absender selbst bestimmt werden. Es ist
10 vielmehr ausreichend, wenn der Absender lediglich pauschal einer Gruppe zugeordnet wird, da üblicherweise bestimmte Gruppen von Personen, die auf das elektrische Feldgerät zugreifen, innerhalb ihrer Gruppe übereinstimmende Zugriffsrechte besitzen. So reicht es beispielsweise aus, die Identität des Absenders als „Parametrierpersonal“ zu erkennen, um
15 die zur Parametrierung notwendigen Funktionen für den Absender freizugeben.

- Eine alternative Weiterbildung dazu sieht vor, dass von der
20 Identitätsdatenbank anhand der absenderspezifischen Daten einen Nutzertyp des Absenders angegebende Typdaten ermittelt werden, von der Identitätsdatenbank anhand der Typdaten dem Nutzertyp des Absenders entsprechende Zugriffsrechtsdaten ermittelt und diese als Absendercharakterisierungsdaten an die
25 Identifizierungseinrichtung zurückgegeben werden, und von der Sicherheitseinrichtung anhand dieser Zugriffsrechtsdaten die Erlaubnis des Absenders zur Ausführung der gesicherten Funktion überprüft wird.

- 30 In diesem Fall muss nicht die Sicherheitseinrichtung selbst eine Zuordnung der Typdaten zu entsprechenden Zugriffsrechtsdaten vornehmen, da dies die Identitätsdatenbank übernimmt.

In diesem Zusammenhang wird es ferner als vorteilhafte Weiterbildung des erfindungsgemäßen Verfahrens angesehen, dass von der Identitätsdatenbank anhand der Typdaten zunächst eine Nutzerrolle des Absenders angegebende Rollendaten ermittelt werden, von der Identitätsdatenbank anhand der ermittelten Rollendaten diesen zugeordnete Zugriffsrechtsdaten ermittelt werden und die ermittelten Zugriffsrechtsdaten als Absendercharakterisierungsdaten an die Identifizierungseinrichtung zurückgegeben werden.

10

Rollendaten sind in diesem Zusammenhang als solche Daten anzusehen, die einen Aufgabenbereich angeben. Durch das Vorsehen von Rollendaten wird zwischen den Typdaten und den Zugriffsrechtsdaten gleichsam eine Zwischenschicht geschaffen, die den Typdaten entsprechende Rollendaten enthält. Beispielsweise können so dem Typ „Parametrierpersonal“ die Rollen „parametrieren“ und „Gerätetest ausführen“ zugeordnet werde. Den jeweiligen Rollendaten sind wiederum verschiedene Zugriffsrechtsdaten zugeordnet. Über das Einfügen dieser Zwischenschicht kann letztendlich eine bequemere Parametrierung der Identitätsdatenbank erfolgen, da die Rollendaten als vor-

eingestellte Aufgabenbereiche bereits herstellerseitig mit den dazu passenden Zugriffsrechtsdaten verknüpft sein können und beim Betreiber des Feldgerätes zur Inbetriebnahme nur noch die gewünschten Typdaten mit entsprechenden Rollendaten verknüpft werden müssen. Hierzu müssen in der Identitätsdatenbank nur vergleichsweise wenige Einstellungen vorgenommen werden.

15

20

25

30

Eine weitere vorteilhafte Weiterbildung des erfindungsgemäßen Verfahrens ist dadurch angegeben, dass bei einer sitzunglosen Kommunikationsverbindung zwischen dem Absender und dem elektrischen Feldgerät die absenderspezifischen Daten eine Absender-Datenverarbeitungseinrichtung angegebende Kennzeich-

nungsdaten enthalten und von der Identitätsdatenbank (4) den Kennzeichnungsdaten die Absendercharakterisierungsdaten zugeordnet werden.

5 Dies ist insbesondere bei Kommunikationsverbindungen über eine Ethernet-Schnittstelle mit einem Sitzungslosen („sessionless“) Kommunikationsprotokoll, wie beispielsweise dem im Internet gebräuchlichen „http“ (Hyper Text Transfer Protocol), von Vorteil. Hier enthalten die absenderspezifischen Daten
10 Kennzeichnungsdaten, die die Absender-Datenverarbeitungseinrichtung charakterisieren. Anhand dieser Kennzeichnungsdaten kann die Identitätsdatenbank nachprüfen, ob der Absender-Datenverarbeitungseinrichtung vertraut wird und welchem Nutzertyp die Absender-Datenverarbeitungseinrichtung zugeordnet
15 ist. So kann ohne großen Aufwand eine Identifizierung der Absender-Datenverarbeitungseinrichtung stattfinden. Beispielsweise können die Kennzeichnungsdaten aus einer MAC-Adresse der Absender-Datenverarbeitungseinrichtung bestehen. Die Identitätsdatenbank erkennt anhand der MAC-Adresse den Nutzertyp des Absenders.
20

Alternativ dazu ist eine weitere vorteilhafte Ausführungsform dadurch gegeben, dass bei einer Sitzungs-basierten Kommunikationsverbindung zwischen dem Absender und dem elektrischen
25 Feldgerät die absenderspezifischen Daten Schlüsseldaten des Absenders enthalten und von der Identitätsdatenbank den Schlüsseldaten die Absendercharakterisierungsdaten zugeordnet werden.

30 Schlüsseldaten sind in diesem Zusammenhang Daten, die einen Codierschlüssel, wie er beispielsweise zur elektronischen Verschlüsselung eingesetzt wird, enthalten. Auf diese Weise kann die Identitätsdatenbank in einfacher Weise bei einer Sitzungs-basierten Kommunikationsverbindung gemäß beispiels-

weise dem https-Protokoll (hyper text transfer protocol secure) anhand von Schlüsseldaten, wie beispielsweise einem öffentlichen Schlüssel des Absenders, eine Identifizierung des Absenders vornehmen.

5

In diesem Zusammenhang wird es außerdem als vorteilhaft angesehen, wenn die Kommunikationsverbindung zwischen einem externen, passiven Datenspeichermodule und dem elektrischen Feldgerät hergestellt wird und die Schlüsseldaten von einem Speicherbereich auf dem externen, passiven Datenspeichermodule an die Identifizierungseinrichtung übertragen werden.

10

Auf diese Weise kann beispielsweise auch eine Kommunikationsverbindung zwischen einem USB-Stick als externem passivem Datenspeichermodule und dem Feldgerät hergestellt werden. Die Schlüsseldaten werden hierbei von dem USB-Stick an die Identifizierungseinrichtung übertragen. Eine Bedienung des Feldgerätes erfolgt in diesem Fall über das lokale Tastenfeld des Feldgerätes, nur die Absendererkennung wird anhand des Schlüssels auf dem USB-Stick vorgenommen.

15

20

Gemäß einer weiteren alternativen Ausführungsform des erfindungsgemäßen Verfahrens kann ferner vorgesehen sein, dass bei einer mittels einer Eingabevorrichtung am Feldgerät aufgebauten Kommunikationsverbindung zwischen dem Absender und dem Feldgerät die absenderspezifischen Daten von dem Absender eingegebene Passwortdaten enthalten. Auf diese Weise kann in einfacher Weise auch eine Identifizierung eines direkt am Gerät arbeitenden Benutzers vorgenommen werden.

25

30

Bezüglich des Feldgerätes wird die oben genannte Aufgabe durch ein elektrisches Feldgerät mit zumindest einer Datenschnittstelle, über die eine Kommunikationsverbindung zum Übertragen von Befehlsdaten zum Ausführen einer gesicherten

Funktion des elektrischen Feldgerätes herstellbar ist, gelöst, bei dem mit der Datenschnittstelle eine Identifizierungseinrichtung in Verbindung steht, wobei die Identifizierungseinrichtung derart ausgebildet ist, dass sie den von der Schnittstelle empfangenen Befehlsdaten einen Absender der Befehlsdaten angegebende Absendercharakterisierungsdaten hinzufügt, und mit der Identifizierungseinrichtung eine Sicherheitseinrichtung in Verbindung steht, wobei die Sicherheitseinrichtung derart ausgebildet ist, dass sie die um die Absendercharakterisierungsdaten erweiterten Befehlsdaten auf eine Erlaubnis überprüft, die gesicherte Funktion des elektrischen Feldgerätes auszuführen, und nur bei bestehender Erlaubnis ein Ausführen der gesicherten Funktion zulässt.

Durch das Zusammenspiel der Identifizierungseinrichtung und der Sicherheitseinrichtung kann hier ein hoher Sicherheitsgrad gegen ungewollte Fremdzugriffe gewährleistet werden.

In diesem Zusammenhang ist eine vorteilhafte Ausführungsform des erfindungsgemäßen elektrischen Feldgerätes dadurch gegeben, dass die Identifizierungseinrichtung eine Identitätsdatenbank aufweist, die derart ausgebildet ist, dass sie anhand von in den Befehlsdaten enthaltenen absenderspezifischen Daten die Absendercharakterisierungsdaten ermittelt. Durch das Vorsehen der Identitätsdatenbank kann eine vergleichsweise flexible und einfache Anpassung der Identifizierungseinrichtung an die Gegebenheiten beim Betreiber des elektrischen Feldgerätes vorgenommen werden.

Eine weitere vorteilhafte Ausführungsform des erfindungsgemäßen elektrischen Feldgerätes sieht schließlich vor, dass die Datenschnittstelle eine Ethernet-Schnittstelle, eine USB-Schnittstelle oder eine serielle Schnittstelle ist. Diese Datenschnittstellen können z. B. nach einem so genannten

Master-Slave-Protokoll, einem Punkt-zu-Punkt-Protokoll (PPP) oder einem netzwerkfähigen Protokoll (IP-basiertes Protokoll) arbeiten. Solche Schnittstellen sind zum Übertragen von elektronischen Kommunikationsdaten im Nah- und Fernbereich besonders weit verbreitet.

Zur weiteren Erläuterung der Erfindung ist in

- Figur 1 in einem schematischen Blockschaltbild ein elektrisches Feldgerät, in
- Figur 2 ein erstes Ausführungsbeispiel einer Identitätsdatenbank, in
- Figur 3 ein zweites Ausführungsbeispiel einer Identitätsdatenbank und in
- Figur 4 ein schematisches Verfahrensfließbild zur Erläuterung einer Identifizierung eines Absenders bei einer sitzungsbasierten Kommunikationsverbindung gezeigt.
- Figur 1 zeigt in schematischer Darstellung ein Blockschaltbild eines elektrischen Feldgerätes 1. Das elektrische Feldgerät 1 kann z. B. Bestandteil einer Automatisierungsanlage zur Steuerung und Regelung der Verteilung elektrischer Energie in einem Energieversorgungsnetz sein. Das Feldgerät 1 weist Datenschnittstellen 2a bis 2e auf, wobei die Datenschnittstelle 2a eine so genannte Mensch-Maschine-Schnittstelle (human-machine-interface = „HMI“) darstellt, also eine lokal an dem elektrischen Feldgerät vorgesehene Eingabevorrichtung wie ein Tastenfeld und eine Ausgabe- bzw. Anzeigevorrichtung wie ein Display. Die Datenschnittstellen 2a - 2e beinhalten hierbei nicht nur die reine physikalische Schnittstelle, sondern auch die informationstechnische Datenanbindung, wie z. B. die der jeweiligen Datenschnittstelle zugeordnete Datenabstraktionsebenen bis zur Schicht 4 des bekann-

ten OSI-Schichtenmoduells („Open Systems Interconnection Reference Model“).

Die Datenschnittstelle 2b ist in Figur 1 als serielle Schnittstelle dargestellt, an die eine serielle Datenübertragungsleitung angeschlossen werden kann. Die Datenschnittstelle 2c ist eine an dem elektrischen Feldgerät vorgesehene USB-Schnittstelle (USB = universal serial bus) zum Anschluss einer USB-Datenübertragungsleitung. Über die serielle Schnittstelle 2b und die USB-Schnittstelle 2c können üblicherweise mittels einer vergleichsweise kurzen Kabelverbindung weitere Geräte, wie beispielsweise ein Laptop, mit dem elektrischen Feldgerät verbunden werden. Hierbei ist die USB-Schnittstelle für eine deutliche höhere Datenübertragungsrate ausgelegt als die serielle Schnittstelle, die beispielsweise nach dem RS 232-Standard arbeitet. Über die USB-Schnittstelle können ferner neben aktiven elektrischen Geräten wie einem Laptop auch passive Datenspeicher, wie beispielsweise ein USB-Stick, an das elektrische Feldgerät angeschlossen werden.

Die Datenschnittstelle 2d stellt eine Datenverbindung zum Anschließen eines Modems dar, wobei ein solches Modem einen Fernzugriff auf das elektrische Feldgerät erlaubt. Prinzipiell kann die Datenschnittstelle 2d als beliebige elektrische Kommunikationsschnittstelle, die ein Anschließen eines Modems erlaubt, ausgelegt sein. Beispielsweise kann es sich bei der Datenschnittstelle 2d auch um eine serielle oder um eine USB-Schnittstelle handeln.

Die Datenschnittstelle 2e stellt schließlich eine Ethernet-Schnittstelle dar, über die das elektrische Feldgerät in ein Datennetzwerk gemäß dem Ethernet-Standard eingebunden werden kann. Hierdurch ist es möglich, das elektrische Feldgerät beispielsweise mit einem Firmen-Intranet oder sogar dem In-

ternet zu verbinden. Auch kann das elektrische Feldgerät 1 über die Ethernet-Schnittstelle 2e in ein Feldgerätenetzwerk beispielsweise gemäß dem internationalen Standard IEC 61850 eingebunden werden.

5

Das elektrische Feldgerät weist ferner eine Identifizierungseinrichtung 3 auf, die mit einer Identitätsdatenbank 4 in Verbindung steht. Die Identifizierungseinrichtung 3 steht weiterhin in Verbindung mit einer Sicherheitseinrichtung 5.

10 Der Sicherheitseinrichtung 5 nachgeordnet sind in höchstschematischer Darstellung unterschiedliche Geräte-Funktionsbausteine 6a bis 6g dargestellt. Diese Funktionsbausteine 6a bis 6g stellen grundlegende Funktionen des elektrischen Feldgerätes 1 dar, beispielsweise eine Lesefunktion eingestellter
15 elektrischer Parameter in dem elektrischen Feldgerät 1 oder eine Schaltfunktion zum Öffnen oder Schließen eines an das elektrische Feldgerät angeschlossenen Leistungsschalters. Üblicherweise werden die Identifizierungseinrichtung 3, die Identitätsdatenbank 4, die Sicherheitseinrichtung 5 und die
20 Geräte-Funktionsbausteine 6a bis 6g nicht als separate elektrische Bausteine in dem elektrischen Feldgerät 1 vorliegen, sondern vielmehr als Programmmodule einer Gerätesoftware ausgebildet sein.

25 Durch das Zusammenspiel der Identifizierungseinrichtung 3, der Identitätsdatenbank 4 und der Sicherheitseinrichtung 5 wird sichergestellt, dass geschützte Funktionen des elektrischen Feldgerätes 1 unabhängig von der elektrischen Datenschnittstelle 2a bis 2e, über die ein Benutzer mit dem
30 elektrischen Feldgerät 1 eine Kommunikationsverbindung aufbaut, nur von autorisierten Benutzern ausgeführt werden können. Dies soll im Folgenden anhand der fünf in Figur 1 beispielhaft dargestellten Datenschnittstellen erläutert werden.

Zunächst wird ein Verfahren zum Ausführen einer geschützten Funktion des elektrischen Feldgerätes 1 betrachtet, wenn der Benutzer des elektrischen Feldgerätes Zugriff auf das elektrische Feldgerät über die lokale Eingabevorrichtung

5 nimmt, also über die Datenschnittstelle 2a. Hierzu verwendet der Benutzer ein an dem elektrischen Feldgerät vorgesehenes Tastenfeld und ein Display, um verschiedene Funktionen des elektrischen Feldgerätes aufzurufen. Diese Funktionen sind üblicherweise zur einfacheren Übersichtlichkeit in so genann-

10 ten Funktionsmenüs angeordnet, wie man sie heutzutage aus verschiedensten Anwendungsprogrammen im Computerbereich kennt. Der Benutzer kann mit Hilfe des Tastenfeldes durch die auf dem Display des elektrischen Feldgerätes angezeigten Funktionsmenüs navigieren und auszuführende Funktionen des

15 elektrischen Feldgerätes auswählen. Wählt der Benutzer eine geschützte Funktion des elektrischen Feldgerätes aus, wie beispielsweise ein Öffnen eines elektrischen Leistungsschalters, so fordert ihn das elektrische Feldgerät auf, ein Passwort einzugeben, das ihn zur Durchführung dieser geschützten

20 Funktion autorisiert. Der Benutzer gibt über das Tastenfeld das entsprechende Passwort ein, das den Befehlsdaten, die den Funktionsaufruf der geschützten Funktion des elektrischen Feldgerätes angeben, als absenderspezifische Daten angefügt wird. Die Identifizierungseinrichtung empfängt die Befehlsda-

25 ten mit den absenderspezifischen Daten in Form der Passwortdaten und übergibt diese Passwortdaten an die Identitätsdatenbank 5. Die Identitätsdatenbank 5 ermittelt anhand der Passwortdaten Absendercharakterisierungsdaten, die den Absender der Befehlsdaten, also den an dem Tastenfeld des elektrischen Feldgerätes tätigen Benutzer, kennzeichnen. Diese Ab-

30 sendercharakterisierungsdaten werden an die Identifizierungseinrichtung 3 zurückgegeben. Die Identifizierungseinrichtung 3 hängt die Absendercharakterisierungsdaten an die Befehlsdaten zum Aufrufen der geschützten Funktion des elektrischen

Feldgerätes 1 an und übermittelt diesen Datensatz an die Sicherheitseinrichtung 5. Die Sicherheitseinrichtung 5 überprüft, ob die mit den Befehlsdaten übermittelten Absendercharakterisierungsdaten ein Ausführen der gewünschten geschützten Funktion des elektrischen Feldgerätes 1 erlauben, in diesem Fall also, ob der an dem elektrischen Feldgerät tätige Benutzer dazu autorisiert ist, den Leistungsschalter zu öffnen. Ermittelt die Sicherheitseinrichtung 5 ein positives Ergebnis, d. h. der Benutzer ist dazu autorisiert, die geschützte Funktion auszuführen, so übermittelt sie den Funktionsaufruf an den entsprechenden Funktionsbaustein mit der gewünschten geschützten Funktion des elektrischen Feldgerätes 1, beispielsweise den Funktionsblock 6d. Daraufhin wird die entsprechende Funktion des elektrischen Feldgerätes 1 ausgeführt. Ermittelt die Sicherheitseinrichtung 5 jedoch, dass die Absendercharakterisierungsdaten ein Ausführen der gewünschten geschützten Funktion des elektrischen Feldgerätes 1 nicht erlauben, d. h. der Benutzer ist nicht autorisiert, die geschützte Funktion des elektrischen Feldgerätes 1 auszuführen, so verweigert sie ein Ausführen der gewünschten geschützten Funktion des elektrischen Feldgerätes 1. In diesem Fall wird der Leistungsschalter über den Funktionsblock 6d folglich nicht geöffnet.

Im zweiten zu betrachtenden Fall wird zwischen dem Benutzer des elektrischen Feldgerätes 1 und dem elektrischen Feldgerät 1 eine Kommunikationsverbindung über die serielle Datenschnittstelle 2b hergestellt. Beispielsweise kann an die serielle Schnittstelle 2b ein serielles Datenkabel angeschlossen sein, das an seinem anderen Ende an eine externe Datenverarbeitungseinrichtung, beispielsweise einen Laptop, angeschlossen ist. Der Benutzer gibt nun nicht mehr lokal am elektrischen Feldgerät 1 über das Tastenfeld Funktionsaufrufe ein, sondern benutzt hierzu den über die serielle Daten-

schnittstelle 2b angeschlossenen Laptop. Beispielsweise kann er über den Laptop einen Funktionsaufruf an das elektrische Feldgerät übermitteln, mit dem bestimmte sicherheitsrelevante Parameter des elektrischen Feldgerätes geändert werden sollen. In diesem Fall würde das Verfahren ähnlich ablaufen wie das oben zur lokalen Datenschnittstelle beschriebene Verfahren. Der Benutzer an dem Laptop würde wiederum zu einer Passworteingabe aufgefordert werden, anhand der seine Identität erkannt werden kann. Mit der Sicherheitseinrichtung 5 kann dann eine Überprüfung stattfinden, ob der Benutzer zur Ausführung der gewünschten geschützten Funktion des elektrischen Feldgerätes 1, hier also dem Ändern der sicherheitsrelevanten Parameter des elektrischen Feldgerätes 1 autorisiert ist. Nur bei positivem Überprüfungsergebnis wird die entsprechende Funktion ausgeführt und die Parametereinstellungen des Gerätes werden geändert.

Analog hierzu könnte ein Laptop bei elektrischen Feldgeräten, die eine USB-Schnittstelle aufweisen, auch über die USB-Schnittstelle 2c mit dem elektrischen Feldgerät verbunden sein und hierüber den Funktionsaufruf zum Ausführen der geschützten Funktion des elektrischen Feldgerätes übermitteln. In diesem Falle würde das Verfahren prinzipiell ebenso ablaufen wie zu der seriellen Schnittstelle beschrieben.

Eine weitere Möglichkeit zum Verwenden der USB-Schnittstelle 2c an dem elektrischen Feldgerät 1 besteht außerdem darin, dass der Benutzer mit dem elektrischen Feldgerät zwar über die lokale Datenschnittstelle, also das Tastenfeld und das Display, eine Kommunikationsverbindung aufbaut, aber zusätzlich ein passives Datenspeichermodule, wie einen USB-Stick, über die USB-Schnittstelle mit dem elektrischen Feldgerät in Verbindung bringt. Der USB-Stick kann hierbei Schlüsseldaten als absenderspezifische Daten enthalten, die anstelle der

Passwortdaten an die Identifizierungseinrichtung 3 übertragen werden. Anhand dieser Schlüsseldaten kann die Identifizierungseinrichtung 3 im Zusammenspiel mit der Identitätsdatenbank 4 die Identität des Absenders bestimmen. Das weitere
5 Verfahren würde jedoch analog ablaufen; die Identitätsdatenbank 4 würde also anhand der absenderspezifischen Daten in Form der Schlüsseldaten Absendercharakterisierungsdaten zur Identifizierung des Absenders der Befehlsdaten ermitteln und diese gemeinsam mit den Befehlsdaten an die Sicherheitseinrichtung 5 übertragen. Diese wiederum überprüft, ob die Absendercharakterisierungsdaten ein Ausführen der gewünschten geschützten Funktion des elektrischen Feldgerätes 1 autorisieren.

15 Über die Datenschnittstelle 2d kann ein Modem mit dem elektrischen Feldgerät 1 verbunden werden, über das ein Fernzugriff auf das elektrische Feldgerät 1 ermöglicht wird. Ein solcher Fernzugriff kann prinzipiell ähnlich erfolgen wie ein lokaler Zugriff auf das elektrische Feldgerät 1 über die serielle Datenschnittstelle 2b oder über die USB-Schnittstelle 2c. In diesem Fall würden wiederum Passwortdaten oder Schlüsseldaten an die Identifizierungseinrichtung 3 als absenderspezifische Daten übermittelt werden. Je nach Art des bei der Kommunikationsverbindung verwendeten Kommunikationsprotokolls
20 können jedoch auch Kennzeichnungsdaten, die eine Absender-Datenverarbeitungseinrichtung kennzeichnen, als anwenderspezifische Daten an die Identifizierungseinrichtung 3 übertragen werden.

30 Dies soll im Zusammenhang mit der Ethernet-Datenschnittstelle 2e des elektrischen Feldgerätes 1 näher erläutert werden. Über die Ethernet-Datenschnittstelle 2e wird üblicherweise ein Fernzugriff auf das elektrische Feldgerät 1 erfolgen. Es ist jedoch auch möglich, eine Absender-Datenverarbeitungsein-

richtung über ein vergleichsweise kurzes Ethernet-Kommunikationskabel lokal mit dem elektrischen Feldgerät zu verbinden. Beim Zugriff auf das elektrische Feldgerät 1 über die Ethernet-Datenschnittstelle 2e sind insbesondere zwei Arten von Kommunikationsverbindungen zu unterscheiden, nämlich die sitzungsbasierte Kommunikationsverbindung und die sitzungslose Kommunikationsverbindung.

Momentan sind die sitzungslosen („session less“) Kommunikationsverbindungen über Ethernet-Schnittstellen noch am weitesten verbreitet. Sie erfolgen beispielsweise gemäß dem aus der Internettechnologie bekannten Kommunikationsprotokoll „http“. Sitzungslos bedeutet in diesem Zusammenhang, dass zwischen dem Absender der Befehlsdaten und dem Empfänger – also dem elektrischen Feldgerät – kein fester Kommunikationskanal etabliert wird. Eine sitzungslose Kommunikationsverbindung lässt sich beispielsweise mit einer Briefsendung vergleichen. Hier werden die Befehlsdaten sozusagen in einen Umschlag verpackt, der an einen Adressaten, in diesem Fall das elektrische Feldgerät, gerichtet ist. Der Adressat wird beispielsweise über eine so genannte IP-Adresse oder eine MAC-Adresse des Empfängergerätes festgelegt. Außerdem sind auf dem Umschlag absenderspezifische Daten in Form von Kennzeichnungsdaten angegeben, die den Absender der Befehlsdaten in dem Umschlag kennzeichnen. Beispielsweise können diese Kennzeichnungsdaten bei einer sitzungslosen Kommunikationsverbindung eine MAC-Adresse der Absender-Datenverarbeitungseinrichtung angeben. Anhand der Kennzeichnungsdaten können die Identifizierungseinrichtung 3 und die Identitätsdatenbank 4 die Identität des Absenders bzw. die Identität der Absender-Datenverarbeitungseinrichtung feststellen. Ist die Absender-Datenverarbeitungseinrichtung als vertrauenswürdig eingestuft (das wäre beispielsweise der Fall, wenn es sich bei der Absender-Datenverarbeitungseinrichtung um eine in der Identität

tätsdatenbank eingetragene Bedienstation in einer Leitwarte zur Steuerung des elektrischen Energieversorgungsnetzes handelt), dann werden entsprechende Absendercharakterisierungsdaten von der Identitätsdatenbank 4 an die Identifizierungseinrichtung 3 übermittelt und die Sicherheitseinrichtung 5 kann anhand dieser Absendercharakterisierungsdaten einen Zugriff auf eine entsprechende geschützte Funktion des elektrischen Feldgerätes zulassen. Werden die Kennzeichnungsdaten der Absender-Datenverarbeitungseinrichtung von der Identitätsdatenbank 4 nicht erkannt oder gelten diese nicht als vertrauenswürdig, so werden keine oder entsprechende andere Absendercharakterisierungsdaten an die Befehlsdaten angehängt und die Sicherheitseinrichtung 5 wird den Zugriff auf die geschützte Funktion des elektrischen Feldgerätes 1 verweigern.

Beim anderen Fall, einer sitzungsbasierten (session based") Kommunikationsverbindung, wird zwischen dem Absender und dem elektrischen Feldgerät 1 ein fester Kommunikationskanal etabliert. Dies ist beispielsweise vergleichbar mit einem Telefonat zwischen zwei Kommunikationspartnern über eine analoge Telefonleitung. Hierbei werden zu Beginn des Kommunikationsaufbaus mit den Befehlsdaten absenderspezifische Daten in Form von Schlüsseldaten übertragen, anhand derer die Identitätsdatenbank 4 die Absendercharakterisierungsdaten zur Identifizierung des Absenders ermitteln kann. Das weitere Verfahren verläuft wie zu den übrigen Datenschnittstellen 2a bis 2d beschrieben.

Anhand der Figuren 2 und 3 soll im Folgenden beschrieben werden, wie die Identitätsdatenbank 4 anhand der absenderspezifischen Daten die Absendercharakterisierungsdaten ermitteln kann.

Hierzu zeigt Figur 2 eine schematische Darstellung der Identitätsdatenbank 4. Über einen eingehenden Pfeil 20, werden die absenderspezifischen Daten von der Identifizierungseinrichtung 3 an die Identitätsdatenbank 4 übertragen. Über
5 einen Dateneingangsport 21 empfängt die Identitätsdatenbank 4 die absenderspezifischen Daten. Gemäß einer in der Identitätsdatenbank 4 abgespeicherten ersten Zuordnungstabelle 22 bestimmt die Identitätsdatenbank 4 den Absender, der von den absenderspezifischen Daten angegeben ist. Dies kann zu einer
10 personengenauen Identifizierung des Absenders führen. In einem solchen Fall muss für jeden möglichen Benutzer des elektrischen Feldgerätes 1 ein Eintrag in der Identitätsdatenbank 4 vorgesehen sein und jeder mögliche Benutzer des elektrischen Feldgerätes muss ihm eigene absenderspezifische
15 Daten besitzen. Üblicherweise ist es jedoch ausreichend, lediglich einen Nutzertyp des Absenders zu bestimmen. Beispielsweise kann ein Nutzertyp „Parametrierpersonal“ des elektrischen Feldgerätes bedeuten. Dem Nutzertyp „Parametrierpersonal“ wären in dem Fall alle Personen zugeordnet,
20 die üblicherweise Parametrieraufgaben des elektrischen Feldgerätes übernehmen dürfen. Andere Möglichkeiten von Nutzertypen sind beispielsweise „Ablesepersonal“, das zwar Messwerte und Einstellungen des elektrischen Feldgerätes ablesen darf, diese jedoch nicht ändern kann, und „Inbetriebsetzungspersonal“, das sämtliche Einstellungen an dem elektrischen Feldgerät ändern darf, aber keine Schalthandlungen mit dem elektrischen Feldgerät vornehmen darf. Hierbei reicht es aus, wenn
25 alle Personen, die zu einem Nutzertyp gehören, dieselben absenderspezifischen Daten an das elektrische Feldgerät mit den Befehlsdaten übermitteln und lediglich anhand eines einzigen
30 Eintrages in der Identitätsdatenbank 4 der Nutzertyp des Absenders bestimmt wird. Eine genauere Identifizierung des Absenders ist - wie oben erwähnt - nicht notwendig. Hierdurch wird insbesondere die in Inbetriebsetzungsphase des elektri-

schen Feldgeräts deutlich verkürzt, da erheblich weniger Einträge in der Identitätsdatenbank 4 vorgenommen werden müssen.

Gemäß dem in Figur 2 dargestellten Beispiel würden also anhand der ersten Zuordnungstabelle 22 den über den Dateneingangsport 21 eintreffenden absenderspezifischen Daten Typdaten, die den Nutzertyp des Absenders angeben, zugeordnet werden. Diesen Typdaten ordnet die Identitätsdatenbank gemäß einer zweiten Zuordnungstabelle 23 die für diesen Nutzertyp erlaubten Zugriffsrechtsdaten zu. Die Zugriffsrechtsdaten geben jeweils diejenigen Gerätefunktionen des elektrischen Feldgerätes 1 an, die der jeweilige Nutzertyp durchführen darf. Beispielsweise wären dem Nutzertyp „Parametrierpersonal“ Zugriffsrechtsdaten zuzuordnen, die Gerätefunktionen wie „Auslesen von Geräteparametern“, „Ändern von Geräteparametern“, „Speichern von Geräteparametern“, „Testen von Geräteparametern“ entsprechen. Einem Benutzertyp-„Betriebspersonal“ wären beispielsweise Zugriffsrechtsdaten für die Gerätefunktionen, „Schalthandlung (Öffnen) am Leistungsschalter vornehmen“ und „Schalthandlung (Schließen) am Leistungsschalter vornehmen“ vorgesehen.

Die gemäß der zweiten Zuordnungstabelle 23 ermittelten Zugriffsrechtsdaten werden über einen Datenausgangsport 24 entlang des Pfeils 25 an die Identifizierungseinrichtung 3 zurückgegeben. Anhand dieser Zugriffsrechtsdaten kann die Sicherheitseinrichtung 5, die der Identifizierungseinrichtung 3 nachgeschaltet ist, die Überprüfung bezüglich der Autorisierung zur Durchführung der geschützten Funktion durchführen.

Zu erwähnen sei bei dem Beispiel gemäß Figur 2 noch, dass auch die Möglichkeit besteht, dass anhand der Identitätsdatenbank lediglich anhand der ersten Zuordnungstabelle 22 den Nutzertyp angegebende Typdaten bestimmt werden und diese Typda-

ten über den Datenausgangsport 24 an die Identifizierungseinrichtung 3 und die Sicherheitseinrichtung 5 übergeben werden. In diesem Fall müsste die Sicherheitseinrichtung 5 eine Zuordnungstabelle entsprechend der zweiten Zuordnungstabelle 23 aufweisen, die den ermittelten Typdaten die entsprechenden Zugriffsrechtsdaten zuordnet.

Figur 3 zeigt eine zu Figur 2 alternative Möglichkeit, wie mit der Identitätsdatenbank die Absendercharakterisierungsdaten bestimmt werden können. Figur 3 entspricht im Wesentlichen der Figur 2. Daher sind auch die übereinstimmenden Komponenten der Figuren 2 und 3 mit den gleichen Bezugszeichen gekennzeichnet. Analog zu Figur 2 werden von der Identifizierungseinrichtung 3 entlang des Pfeils 20 an die Identitätsdatenbank 4 die absenderspezifischen Daten übertragen. Diese werden von der Identitätsdatenbank 4 mit dem Eingangsdatenport 21 empfangen. Anhand der ersten Zuordnungstabelle 22 werden den absenderspezifischen Daten den Nutzertyp des Absenders angegebene Typdaten zugeordnet.

Diesen Typdaten werden nun jedoch in einer zwischengeschalteten Zuordnungstabelle 26 zunächst Rollendaten zugeordnet. Rollendaten geben die von dem entsprechenden Nutzertyp üblicherweise dargestellten Nutzerrollen an. Mit anderen Worten geben die Rollendaten die von dem entsprechenden Nutzertyp üblicherweise durchzuführenden Aufgabenbereiche an. So können beispielsweise dem Nutzertyp „Parametrierpersonal“ die Aufgabenbereiche „Parametrieren“ und „Testen“ zugeordnet sein. Dem Nutzertyp „Bedienpersonal“ wären beispielsweise die Rollendaten „Schalthandlung durchführen“ und „Messwerte auslesen“ zugeordnet. Erst diesen so ermittelten Rollendaten werden die feiner granulierten Zugriffsrechtsdaten anhand der zweiten Zuordnungstabelle 23 zugeordnet. Den Rollendaten „Schalthandlung durchführen“ wären beispielsweise die Zugriffsrechtsda-

ten „Schalthandlung (Öffnen) des Leistungsschalters durchführen“ und „Schalthandlung (Schließen) des Leistungsschalters durchführen“ zugeordnet.

5 Die auf diese Weise ermittelten Zugriffsrechtsdaten werden als Absendercharakterisierungsdaten analog wie bei Figur 2 über den Datenausgangsport 24 der Identitätsdatenbank 4 an die Identifizierungseinrichtung 3 übertragen. Der Vorteil des Ausführungsbeispiels gemäß Figur 3 liegt darin, dass bereits
10 vom Hersteller des elektrischen Feldgerätes eine weitgehende Vorkonfigurierung der Identitätsdatenbank 4 vorgenommen werden kann. So können nämlich allen Gerätefunktionen bereits entsprechende Zugriffsrechtsdaten zugeordnet werden, die wiederum anhand der zweiten Zuordnungstabelle 23 in entsprechende
15 Aufgabenbereiche aufgeteilt und damit den entsprechenden Rollendaten zugeordnet werden. Mit dem Betreiber des elektrischen Feldgerätes müssen letztendlich nur noch entsprechende Nutzertypen vereinbart werden und diesen Nutzertypen gemäß der zwischengeschalteten Zuordnungstabelle 26 entsprechende
20 Rollendaten zugeordnet werden. Hierdurch wird die Konfigurierungsphase beim Betreiber des elektrischen Feldgerätes merklich verkürzt. Da solche Konfigurierungsphasen üblicherweise mit einem sehr großen Aufwand verbunden sind, können durch die herstellerseitige Vorkonfigurierung erhebliche
25 Kosten eingespart werden.

Anhand von Figur 4 soll schließlich erläutert werden, wie bei einer sitzungsbasierten Kommunikationsverbindung die Identität des Absenders ermittelt werden kann. Hierzu werden so ge-
30 nannte Zertifikate verwendet, die eine Signatur der Befehlsdaten ermöglichen. Beispielsweise kann das aus der elektronischen Verschlüsselungstechnik bekannte Zertifikat X.509 in der momentan aktuellen Version 3 oder einer höheren Version verwendet werden. Das Zertifikat enthält in diesem Fall drei

Schlüssel: ein Schlüsselpaar des Benutzers, bestehend aus einem auch dem Feldgerät bekannten öffentlichen Schlüssel des Benutzers und einem - nur dem Benutzer bekannten - privaten Schlüssel des Benutzers und einen öffentlichen Zertifikats-
5 schlüssel zum Angeben der Echtheit des Zertifikats.

Zunächst prüft das elektrische Feldgerät anhand eines öffentlichen Zertifikatsschlüssels, der mit den Befehlsdaten übermittelt wird, ob dieser von derselben Zertifizierungsstelle
10 ausgestellt worden ist ein in dem elektrischen Feldgerät vorgesehenes Zertifikat. Anhand dieses öffentlichen Zertifikatsschlüssels wird geprüft, ob der Absender von der für das Feldgerät 1 (oder eine gesamte Automatisierungsanlage, deren Bestandteil Feldgerät 1 ist) vorgegebenen Zertifizierungs-
15 stelle beglaubigt wurde, also als vertrauenswürdig einzustufen ist. Ist der Absender hierbei als vertrauenswürdig erkannt worden, wird überprüft, ob der Absender tatsächlich mit dem Zertifikats-Inhaber identisch ist. Dazu wird der dem Absender zugeordnete öffentliche Schlüssel des Zertifikats ver-
20 wendet. Hierzu benötigt der Absender den nur dem Zertifikats-Inhaber zugänglichen privaten Zertifikats-Schlüssel für das Zertifikat. Der Absender wird daher aufgefordert, einen beliebigen Text, z. B. eine Zufallszeichenfolge, mit seinem privaten Zertifikats-Schlüssel zu signieren. Die Gültigkeit
25 dieser Signatur kann dann mit dem öffentlichen Schlüssel des Zertifikats überprüft werden.

Diese Vorgehensweise wird im Folgenden anhand von Figur 4 näher erläutert:

30

Zur sicheren Identifizierung des Absenders der Befehlsdaten und zum Ausbilden eines gesicherten Kommunikationskanals wird das in Figur 4 dargestellte Verfahren durchgeführt. Hierbei stellt ein erster Kasten 41 die Vorgänge in dem elektrischen

Feldgerät und ein zweiter Kasten 42 die Vorgänge auf Seiten der Absender-Datenverarbeitungseinrichtung beim Benutzer des elektrischen Feldgerätes dar.

5 In einem ersten Schritt 43 wird hierbei vom elektrischen Feldgerät eine Zufallszeichenfolge RND erzeugt und mit einem öffentlichen Schlüssel des Benutzers des Feldgerätes verschlüsselt. Dies erfolgt in Schritt 44. In Schritt 45 liegt die verschlüsselte Zufallszeichenfolge RND im elektrischen
10 Feldgerät vor. Sie wird, wie durch den Pfeil 46 angedeutet, an die Absender-Datenverarbeitungseinrichtung übertragen. In Schritt 47 liegt die verschlüsselte Zufallszeichenfolge auf der Absender-Datenverarbeitungseinrichtung des Benutzers vor und wird in Schritt 48 mit Hilfe des zu dem öffentlichen
15 Schlüssel des elektrischen Benutzers gehörenden privaten Schlüssels, der auf der Absender-Datenverarbeitungseinrichtung hinterlegt ist, entschlüsselt. Hierzu ist eine Eingabe einer Code-Zeichenfolge vom Benutzer der Absender-Datenverarbeitungseinrichtung erforderlich. Dies ist im Schritt 51 an-
20 gedeutet. Durch die Eingabe der Code-Zeichenfolge oder auch PIN (PIN = personal identity number) wird sozusagen die Verwendung des privaten Schlüssels des Benutzers aktiviert. In Schritt 49 liegt die nunmehr entschlüsselte Zufallszeichenfolge RND in der Absender-Datenverarbeitungseinrichtung vor.

25

Diese wird nun unter Zuhilfenahme des öffentlichen Schlüssels des elektrischen Feldgerätes, der dem Benutzer bekannt oder beispielsweise mit den Befehlsdaten übermittelt worden ist, in Schritt 50 erneut verschlüsselt. Die Zufallszeichenfolge
30 RND liegt in Schritt 52 in erneut verschlüsselter Form auf der Absender-Datenverarbeitungseinrichtung vor.

In Schritt 53 wird diese erneut verschlüsselte Zufallszeichenfolge RND an das elektrische Feldgerät zurück übertragen

und liegt in Schritt 54 auf dem elektrischen Feldgerät vor.
In Schritt 55 erfolgt eine Entschlüsselung der Zufallszeichenfolge unter Verwendung des privaten Schlüssels des Feldgerätes. Schließlich liegt die Zufallszeichenfolge in Schritt
5 56 wieder in entschlüsselter Form auf dem elektrischen Feldgerät vor und kann mit der Ausgangszufallszeichenfolge gemäß Schritt 43 verglichen werden. Stimmen beide Zufallszeichenfolgen überein, so ist der Absender eindeutig identifiziert und eine gesicherte Kommunikationsverbindung zwischen dem
10 elektrischen Feldgerät und dem Benutzer etabliert worden. Zur Verschlüsselung der zwischen dem Absender und dem elektrischen Feldgerät ausgetauschten Daten kann die Zufallszeichenfolge verwendet werden.

15 Das elektrische Feldgerät hat nunmehr anhand des öffentlichen Zertifikatsschlüssels des Benutzers, der mit den Befehlsdaten übertragen wird, die Identität des Benutzers bestimmt und anhand der nachgeschalteten Überprüfung mittels der Zufallszeichenfolge verifiziert. Das weitere Verfahren verläuft analog
20 zu der oben beschriebenen Verfahrensweise.

Schließlich sei noch zu erwähnen, dass das Zertifikat mit den entsprechenden Schlüsseln des Benutzers anstelle auf einer Absender-Datenverarbeitungseinrichtung auch beispielsweise
25 auf einem USB-Stick des Benutzers vorliegen kann, der über die USB-Schnittstelle mit dem elektrischen Feldgerät verbunden ist. In diesem Fall würde der Benutzer, wie bereits weiter oben erwähnt, über die lokale Eingabevorrichtung und das Display am elektrischen Feldgerät eine Kommunikationsverbin-
30 dung mit dem elektrischen Feldgerät aufbauen. Anstelle der Eingabe von Passwortdaten würde das elektrische Feldgerät aber das Zertifikat auf dem USB-Stick abfragen und es würde sozusagen zwischen dem elektrischen Feldgerät und dem Benutzer unter Verwendung des auf dem USB-Stick gespeicherten Zer-

tifikates analog zu den in Figur 4 dargestellten und oben erläuterten Verfahren eine gesicherte Kommunikationsverbindung aufgebaut werden. Die PIN-Eingabe zur Aktivierung des privaten Schlüssels gemäß Schritt 51 würde in diesem Fall auch direkt über die Eingabetastatur am elektrischen Feldgerät vom Benutzer vorgenommen werden. Dies hat den Vorteil, dass der Benutzer nicht verschiedene Passwortdaten im Gedächtnis behalten muss, sondern lediglich das zu dem entsprechenden USB-Stick gehörende Codierzeichenfolge oder PIN.

Patentansprüche

1. Verfahren zum Ausführen einer geschützten Funktion eines elektrischen Feldgerätes (1), bei dem folgende Schritte

5 durchgeführt werden:

- von dem elektrischen Feldgerät (1) werden Befehlsdaten empfangen, die einen Funktionsaufruf zum Ausführen einer geschützten Funktion des elektrischen Feldgerätes (1) angeben;

10 - von einer Identifizierungseinrichtung (3) des elektrischen Feldgerätes (1) werden den jeweiligen Absender der Befehlsdaten charakterisierende Absendercharakterisierungsdaten ermittelt und an die Befehlsdaten angefügt;

15 - von einer Sicherheitseinrichtung (5) werden die um die Absendercharakterisierungsdaten erweiterten Befehlsdaten empfangen und daraufhin überprüft, ob sie eine Ausführung der von den Befehlsdaten angegebenen geschützten Funktion des elektrischen Feldgerätes (1) erlauben, wobei

20 - bei bestehender Erlaubnis die Befehlsdaten an die geschützte Funktion übermittelt werden und diese ausgeführt wird und

- bei fehlender Erlaubnis eine Ausführung der geschützten Funktion verweigert wird.

2. Verfahren nach Anspruch 1,

25 d a d u r c h g e k e n n z e i c h n e t, dass zur Ermittlung der Absendercharakterisierungsdaten

- von der Identifizierungseinrichtung (3) den Befehlsdaten zugeordnete, den Absender bezeichnende absenderspezifische Daten an eine Identitätsdatenbank (4) übergeben werden,

30 - von der Identitätsdatenbank (4) den absenderspezifischen Daten entsprechende Absendercharakterisierungsdaten ermittelt werden und

- die ermittelten Absendercharakterisierungsdaten an die Identifizierungseinrichtung (3) zurückgegeben werden.

3. Verfahren nach Anspruch 2,

d a d u r c h g e k e n n z e i c h n e t, dass

- von der Identitätsdatenbank (4) anhand der absenderspezifischen Daten einen Nutzertyp des Absenders angegebende Typdaten ermittelt und diese als Absendercharakterisierungsdaten an die Identifizierungseinrichtung (3) zurückgegeben werden und
- von der Sicherheitseinrichtung (5) anhand dieser Typdaten die Erlaubnis des Absenders zur Ausführung der gesicherten Funktion überprüft wird.

4. Verfahren nach Anspruch 2,

d a d u r c h g e k e n n z e i c h n e t, dass

- von der Identitätsdatenbank (4) anhand der absenderspezifischen Daten einen Nutzertyp des Absenders angegebende Typdaten ermittelt werden,
- von der Identitätsdatenbank (4) anhand der Typdaten dem Nutzertyp des Absenders entsprechende Zugriffsrechtsdaten ermittelt und diese als Absendercharakterisierungsdaten an die Identifizierungseinrichtung (3) zurückgegeben werden, und
- von der Sicherheitseinrichtung (5) anhand dieser Zugriffsrechtsdaten die Erlaubnis des Absenders zur Ausführung der gesicherten Funktion überprüft wird.

5. Verfahren nach Anspruch 4,

d a d u r c h g e k e n n z e i c h n e t, dass

- von der Identitätsdatenbank (4) anhand der Typdaten zunächst eine Nutzerrolle des Absenders angegebende Rollendaten ermittelt werden,

- von der Identitätsdatenbank (4) anhand der ermittelten Rollendaten diesen zugeordnete Zugriffsrechtsdaten ermittelt werden und

- die ermittelten Zugriffsrechtsdaten als Absendercharakterisierungsdaten an die Identifizierungseinrichtung (3) zurückgegeben werden.

- 5 6. Verfahren nach einem der Ansprüche 2 bis 5,
d a d u r c h g e k e n n z e i c h n e t, dass
- bei einer sitzungslosen Kommunikationsverbindung zwischen dem Absender und dem elektrischen Feldgerät (1) die absenderspezifischen Daten eine Absender-Datenverarbeitungseinrichtung angegebende Kennzeichnungsdaten enthalten und
10 - von der Identitätsdatenbank (4) den Kennzeichnungsdaten die Absendercharakterisierungsdaten zugeordnet werden.

7. Verfahren nach Anspruch 6,
15 d a d u r c h g e k e n n z e i c h n e t, dass
- als Kennzeichnungsdaten eine MAC-Adresse der Absender-Datenverarbeitungseinrichtung verwendet wird.

8. Verfahren nach einem der Ansprüche 2 bis 5,
20 d a d u r c h g e k e n n z e i c h n e t, dass
- bei einer sitzungsbasierten Kommunikationsverbindung zwischen dem Absender und dem elektrischen Feldgerät (1) die absenderspezifischen Daten Schlüsseldaten des Absenders enthalten und
25 - von der Identitätsdatenbank (4) den Schlüsseldaten die Absendercharakterisierungsdaten zugeordnet werden.

9. Verfahren nach Anspruch 8,
d a d u r c h g e k e n n z e i c h n e t, dass
30 - die Kommunikationsverbindung zwischen einem externen, passiven Datenspeichermodule und dem elektrischen Feldgerät (1) hergestellt wird und

- die Schlüsseldaten von einem Speicherbereich auf dem externen, passiven Datenspeichermodul an die Identifizierungseinrichtung (3) übertragen werden.

5 10. Verfahren nach einem der Ansprüche 2 bis 5,
d a d u r c h g e k e n n z e i c h n e t, dass
- bei einer mittels einer Eingabevorrichtung am elektrischen
Feldgerät (1) aufgebauten Kommunikationsverbindung zwischen
dem Absender und dem Feldgerät (1) die absenderspezifischen
10 Daten von dem Absender eingegebene Passwortdaten enthalten.

11. Elektrisches Feldgerät (1) mit zumindest einer Datenschnittstelle (2a,2b,2c,2d,2e), über die eine Kommunikationsverbindung zum Übertragen von Befehlsdaten zum Ausführen
15 einer gesicherten Funktion des elektrischen Feldgerätes (1) herstellbar ist,
d a d u r c h g e k e n n z e i c h n e t, dass
- mit der Datenschnittstelle (2a,2b,2c,2d,2e) eine Identifizierungseinrichtung (3) in Verbindung steht, wobei die Identifizierungseinrichtung (3) derart ausgebildet ist, dass sie
20 den von der Datenschnittstelle (2a,2b,2c,2d,2e) empfangenen Befehlsdaten einen Absender der Befehlsdaten charakterisierende Absendercharakterisierungsdaten hinzufügt, und
- mit der Identifizierungseinrichtung (3) eine Sicherheitseinrichtung (5) in Verbindung steht, wobei die Sicherheitseinrichtung (5) derart ausgebildet ist, dass sie die um die Absendercharakterisierungsdaten erweiterten Befehlsdaten auf eine Erlaubnis überprüft, die gesicherte Funktion des
25 elektrischen Feldgerätes (1) auszuführen, und nur bei bestehender Erlaubnis ein Ausführen der gesicherten Funktion zulässt.
30

12. Elektrisches Feldgerät (1) nach Anspruch 11,
d a d u r c h g e k e n n z e i c h n e t, dass

- die Identifizierungseinrichtung (3) eine Identitätsdatenbank (4) aufweist, die derart ausgebildet ist, dass sie anhand von in den Befehlsdaten enthaltenen absenderspezifischen Daten die Absendercharakterisierungsdaten ermittelt.

5

13. Elektrisches Feldgerät (1) nach Anspruch 11 oder 12,
d a d u r c h g e k e n n z e i c h n e t, dass
- die Datenschnittstelle (2c,2e) eine Ethernet-Schnittstelle,
eine USB-Schnittstelle oder eine serielle Schnittstelle ist.

10

FIG 1

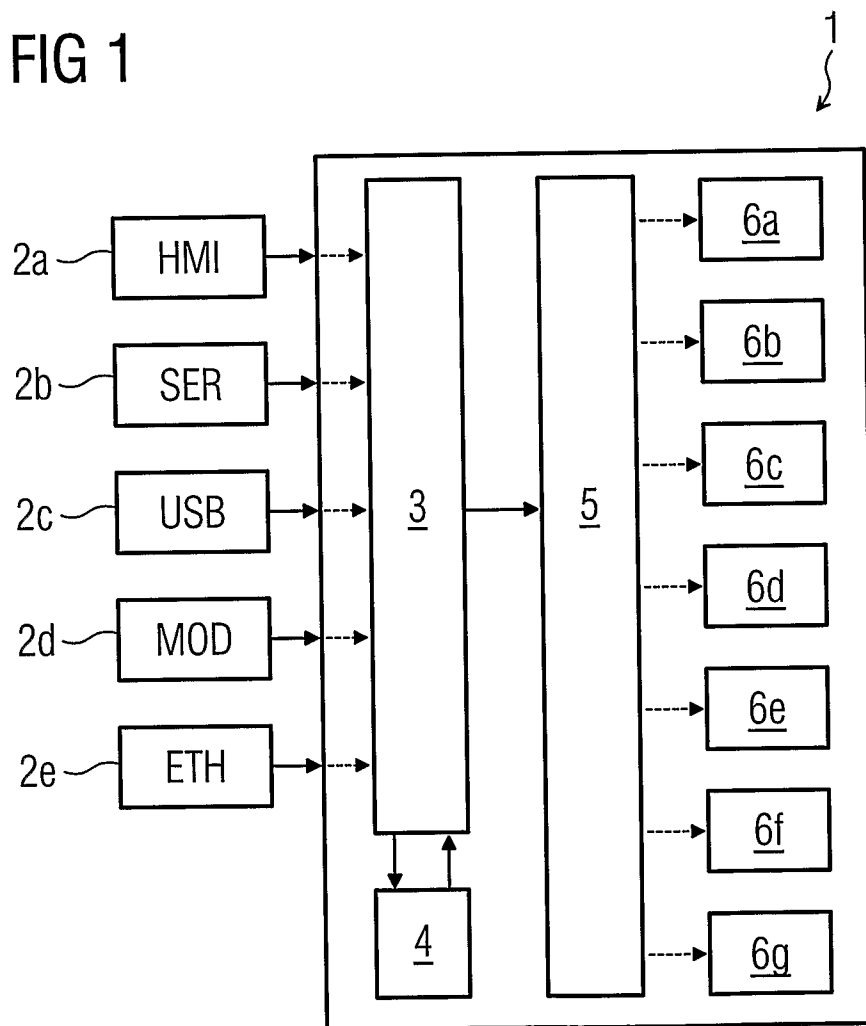


FIG 2

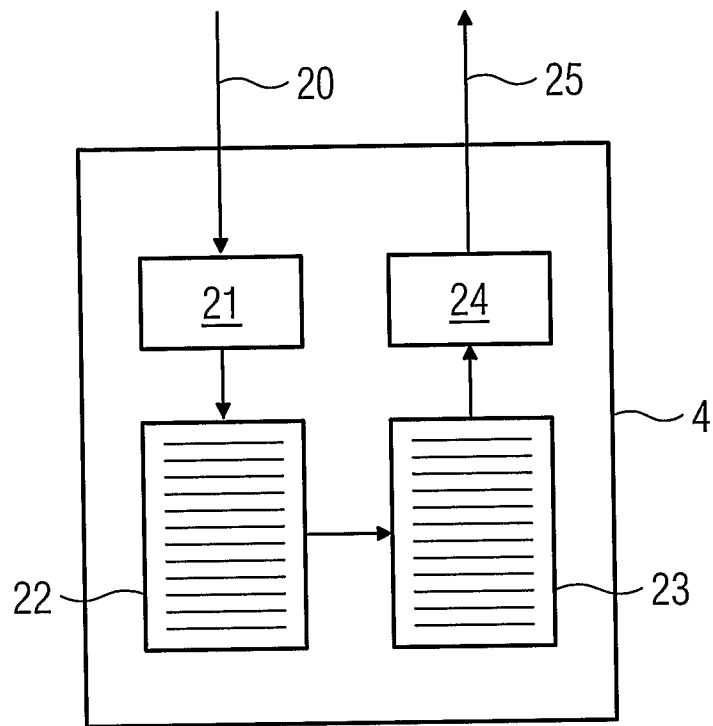


FIG 3

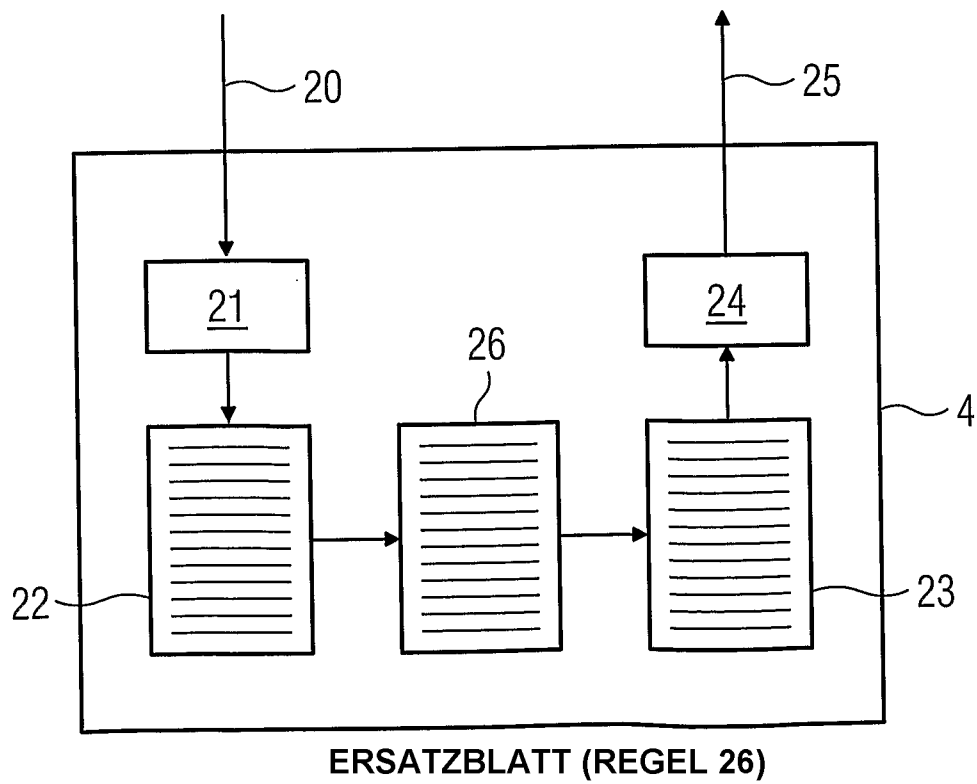
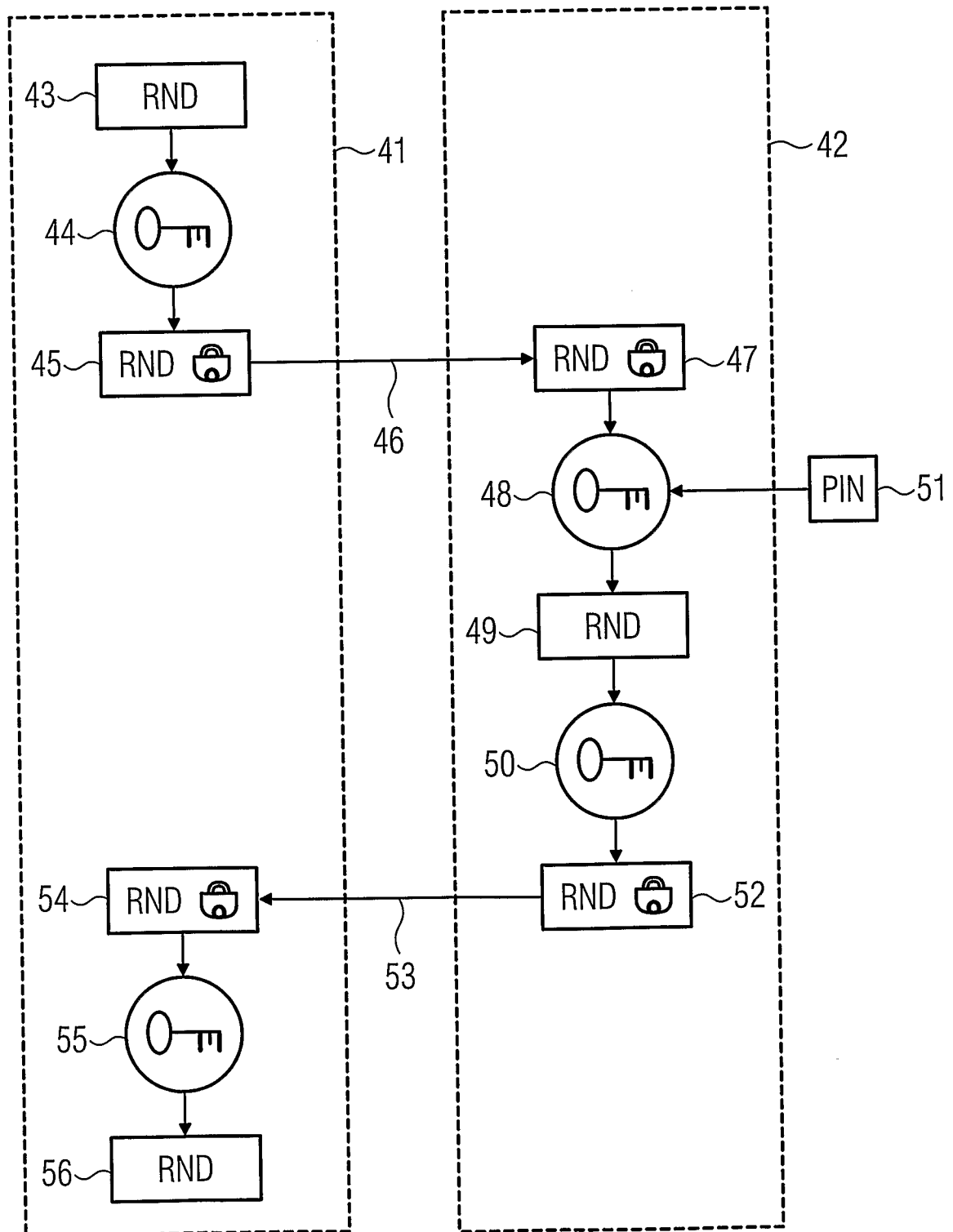


FIG 4



INTERNATIONAL SEARCH REPORT

International application No

PCT/DE2005/001751

A. CLASSIFICATION OF SUBJECT MATTER
INV. G05B19/042

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G05B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	GB 2 368 701 A (* FISHER-ROSEMOUNT SYSTEMS, INC) 8 May 2002 (2002-05-08) figure 1 page 4, line 3 - page 5, line 5 page 14, line 24 - page 15, line 4 page 18, line 9 - page 19, line 21 page 20, line 12 - line 30 page 21, line 25 - page 22, line 2 page 9, line 11 - line 29	1-5, 8, 9, 11-13
Y	-----	6, 7
X	US 2004/107025 A1 (RANSOM DOUGLAS S ET AL) 3 June 2004 (2004-06-03) paragraph [0071]	1, 2, 8, 11, 12
X	DE 198 12 424 A1 (MOELLER GMBH) 23 September 1999 (1999-09-23) column 2, line 22 - line 35 column 3, line 7 - line 30	1, 2, 10-12
	----- -/--	

☒ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

T later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

X document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

Y document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

& document member of the same patent family

Date of the actual completion of the international search

7 June 2006

Date of mailing of the international search report

19/06/2006

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Hasubek, B

INTERNATIONAL SEARCH REPORT

International application No
PCT/DE2005/001751

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2003/182396 A1 (REICH DANIEL ET AL) 25 September 2003 (2003-09-25) paragraph [0042] figure 7 -----	6,7

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/DE2005/001751

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
GB 2368701	A	08-05-2002	DE 10128829 A1 25-04-2002 JP 2002099512 A 05-04-2002
US 2004107025	A1	03-06-2004	NONE
DE 19812424	A1	23-09-1999	NONE
US 2003182396	A1	25-09-2003	NONE

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/DE2005/001751

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. G05B19/042

Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
G05B

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

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EPO-Internal, WPI Data, PAJ

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	GB 2 368 701 A (* FISHER-ROSEMOUNT SYSTEMS, INC) 8. Mai 2002 (2002-05-08) Abbildung 1 Seite 4, Zeile 3 - Seite 5, Zeile 5 Seite 14, Zeile 24 - Seite 15, Zeile 4 Seite 18, Zeile 9 - Seite 19, Zeile 21 Seite 20, Zeile 12 - Zeile 30 Seite 21, Zeile 25 - Seite 22, Zeile 2	1-5, 8, 9, 11-13
Y	Seite 9, Zeile 11 - Zeile 29 -----	6, 7
X	US 2004/107025 A1 (RANSOM DOUGLAS S ET AL) 3. Juni 2004 (2004-06-03) Absatz [0071] -----	1, 2, 8, 11, 12
X	DE 198 12 424 A1 (MOELLER GMBH) 23. September 1999 (1999-09-23) Spalte 2, Zeile 22 - Zeile 35 Spalte 3, Zeile 7 - Zeile 30 ----- -/-	1, 2, 10-12

☒ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen ☒ Siehe Anhang Patentfamilie

- * Besondere Kategorien von angegebenen Veröffentlichungen :
- *A* Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
 - *E* älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
 - *L* Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
 - *O* Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
 - *P* Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
 - *T* Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
 - *X* Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
 - *Y* Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
 - *Z* Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

7. Juni 2006

Absendedatum des internationalen Recherchenberichts

19/06/2006

Name und Postanschrift der Internationalen Recherchenbehörde
Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Hasubek, B

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/DE2005/001751

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	US 2003/182396 A1 (REICH DANIEL ET AL) 25. September 2003 (2003-09-25) Absatz [0042] Abbildung 7 -----	6,7

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/DE2005/001751

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
GB 2368701	A	08-05-2002	DE	10128829 A1	25-04-2002
			JP	2002099512 A	05-04-2002
US 2004107025	A1	03-06-2004	KEINE		
DE 19812424	A1	23-09-1999	KEINE		
US 2003182396	A1	25-09-2003	KEINE		