(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 1 942 466 A2**

(12) **EUROPÄISCHE PATENTANMELDUNG**

(43) Veröffentlichungstag:
09.07.2008 Patentblatt 2008/28

(51) Int Cl.:
G07C 9/00 *(2006.01)*

(21) Anmeldenummer: **07024728.3**

(22) Anmeldetag: **20.12.2007**

(84) Benannte Vertragsstaaten:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC MT NL PL PT RO SE SI SK TR
Benannte Erstreckungsstaaten:
AL BA HR MK RS

(30) Priorität: **27.12.2006 DE 102006062306**

(71) Anmelder: **ASTRA Gesellschaft für Asset Management mbH & Co. KG**
30890 Barsinghausen (DE)

(72) Erfinder:
- **Stobbe, Anatoli**
  30890 Barsinghausen (DE)
- **Gries, Thomas**
  30890 Barsinghausen (DE)

(74) Vertreter: **Körner, Peter**
Thömen & Körner
Zeppelinstrasse 5
30175 Hannover (DE)

(54) **Zugangs-, Überwachungs- und Kommunikationseinrichtung sowie Zugangs-, Überwachungs- und Kommunikationsverfahren**

(57) Es wird eine Zugangs-, Überwachungs- und Kommunikationseinrichtung für wenigstens einen geschützten örtlichen Bereich von Gebäuden, Räumen oder Grundstücken beschrieben. Die Einrichtung umfasst wenigstens ein Hauptgerät, wobei das Hauptgerät als Komponenten einen Bildschirm, eine Kamera, einen Lautsprecher, ein Mikrofon, wenigstens eine Funktionstaste, ein Steuergerät, einen Speicher und ein Signal- und Datenübertragungsgerät mit einer Netzwerkschnittstelle zur Signalübertragung zu und von wenigstens einer Gegenstelle über ein IP-Netzwerk umfasst.

Das Hauptgerät umfasst als zusätzliche Komponente ein Lesegerät zum Lesen von auf Identifikationskarten gespeicherten Ausweisnummern als Bestandteil von Identifikationsmerkmalen.

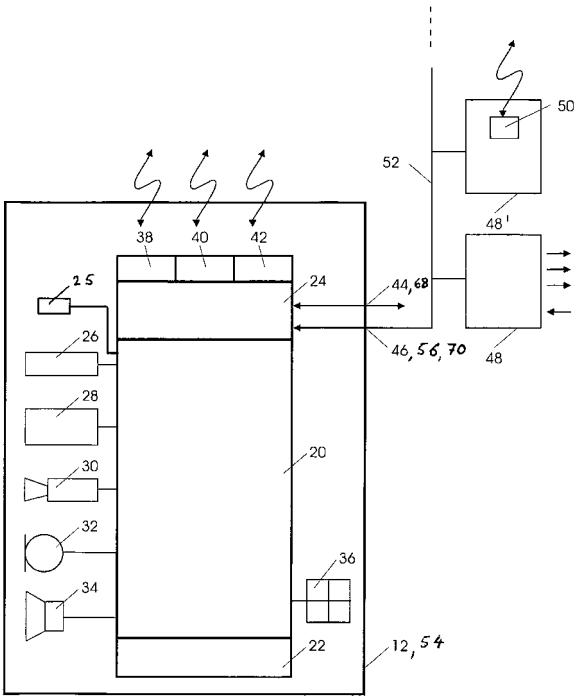

Fig.2

EP 1 942 466 A2

Beschreibung

[0001] Die Erfindung betrifft eine Zugangs-, Überwachungs- und Kommunikationseinrichtung nach dem Oberbegriff des Anspruchs 1.

[0002] Derartige Einrichtungen werden eingesetzt, um den Zugang und Aufenthalt von Personen zu bzw. in sicherheitsrelevanten Bereichen zu gewähren, zu sperren oder zu überwachen sowie die sicherheitsrelevanten Bereiche auch selbst zu überwachen.

[0003] Eine bekannte Einrichtung umfasst ein Terminal mit einem Bildschirm, einem Lautsprecher, einem Mikrofon, einer Ruftaste und/oder Tastatur und einem Türöffnertreiber. Optional kann auch eine externe Kamera an das Terminal angeschlossen werden.

[0004] Das Terminal und ggf. weitere Terminals sind mit einer Zentrale verbunden, die eine Signal- und Datenverbindung zwischen anderen Terminals herstellt. Auch eine Netzwerkschnittstelle zur Signal- und Datenübertragung zu einem weitern Terminal ist erwähnt.

[0005] Der Erfindung liegt die Aufgabe zugrunde, eine Zugangs-, Überwachungs- und Kommunikationseinrichtung zu schaffen, die neben einer Ausweisnummer auch weitere personenspezifischen Daten erfassen und ohne Umweg über eine Zentrale, d. h. direkt über ein Netzwerk mit einer Gegenstelle kommunizieren und Daten austauschen kann.

[0006] Diese Aufgabe wird bei einer Zugangs-, Überwachungs- und Kommunikationseinrichtung nach dem Oberbegriff des Anspruchs 1 durch die Merkmale dieses Anspruchs gelöst.

[0007] Weiterbildungen und vorteilhafte Ausgestaltungen ergeben sich aus den zugeordneten Unteransprüchen.

[0008] Nachfolgend werden in der Beschreibung und den Ansprüchen verwendete Begriffe definiert:

[0009] Ausweisnummer ist eine auf einer Identifikationskarte elektronisch gespeicherte und elektronisch lesbare Nummer, die einer Person oder einem Nutzer zugeordnet sind.

[0010] Biometrische Merkmale sind von einem Lesegerät gelesene biometrische Merkmale einer Person, wie Fingerabdrücke, Irisbild, Gesichtsbild, die einer Ausweisnummer zugeordnet ist.

[0011] Eine PIN ist eine geheime, nur einer Person bekannte Zeichenfolge, die über eine Tastatur manuell eingegeben wird und einer Ausweisnummer zugeordnet ist.

[0012] Identifikationsmerkmale sind einzelne oder logisch verknüpfte Merkmale aus der Menge gelesenen Ausweisnummer, gelesene biometrische Merkmale, eingegebene PIN.

[0013] Identifikationsmerkmale sind in einem Speicher eines Haupt- und/oder Nebengerätes und/oder Servers zum Vergleich mit Identifikationsmerkmalen abgelegte Daten.

[0014] Zugangsprofil ist eine einer Person zugeordnete Liste von zugänglichen und/oder gesperrten Bereichen und Zugangstüren zu diesen Bereichen.

[0015] Zeitprofil ist eine einer Person zugeordnete Liste von zeitlichen Abschnitten, wie Uhrzeit, Wochenplan und Datum, in denen für sich oder in Verbindung mit dem Zugangsprofil ein Zugang erlaubt oder ein Zugangsbegehren abgewiesen wird.

[0016] Zugangsdaten sind in einem Speicher eines Haupt- und/oder Nebengerätes und/oder Servers abgelegte einzelne oder logisch verknüpfte Identifikationsdaten, Zugangsprofile, Zeitprofile.

[0017] Ereignisse sind vom Haupt- und/oder Nebengerät erfasste einzelne oder kombinierte Vorgänge aus der Menge Identifikationsmerkmale, Identifikationskarte gelesen oder nicht gelesen, biometrische Merkmale gelesen oder nicht gelesen, PIN eingegeben oder nicht eingegeben, biometrische Merkmale und/oder PIN sind der Ausweisnummer zugeordnet oder nicht zugeordnet, Drücken einer Funktionstaste, Zugang nach Zugangsprofil erlaubt oder nicht erlaubt, Zugang nach Zeitprofil erlaubt oder nicht erlaubt, Tür nicht geöffnet, Tür zulange offen, Tür blockiert, Türaufbruch, Kamerabild erfasst oder nicht erfasst, Kamerabild verdeckt, Kamerabild manipuliert, Netzwerkausfall, Netzwerk aktiv, jeweils verknüpft mit einem Zeitstempel aus Uhrzeit und Datum.

[0018] Historiedaten sind im Haupt- und/oder Nebengerät zwischengespeicherte Ereignisse, optional weiter verknüpft mit Standbildern und/oder Bewegtbildsequenzen und/oder Sprachaufzeichnungen.

[0019] Durch ein Lesegerät zum Lesen von auf Identifikationskarten gespeicherten Ausweisnummern als Bestandteil von Identifikationsmerkmalen als weitere Komponente des Hauptgeräts lässt sich durch Vergleich mit unverschlüsselt oder verschlüsselt gespeicherten Zugangsdaten eine lokale Authentifikation von Nutzern durchführen. Dies ermöglicht eine schnelle und sichere Identifizierung auch ohne Aufbau einer Verbindung über das Netzwerk zu einem Server oder einer Gegenstelle. Bei Bedarf können Zugangsdaten zwischen dem Speicher des Hauptgeräts und dem Server über das IP-Netzwerk geladen, gelöscht, ausgetauscht, überprüft und aktualisiert werden.

[0020] Das Hauptgerät kann wenigstens eine weitere Schnittstelle zur Daten- und/oder Signalübertragung zu und von wenigstens einem Nebengerät umfassen.

[0021] Dadurch kann unabhängig vom IP-Netzwerk eine Verbindung zu einem Nebengerät aufgebaut werden.

[0022] Das wenigstens eine Nebengerät kann mit dem Hauptgerät verbunden sein, wobei das Nebengerät als Komponenten ein Steuergerät mit einem Prozessor, einen Speicher und ein Signal- und Datenübertragungsgerät mit einer Schnittstelle zum Hauptgerät und ein Lesegerät für Identifikationsmerkmale umfassen.

[0023] Das Nebengerät kann mit unverschlüsselt oder verschlüsselt gespeicherten Zugangsdaten eine lokale Authentifikation von Nutzern durchführen und ferner können Zugangsdaten zwischen dem Speicher des Hauptgeräts und dem Speicher des Nebengeräts geladen, gelöscht, ausgetauscht, überprüft und aktualisiert werden.

[0024] Das Nebengerät kann zusätzlich eine Netzwerkschnittstelle zur Signal- und Datenübertragung zu und von dem wenigstens einen Server und/oder einem Hauptgerät und/oder der wenigstens einen Gegenstelle über das IP-Netzwerk umfassen.

[0025] Dadurch kann auch eine direkte Signal- und Datenübertragung zu und von dem wenigstens einen Server und/oder einem Hauptgerät und/oder der wenigstens einen Gegenstelle erfolgen.

[0026] Das Haupt- und/oder Nebengerät kann zusätzlich wenigstens eine weitere Schnittstelle zur Signal- und Datenübertragung zu und von dem wenigstens einen Server und der wenigstens einen Gegenstelle über wenigstens ein weiteres Netzwerk aus der Menge Mobilfunkwählnetz, insbesondere GSM-Netz, oder Festwählnetz, insbesondere ISDN-Netz oder Analog-Netz umfassen.

[0027] Durch ein weiteres Netzwerk kann die Übertragungssicherheit, zum Beispiel bei Störung eines globalen IP-Netzwerks sichergestellt werden. Zeitkritische Daten lassen sich so über einen redundanten Datenkanal in den Speicher der Haupt- und/oder Nebengeräte übertragen.

[0028] Das Haupt- und/oder Nebengerät kann als zusätzliche Komponente ein Lesegerät zum Lesen von biometrischen Merkmalen als Bestandteil von Identifikationsmerkmalen umfassen.

[0029] Dadurch lässt sich die Erkennungssicherheit weiter verbessern. Ein Zugang eines Unberechtigten mit gestohlener oder kopierter Identifikationskarte wird so verhindert.

[0030] Das Haupt- und/oder Nebengerät kann als zusätzliche Komponente eine Tastatur zur Eingabe einer PIN umfassen.

[0031] Auch hierdurch lässt sich die Erkennungssicherheit weiter verbessern.

[0032] Im Speicher des Hauptgeräts und/oder Nebengeräts können die dem Hauptgerät und/oder Nebengerät zugeordneten Zugangsdaten für einen Vergleich mit erfassten Identifikationsmerkmalen unverschlüsselt oder verschlüsselt gespeichert sein.

[0033] Im Falle einer verschlüsselten Speicherung von Zugangsdaten wird es einem Unberechtigten erschwert oder unmöglich gemacht, durch Stehlen des Hauptgeräts oder Nebengeräts und Auslesen des Speichers in den Besitz von Zugangsdaten zu gelangen oder Zugangsdaten zu manipulieren um gefälschte Identifikationskarten zu erstellen und zu benutzen. Der beschriebene Vorteil einer verschlüsselten Speicherung gilt auch für andere Arten von Daten, wie Programme, Codecs und Historiedaten.

[0034] Im Speicher des Haupt- und/oder Nebengeräts können Zugangsprofile als Bestandteil der Zugangsdaten unverschlüsselt oder verschlüsselt gespeichert sein.

[0035] Dadurch können Nutzer mit unterschiedlichen Zugangsberechtigungen entsprechend ihrer persönlichen Sicherheitshierarchiestufe und Sicherheitsstufe der geschützten Bereiche unterschieden werden.

[0036] Im Speicher des Haupt- und/oder Nebengeräts können Zeitprofile als Bestandteil der Zugangsdaten unverschlüsselt oder verschlüsselt gespeichert sein.

[0037] Auf diese Weise können individuelle und generelle zeitliche Rahmen festgelegt werden, in denen Nutzern der Zugang gewährt wird. Darüber hinaus können auch zeitliche Regeln für Ziele der Übertragung von Signalen und Daten zu Servern und Gegenstellen berücksichtigt werden.

[0038] Im Speicher des Hauptgeräts können die dem Hauptgerät zugeordneten Zugangsdaten und die den angeschlossenen Nebengeräten zugeordneten Zugangsdaten für einen Vergleich mit Identifikationsmerkmalen unverschlüsselt oder verschlüsselt gespeichert sein.

[0039] Das Hauptgerät kann so auch die Zugangsdaten der angeschlossenen Nebengeräte verwalten und aktualisieren.

[0040] Im Speicher des Nebengeräts sind vorzugsweise nur die dem Nebengerät lokal zugeordneten Zugangsdaten für einen Vergleich mit Identifikationsmerkmalen unverschlüsselt oder verschlüsselt gespeichert.

[0041] Diese Ausgestaltung ermöglicht es, Zugangsdaten nur einmalig im Hauptgerät einzuschreiben und von dort aus auf die angeschlossenen Nebengeräte zu übertragen und zu speichern. Eine individuelle Dateneingabe an den Nebengeräten entfällt. In der Annahme, dass die von einem Nebengerät benötigten Zugangsdaten geringer als die Summe der im Hautgerät gespeicherten Zugangsdaten ist, kommt das Nebengerät mit einem kleineren und damit preiswerteren Speicher aus. Neben einem geringeren Speicherbedarf der Nebengeräte lässt sich aufgrund der geringen Anzahl der im Nebengerät zu vergleichenden Zugangsdaten die Auswertezeit für einen Zugangswunsch vermindern oder bei gleicher Auswertezeit wie im Hauptgerät ein leistungsschwächerer Prozessor einsetzen.

[0042] Dies wirkt sich vorteilhaft auf die Herstellungskosten und den Energiebedarf aus, insbesondere, wenn die Geräte über ein Ethernetkabel als Bestandteil des IP-Netzwerks mit Energie versorgt werden.

[0043] Das Hauptgerät kann mit dem Server über das IP-Netzwerk dauerhaft oder temporär zur Aktualisierung der Betriebssoftware oder der im Speicher des Hauptgeräts unverschlüsselt oder verschlüsselt gespeicherten Zugangsdaten verbunden sein.

[0044] Eine dauerhafte Verbindung hat den Vorteil, dass bei Änderung von Zugangsdaten im Server diese Änderung sofort an das Hauptgerät übertragen und bei nachfolgen Zugangswünschen berücksichtigt werden kann.

[0045] Eine temporäre Übertragung kann bei selten eintretenden Änderungen ausreichen und vermindert den Energiebedarf der IP-Netzwerkschnittstelle.

[0046] Im Speicher des Haupt- und/oder Nebengeräts können die erfassten Ereignisse unverschlüsselt oder verschlüsselt zwischengespeichert sein.

[0047] Dadurch wird ermöglicht, eine genaue Historie von sämtlichen am Haupt- und/oder Nebengerät eintre-

tenden Ereignisse für eine nachträgliche Überprüfung zu protokollieren.

[0048] Das Nebengerät kann weitere Komponenten aus der Menge von Bildschirm, Kamera, Lautsprecher, Mikrofon, Funktionstaste umfassen.

[0049] Das Nebengerät kann so die gleiche Funktionalität hinsichtlich Datenerfassung und Kommunikation mit einer Gegenstelle erhalten.

[0050] Im Speicher des Haupt- und/oder Nebengeräts kann wenigstens ein von der Kamera bei einem Zugangswunsch erfasstes Standbild oder auch vom Mikrofon erfasste Sprachsignale als komprimierter Datensatz verknüpft mit Ereignissen verschlüsselt oder unverschlüsselt zwischengespeichert sein.

[0051] Durch zusätzliche Erfassung eines Standbildes bei einem Zugangswunsch können Manipulationsversuche mit gestohlenen, geliehenen oder ausgetauschten Identifikationskarten besser nachgewiesen werden. Die gespeicherten Bilddaten ermöglichen es, Bilder von Personen zu erfassen, die erfolgreiche und erfolglose Identifikationsversuche durchführen, um Zugangsversuche durch Zuordnen von Bildern der Zugang wünschenden Person protokollieren und so nachträglich auf Manipulationen überprüfen zu können.

[0052] Das Haupt- und/oder Nebengerät kann einen Türöffnertreiber zur unverschlüsselten oder verschlüsselten Generierung von Türöffnungssignalen an ein abgesetztes Türöffnersystem umfassen.

[0053] Hierdurch ist es möglich, von einem im ungesicherten Bereich angeordneten Hauptgerät aus ein abgesetztes Türöffnersystem im gesicherten Bereich zu steuern. Eine Manipulation durch Entfernen des Hauptgeräts und direktes Ansteuern des Türöffners durch Kurzschließen von Kontakten wird so vermieden.

[0054] An eine der Schnittstellen des Haupt- und/oder Nebengeräts kann wenigstes ein applikationsspezifisches Modul mit einer Schnittstelle zum Haupt- und/oder Nebengerät angeschlossen sein und das applikationsspezifische Modul kann wenigstens eine weitere Schnittstelle zu einer Peripherieanlage aus der Menge Einbruchmeldeanlage, Brandmeldeanlage, Alarmanlage, Heizung-, Lüftung-, Klimaanlage, Beleuchtungsanlage, Aufzugsanlage und/oder einem Peripheriegerät aus der Menge Feuermelder, Rauchmelder, Gasmelder, Wassermelder, Feuchtemelder, Temperaturmelder, Bewegungsmelder, Öffnungsmelder, Glasbruchmelder, Dämmerungsmelder als Eingabegeräte und optische Alarmgeber, akustische Alarmgeber, Wählgeräte, Schaltelemente, Heizung-, Lüftung-, Klimasteuerungen, Beleuchtungssteuerungen, Aufzugssteuerungen als Ausgabegeräten umfassen.

[0055] Dadurch lässt sich die Hard- und Software des Hauptgerätes oder Nebengerätes zur autonomen, intelligenten Steuerung von gebäudetechnischen Anlagen mit nutzen.

[0056] Das applikationsspezifische Modul kann ein Protokollumsetzer sein.

[0057] Mittels des Protokollumsetzers kann ein von der gebäudetechnischen Anlage genutztes Datenübertragungsprotokoll auf das Vom Hauptgerät oder Nebengerät genutzte Protokoll umgesetzt werden. Das Haupt- oder Nebengerät kann dann die gleiche Schnittstelle und das gleiche Protokoll für den Datenaustausch und die Steuerung der gebäudetechnischen Anlage wie für den Datenaustausch untereinander nutzen.

[0058] Das applikationsspezifische Modul kann ein Wandler aus der Menge Analog/Digital-Wandler, Digital/Analogwandler, Impedanzwandler, Schnittstellenwandler, Drahtgebunden/Funkwandler sein.

[0059] Dadurch lassen sich auch einzelne Melder und Sensoren der Gebäudetechnik vom Haupt- oder Nebengerät abfragen und steuern.

[0060] Das Steuergerät des Haupt- und/oder Nebengerätes kann einen Hauptprozessor zur Datenverarbeitung aus der Menge Codierung, oder Dekodierung von Zugangs-, Sprach- und Bilddaten zum Beschreiben oder Lesen des Speichers; Senden oder Empfangen von Daten über das IP-Netzwerk oder wenigstens ein weiteres Netzwerk oder wenigstes eine Schnittstelle; Auswerten von Daten, die über das IP-Netzwerk oder das wenigstens eine weitere Netzwerk oder die wenigstens Schnittstelle empfangen werden; Auswerten von empfangenen Daten von Peripherieanlagen oder Peripheriegeräten; Steuern von Peripherieanlagen oder Peripheriegeräten; autarkes Steuern von Peripherieanlagen oder Peripheriegeräten auf Basis von Peripherieanlagen oder Peripheriegeräten empfangener Daten, Bewertung von Identifikationsmerkmalen, Generierung von unverschlüsselten oder verschlüsselten Türöffnungssignalen umfassen.

[0061] Bei dieser Lösung lässt sich derselbe Hauptprozessor für alle Codier-, Decodier- Steuerungsaufgaben im Haupt oder Nebengerät nutzen.

[0062] Das den Hauptprozessor im Steuergerät des Hauptgeräts steuernde und im Speicher unverschlüsselt oder verschlüsselt gespeicherte Steuerprogramm kann ein Betriebssystem-unabhängig übergreifendes Programm sein.

[0063] Das Steuerprogramm kann in einer einheitlichen Hochsprache verfasst und in sämtlichen Hauptgeräten unabhängig von deren individuellen Betriebssystem installiert werden und ablaufen.

[0064] Vorzugsweise ist das Betriebssystem-unabhängig übergreifende Programm JAVA.

[0065] Java-Programme laufen in aller Regel ohne weitere Anpassungen auf verschiedenen Computern und Betriebssystemen, für die eine Java-Virtual-Machine existiert.

[0066] Im Speicher des Haupt- und/oder Nebengeräts können Codecs für Signale aus der Menge Sprachsignale, Standbildsignale und Bewegtbildsignale zur Ausführung durch den Hauptprozessor unverschlüsselt oder verschlüsselt gespeichert sowie ladbar und damit aktualisierbar sein.

[0067] Dadurch können Sprachsignale und Bewegtbildsignale in standardisierten Protokollen über das IP-

Netzwerk mit einer Gegenstelle ausgetauscht werden. Hierbei kann es sich um Protokolle handeln, die Internet-Telephonie oder Internet-Video-Telefone nutzen oder die von anderem Anbieter wie Skype oder Windows Live Messenger genutzt werden. Ferner können Sprachsignale, Standbildsignale und Bewegtbildsignale in komprimierter Form unverschlüsselt oder verschlüsselt gespeichert und als Dateien z. B. in den Dateiformaten wav, mp3, wma, wmv, jpeg, mpeg zum Server oder zur Gegenstelle übertragen werden. Dies kann parallel zu den übrigen Daten und über dasselbe IP-Netzwerk oder ein weiteres Netzwerk erfolgen.

[0068] Im Speicher des Haupt- und/oder Nebengeräts kann eine Menü-geführte Bedienanweisung unverschlüsselt oder verschlüsselt gespeichert sein.

[0069] Ein unerfahrener Nutzer kann so zunächst in Kommunikation mit dem Hauptgerät durch Sprach- und/oder Bildanweisungen Bedienhinweise abrufen, um gezielt die nötigen Schritte für einen Zugang vorzunehmen. Dabei ist keine Kommunikation mit einer personell besetzten Gegenstelle erforderlich.

[0070] Im Speicher des Haupt- und/oder Nebengeräts können Steuerprogramme zur Ausführung von Programmen aus der Menge von Inbetriebnahme-, Einstell- und Wartungsarbeiten durch den Hauptprozessor unverschlüsselt oder verschlüsselt gespeichert sein.

[0071] Für Inbetriebnahme-, Einstell- und Wartungsarbeiten kann das Haupt- und/oder Nebengerät bereits an seinem Einsatzort installiert sein oder installiert bleiben. Dies hat den Vorteil, dass sämtliche Arbeiten unter realen Einsatzbedingungen durchgeführt werden können.

[0072] Die dem Haupt- oder Nebengerät zugeordneten Komponenten aus der Menge Lesegerät zum Lesen von Ausweisnummern, Lesegerät zum Lesen von biometrischen Merkmalen, Tastatur zur Eingabe einer PIN können außerhalb des Hauptgeräts oder Nebengeräts in einem ungeschützten Bereich angeordnet sein.

[0073] Zugangswünsche können so außerhalb eines geschützten Bereichs eingegeben werden, während Überwachungen des geschützten Bereichs auch direkt ausgeführt werden können oder Notrufe auch vom geschützten Bereich selbst abgesetzt werden können.

[0074] Im Speicher des Nebengeräts können vom Hauptgerät zum Nebengerät übertragene Zugangsdaten unverschlüsselt oder verschlüsselt gespeichert sein.

[0075] Das Nebengerät kann nach Datenempfang vom Hauptgerät damit autark, z. B. bei Störungen des Hauptgeräts oder Unterbrechung der Datenleitung zum Hauptgerät, Zugangsberechtigungen erteilen oder Zugangswünsche abweisen.

[0076] Im Speicher des Hauptgerätes kann ein Steuerprogramm zur Steuerung eines selektiven Datentransfers der lokal benötigten Zugangsdaten zum jeweiligen Nebengerät unverschlüsselt oder verschlüsselt gespeichert sein.

[0077] Dadurch kann das Hauptgerät unmittelbar das Nebengerät mit allen erforderlichen Programmen und Daten ausstatten, ohne dass dazu eine Verbindung mit dem Server erforderlich ist.

[0078] Im Speicher des Nebengerätes kann ein Steuerprogramm zur Abfrage und eigenen Speicherung der lokal benötigten Zugangsdaten vom Speicher des Hauptgerätes unverschlüsselt oder verschlüsselt gespeichert sein.

[0079] Bei dieser Alternative kann das Nebengerät auch von sich aus die erforderlichen Programmen und Daten anfordern, ohne dass hierzu eine Initiative des Hauptgerätes erforderlich wäre.

[0080] Im Speicher des Hauptgerätes kann ein durch den Hauptprozessor ausgeführtes Steuerprogramm zur automatischen Übersetzung eines in einer Hochsprache verfassten Steuerprogramms des Hauptgerätes in ein abstrahiertes aber funktionsgleiches Steuerprogramm des jeweiligen Nebengerätes, sowie zur Konvertierung einer Datenbank mit standardisierten Datensätzen aus dem Hauptgerät in eine Datenbank mit komprimierten Datensätzen des jeweiligen Nebengeräts und zur Übertragung auf das jeweilige Nebengerät unverschlüsselt oder verschlüsselt gespeichert sein.

[0081] Hierdurch kann das Nebengerät automatisch vom Hauptgerät aus programmiert werden. Dabei entfallen der Speicherplatz und die Prozessorleistung, welche sonst für die Hochsprache, einen Programmübersetzter, für eine virtuell machine und zur Abfrage einer Datenbank mit standardisierten Datensätzen benötigt würden.

[0082] Im Speicher des Nebengerätes kann ein Steuerprogramm zur Steuerung eines Vergleichs zwischen Identifikationsmerkmalen und komprimierten Zugangsdaten unverschlüsselt oder verschlüsselt gespeichert sein, wobei die komprimierten Zugangsdaten aus vom Hauptgerät oder vom Server aufbereiteten standardisierten Datensätzen in komprimierte Datensätze konvertiert im Speicher des Nebengeräts unverschlüsselt oder verschlüsselt gespeichert sind.

[0083] Dadurch können vom Nebengerät auch die bereits im Hauptgerät oder Server generierten Datensätze ausgewertet werden. Durch Beschränkung auf nur für das Nebengerät aufbereiteter komprimierter Datensätze kann der Vergleich vereinfacht und beschleunigt werden.

[0084] Im Speicher des Haupt- und/oder Nebengerätes und/oder Server kann ein durch den Hauptprozessor im Haupt- und/oder Nebengerät und/oder Server ausgeführter Webserver und/oder Webbrowser unverschlüsselt oder verschlüsselt gespeichert sein.

[0085] Dadurch können mittels eines standardisierten Webbrowser der Gegenstelle, des Servers, des Hauptgeräts oder des Nebengeräts Daten vom Server, Haupt- und/oder Nebengerät empfangen oder in diese eingeben werden sowie Strukturen der Einrichtung dargestellt werden.

[0086] Die Erfindung betrifft ferner ein Zugangs-, Überwachungs- und Kommunikationsverfahren nach dem Oberbegriff des Anspruchs 35.

[0087] Diesbezüglich liegt ihr die Aufgabe zugrunde,

mittels einer Zugangs-, Überwachungs- und Kommunikationseinrichtung nach einem der Ansprüche 1 bis 34 eine autarke, schnelle und sichere Authentifikation durchzuführen.

[0088] Diese Aufgabe wird bei einem Zugangs-, Überwachungs- und Kommunikationsverfahren nach dem Oberbegriff des Anspruchs 34 durch die Merkmale dieses Anspruchs gelöst.

[0089] Weiterbildungen und vorteilhafte Ausgestaltungen ergeben sich aus den zugeordneten Unteransprüchen.

[0090] Indem Identifikationsmerkmale mit im Speicher des Haupt- und/oder Nebengerätes unverschlüsselt oder verschlüsselt gespeicherten und dem Haupt- und/oder Nebengerät zugeordneten Zugangsdaten verglichen werden, kann eine lokale Authentifikation von Nutzern schnell und sicher durchgeführt werden. Darüber hinaus können Zugangsdaten zwischen dem Hauptgeräts und dem Server über das IP-Netzwerk geladen, gelöscht, ausgetauscht, überprüft und aktualisiert werden.

[0091] Vor dem Vergleich können die verschlüsselt gespeicherten Zugangsdaten entschlüsselt werden.

[0092] Dadurch wird der Datenvergleich vereinfacht und eindeutig.

[0093] Vom Server können die dem Haupt- und/oder Nebengerät zugeordneten Zugangsdaten verwaltet und bei Änderungen aktualisierte Zugangsdaten über das IP-Netzwerk oder eines der weiteren Netzwerke zum Hauptgerät übertragen und im Speicher des Hauptgeräts unverschlüsselt oder verschlüsselt gespeichert werden.

[0094] Dadurch wird die Datenpflege der Haupt- und/oder Nebengeräte zentral durchgeführt und erheblich vereinfacht. Aktualisierte Zugangsdaten stehen gleichzeitig allen Haupt- und/oder Nebengeräten zu Verfügung.

[0095] Eine IP-Netzwerkverbindung und/oder eine über eines der weiteren Netzwerke bestehende Verbindung zwischen dem Server und dem Hauptgerät kann vom Server und/oder vom Hauptgerät überwacht werden und nach einem Ausfall und anschließender Wiederherstellung der IP-Netzwerkverbindung und/oder der weiteren Netzwerkverbindung kann vom Server direkt oder vom Server auf Anforderung durch das Hauptgerät eine Prüfung auf geänderte Zugangsdaten durchgeführt werden. Bei zwischenzeitlicher Änderung der dem Hauptgerät zugeordneten Zugangsdaten während des Ausfalls der IP-Netzwerkverbindung oder der weiteren Netzwerkverbindung können aktualisierte Zugangsdaten über das IP-Netzwerk und/oder des weiteren Netzwerks zum Hauptgerät übertragen und im Speicher des Hauptgerätes verschlüsselt gespeichert werden.

[0096] Bei bestehender IP-Netzwerkverbindung werden im Normalfall aktualisierte Daten sofort zum Haupt- und/oder Nebengerät übertragen. Wenn bei Störungen der IP-Netzwerkverbindung Aktualisierungen anstehen, können unverbundene Haupt- und/oder Nebengeräte keine Daten empfangen. Dieser Fall wird durch die Überwachung erkannt und eine zusätzliche Übertragung bei Widerherstellung der IP-Netzwerkverbindung durchgeführt. Auf diese Weise gehen keine Aktualisierungen verloren.

[0097] Die erfassten Identifikationsmerkmale können als Identifikationsdaten im Speicher des Haupt- oder Nebengeräts unverschlüsselt oder verschlüsselt zwischengespeichert, zum Server übertragen und in einem Speicher des Servers gespeichert werden.

[0098] Dadurch wird ermöglicht, eine genaue Historie von erfolgreichen und abgewiesenen Zugangsversuchen für eine nachträgliche Überprüfung zu protokollieren.

[0099] Daten zwischen dem Haupt- und/oder Nebengerät und dem wenigstens einen Server und der wenigstens einen Gegenstelle können wahlweise oder zusätzlich über eine weitere Schnittstelle und/oder über wenigstens ein weiteres Netzwerk aus der Menge Mobilfunkwählnetz, insbesondere GSM-Netz, oder Festwählnetz, insbesondere ISDN-Netz oder Analog-Netz, generell oder bedarfsweise übertragen werden.

[0100] Durch ein weiteres Netzwerk kann die Übertragungssicherheit, zum Beispiel bei Störung eines globalen IP-Netzwerks sichergestellt werden. Zeitkritische Daten lassen sich so über einen redundanten Datenkanal in den Speicher der Haupt- und/oder Nebengeräte übertragen.

[0101] Vom Haupt- und/oder Nebengerät können zusätzlich oder alternativ biometrischen Daten erfasst und ausgewertet werden.

[0102] Dadurch lässt sich die Erkennungssicherheit weiter verbessern. Ein Zugang eines Unberechtigten mit gestohlener oder kopierter Identifikationskarte wird so verhindert.

[0103] Vom Haupt- und/oder Nebengerät können zusätzlich oder alternativ Tastatureingaben einer PIN erfasst und ausgewertet werden.

[0104] Auch hierdurch lässt sich die Erkennungssicherheit weiter verbessern.

[0105] Vom Hauptgerät und/oder Nebengerät können die dem Hauptgerät oder Nebengerät zugeordneten Zugangsdaten für einen Vergleich mit Identifikationsmerkmalen unverschlüsselt oder verschlüsselt gespeichert und ausgewertet werden.

[0106] Im Falle einer verschlüsselten Speicherung von Zugangsdaten wird es einem Unberechtigten erschwert oder unmöglich gemacht, durch Stehlen des Hauptgeräts oder Nebengeräts und Auslesen des Speichers in den Besitz von Zugangsdaten zu gelangen oder Zugangsdaten zu manipulieren um gefälschte Identifikationskarten zu erstellen und zu benutzen. Der beschriebene Vorteil einer verschlüsselten Speicherung gilt auch für andere Arten von Daten, wie Programme, Codecs und Historiedaten.

[0107] Vom Haupt- und/oder Nebengerät können Zugangsprofile unverschlüsselt oder verschlüsselt gespeichert und ausgewertet werden.

[0108] Dadurch können Nutzer mit unterschiedlichen Zugangsberechtigungen entsprechend ihrer persönli-

chen Sicherheitshierarchiestufe und Sicherheitsstufe der geschützten Bereiche unterschieden werden.

[0109] Vom Haupt- und/oder Nebengerät können Zeitprofile unverschlüsselt oder verschlüsselt gespeichert und ausgewertet werden.

[0110] Auf diese Weise können individuelle und generelle zeitliche Rahmen festgelegt werden, in denen Nutzern der Zugang gewährt wird. Darüber hinaus können auch zeitliche Regeln für Ziele der Übertragung von Signalen und Daten zu Servern und Gegenstellen berücksichtigt werden.

[0111] Vom Hauptgerät können die dem Hauptgerät zugeordneten Zugangsdaten und die den angeschlossenen Nebengeräten zugeordneten Zugangsdaten für einen Vergleich mit Identifikationsmerkmalen unverschlüsselt oder verschlüsselt gespeichert und ausgewertet werden.

[0112] Das Hauptgerät kann so auch die Zugangsdaten der angeschlossenen Nebengeräte verwalten und aktualisieren.

[0113] Vom Nebengerät werden vorzugsweise nur die dem Nebengerät lokal zugeordneten Zugangsdaten für einen Vergleich mit Identifikationsmerkmalen unverschlüsselt oder verschlüsselt gespeichert und ausgewertet.

[0114] Diese Ausgestaltung ermöglicht es, Zugangsdaten nur einmalig im Hauptgerät einzuschreiben und von dort aus auf die angeschlossenen Nebengeräte zu übertragen und zu speichern. Eine individuelle Dateneingabe an den Nebengeräten entfällt. In der Annahme, dass die von einem Nebengerät benötigten Zugangsdaten geringer als die Summe der im Hautgerät unverschlüsselt oder verschlüsselt gespeicherten Daten ist, kommt das Nebengerät mit einem kleineren und damit preiswerteren Speicher aus. Neben einem geringeren Speicherbedarf der Nebengeräte lässt sich aufgrund der geringen Anzahl der im Nebengerät zu vergleichenden Zugangsdaten die Auswertezeit für einen Zugangswunsch vermindern oder bei gleicher Auswertezeit wie im Hauptgerät ein leistungsschwächerer Prozessor einsetzen.

[0115] Das Hauptgerät kann mit dem Server über das IP-Netzwerk dauerhaft oder temporär zur Aktualisierung der Betriebssoftware oder der im Speicher des Hauptgeräts unverschlüsselt oder verschlüsselt gespeicherten Zugangsdaten verbunden werden.

[0116] Eine dauerhafte Verbindung hat den Vorteil, dass bei Änderung von Zugangsdaten im Server diese Änderung sofort an das Hauptgerät übertragen und bei nachfolgen Zugangswünschen berücksichtigt werden kann.

[0117] Eine temporäre Übertragung kann bei selten eintretenden Änderungen ausreichen und vermindert den Energiebedarf der IP-Netzwerkschnittstelle.

[0118] Im Speicher des Haupt- und/oder Nebengeräts können die Im Speicher des Haupt- und/oder Nebengeräts können die erfassten Ereignisse als Historiendaten unverschlüsselt oder verschlüsselt zwischengespeichert werden.

[0119] Dadurch wird ermöglicht, eine genaue Historie von erfolgreichen und abgewiesenen Zugangsversuchen für eine nachträgliche Überprüfung zu protokollieren.

[0120] Im Speicher des Haupt- und/oder Nebengeräts kann wenigstens ein von der Kamera bei einem Zugangswunsch erfasstes Standbild als komprimierter Datensatz verknüpft mit Ereignissen als Historiendaten verschlüsselt oder unverschlüsselt zwischengespeichert werden.

[0121] Durch zusätzliche Erfassung eines Standbildes bei einem Zugangswunsch können Manipulationsversuche mit gestohlenen, geliehenen oder ausgetauschten Identifikationskarten besser nachgewiesen werden. Die unverschlüsselt oder verschlüsselt gespeicherten Bilddaten ermöglichen es, Bilder von Personen zu erfassen, die erfolgreiche und erfolglose Identifikationsversuche durchführen, um Zugangsversuche durch Zuordnen von Bildern der Zugang wünschenden Person protokollieren und so nachträglich auf Manipulationen überprüfen zu können.

[0122] Mittels eines Türöffnertreibers im Haupt- und/oder Nebengerät können unverschlüsselte oder verschlüsselte Türöffnungssignale generiert und an ein abgesetztes Türöffnersystem drahtlos oder drahtgebunden übertragen werden.

[0123] Hierdurch ist es möglich, von einem im ungesicherten Bereich angeordneten Hauptgerät aus ein abgesetztes Türöffnersystem zu steuern. Eine Manipulation durch Entfernen des Hauptgeräts und direktes Ansteuern des Türöffners durch Kurzschließen von Kontakten wird so vermieden.

[0124] Über eine der Schnittstellen des Haupt- und/oder Nebengeräts kann wenigstes ein applikationsspezifisches Modul mit einer Schnittstelle zum Haupt- und/oder Nebengerät und wenigstens einer weiteren Schnittstelle zu einer Peripherieanlage aus der Menge Einbruchmeldeanlage, Brandmeldeanlage, Alarmanlage, Heizung-, Lüftung-, Klimaanlage, Beleuchtungsanlage, Aufzugsanlage und/oder einem Peripheriegerät aus der Menge Feuermelder, Rauchmelder, Gasmelder, Wassermelder, Feuchtemelder, Temperaturmelder, Bewegungsmelder, Öffnungsmelder, Glasbruchmelder, Dämmerungsmelder als Eingabegeräte und optische Alarmgeber, akustische Alarmgeber, Wählgeräte, Schaltelemente, Heizung-, Lüftung-, Klimasteuerungen, Beleuchtungssteuerungen, Aufzugssteuerungen als Ausgabegeräten gesteuert werden.

[0125] Dadurch lässt sich die Hard- und Software des Hauptgerätes oder Nebengerätes zur autonomen, intelligenten Steuerung von gebäudetechnischen Anlagen mit nutzen, und zwar dann, wenn Entscheidungen bei einem temporären Ausfall eines IP-Netzwerks autark getroffen werden können.

[0126] Durch das applikationsspezifische Modul können Protokolle zwischen den Schnittstellen umgesetzt werden.

[0127] Durch Umsetzen der Protokolle kann ein von der gebäudetechnischen Anlage genutztes Datenübertragungsprotokoll auf das Vom Hauptgerät oder Nebengerät genutzte Protokoll umgesetzt werden. Das Haupt- oder Nebengerät kann dann die gleiche Schnittstelle und das gleiche Protokoll für den Datenaustausch und die Steuerung der gebäudetechnischen Anlage wie für den Datenaustausch untereinander nutzen.

[0128] Durch das applikationsspezifische Modul kann eine Signalwandlung aus der Menge Analog/Digital-Wandlung, Digital/Analogwandlung, Impedanzwandlung und Schnittstellenwandlung, Drahtgebunden/Funkwandler vorgenommen werden.

[0129] Dadurch lassen sich auch einzelne Melder und Sensoren der Gebäudetechnik vom Haupt- oder Nebengerät abfragen und steuern.

[0130] Durch einen Hauptprozessor des Steuergeräts des Haupt- und/oder Nebengerätes kann eine Datenverarbeitung aus der Menge Codierung, oder Dekodierung von Zugangs-, Sprach- und Bilddaten zum Beschreiben oder Lesen des Speichers; Senden oder Empfangen von Daten über das IP-Netzwerk oder wenigstens ein weiteres Netzwerk oder wenigstes eine Schnittstelle; Auswerten von Daten, die über das IP-Netzwerk oder das wenigstens eine weitere Netzwerk oder die wenigstens Schnittstelle empfangen werden; Auswerten von empfangenen Daten von Peripherieanlagen oder Peripheriegeräten; Steuern von Peripherieanlagen oder Peripheriegeräten; autarkes Steuern von Peripherieanlagen oder Peripheriegeräten auf Basis von Peripherieanlagen oder Peripheriegeräten empfangener Daten, Bewertung von Identifikationsmerkmalen, Generierung von verschlüsselten oder unverschlüsselten Türöffnungssignalen durchgeführt werden.

[0131] Bei dieser Lösung lässt sich derselbe Hauptprozessor für alle Codier-, Decodier- Steuerungsaufgaben im Haupt oder Nebengerät nutzen. Sämtliche Programme und Unterprogramme können daher als gemeinsames Programmpaket erstellt auf derselben Plattform laufen.

[0132] Im Hauptprozessor im Steuergerät des Hauptgerätes kann ein ein Betriebssystem-unabhängig übergreifendes Steuerprogramm ausgeführt werden.

[0133] Das Steuerprogramm kann in einer einheitlichen Hochsprache verfasst und in sämtlichen Hauptgeräten unabhängig von deren individuellen Betriebssystem installiert werden und ablaufen.

[0134] Vorzugsweise wird als Betriebssystem-unabhängig übergreifendes Steuerprogramm JAVA ausgeführt.

[0135] Java-Programme laufen in aller Regel ohne weitere Anpassungen auf verschiedenen Computern und Betriebssystemen, für die eine Java-Virtual-Machine existiert.

[0136] Im Hauptprozessor im Steuergerät des Haupt- und/oder Nebengeräts können Codecs für Signale aus der Menge Sprachsignale, Standbildsignale und Bewegtbildsignale ausgeführt werden.

[0137] Dadurch können Sprachsignale und Bewegtbildsignale in standardisierten Protokollen über das IP-Netzwerk mit einer Gegenstelle ausgetauscht werden. Hierbei kann es sich um Protokolle handeln, die Internet-Telephonie oder Internet-VideoTelefonie nutzen oder die von anderem Anbieter wie Skype oder Windows Live Messenger genutzt werden. Ferner können Sprachsignale, Standbildsignale und Bewegtbildsignale in komprimierter Form unverschlüsselt oder verschlüsselt gespeichert und als Dateien z. B. in den Dateiformaten wav, mp3, wma, wmv, jpeg, mpeg zum Server oder einer Gegenstelle übertragen werden. Dies kann parallel zu den übrigen Daten und über dasselbe IP-Netzwerk oder ein weiteres Netzwerk erfolgen.

[0138] Im Haupt- und/oder Nebengerät kann eine Menü-geführte Bedienanweisung unverschlüsselt oder verschlüsselt gespeichert und ausgeführt werden.

[0139] Ein unerfahrener Nutzer kann so zunächst in Kommunikation mit dem Haupt- und/oder Nebengerät durch Sprach- und/oder Bildanweisungen Bedienhinweise abrufen, um gezielt die nötigen Schritte für einen Zugang vorzunehmen. Dabei ist keine Kommunikation mit einer personell besetzten Gegenstelle erforderlich.

[0140] Im Haupt- und/oder Nebengerät können Steuerprogramme zur Durchführung von aus der Menge Inbetriebnahme-, Einstell- und Wartungsarbeiten unverschlüsselt oder verschlüsselt gespeichert und ausgeführt werden.

[0141] Für Inbetriebnahme-, Einstell- und Wartungsarbeiten kann das Haupt- und/oder Nebengerät bereits an seinem Einsatzort installiert sein oder installiert bleiben. Dies hat den Vorteil, dass sämtliche Arbeiten unter realen Einsatzbedingungen durchgeführt werden können.

[0142] Vom Hauptgerät zum Nebengerät können Zugangsdaten übertragen und im Speicher des Nebengeräts unverschlüsselt oder verschlüsselt gespeichert werden.

[0143] Das Nebengerät kann nach Datenempfang vom Hauptgerät damit autark, z. B. bei Störungen des Hauptgeräts oder Unterbrechung der Datenleitung zum Hauptgerät, Zugangsberechtigungen erteilen oder Zugangswünsche abweisen.

[0144] Im Hauptgerät kann ein Steuerprogramm zur Steuerung eines selektiven Datentransfers der lokal benötigten Zugangsdaten zum jeweiligen Nebengerät unverschlüsselt oder verschlüsselt gespeichert und ausgeführt werden.

[0145] Dadurch kann das Hauptgerät unmittelbar das Nebengerät mit allen erforderlichen Programmen und Daten ausstatten, ohne dass dazu eine Verbindung mit dem Server erforderlich ist.

[0146] Im Nebengerät kann ein Steuerprogramm zur Abfrage und eigenen Speicherung der lokal benötigten Zugangsdaten vom Speicher des Hauptgerätes unverschlüsselt oder verschlüsselt gespeichert und ausgeführt werden.

[0147] Bei dieser Alternative kann das Nebengerät

auch von sich aus die erforderlichen Programmen und Daten anfordern, ohne dass hierzu eine Initiative des Hauptgerätes erforderlich wäre.

[0148] Im Hauptgerät oder im Server kann ein Steuerprogramm zur automatischen Übersetzung eines in einer Hochsprache verfassten Steuerprogramms des Hauptgerätes oder des Servers in ein abstrahiertes aber funktionsgleiches Steuerprogramm des jeweiligen Nebengerätes und zur Übertragung auf das Nebengerät unverschlüsselt oder verschlüsselt gespeichert und ausgeführt werden.

[0149] Unabhängig oder gemeinsam kann auch ein Steuerprogramm zur Konvertierung einer Datenbank mit standardisierten Datensätzen aus dem Hauptgerät oder dem Server in eine Datenbank mit komprimierten Datensätzen des jeweiligen Nebengeräts und zur Übertragung auf das jeweilige Nebengerät unverschlüsselt oder verschlüsselt gespeichert und ausgeführt werden.

[0150] Hierdurch kann das Nebengerät automatisch vom Hauptgerät oder vom Server aus programmiert werden. Dabei entfallen der Speicherplatz und die Prozessorleistung, welche sonst für die Hochsprache, einen Programmübersetzter und für eine virtuell machine und/oder zur Abfrage einer Datenbank mit standardisierten Datensätzen benötigt würden.

[0151] Im Nebengerät kann ein Konvertierungsprogramm zur Konvertierung von aus vom Hauptgerät oder vom Server aufbereiteten und zum Nebengerät übertragenen standardisierten Datensätzen von Zugangsdaten in komprimierte Datensätze mit komprimierten Feldinhalten aus den Zugangsdaten unverschlüsselt oder verschlüsselt gespeichert und ausgeführt werden.

[0152] Dadurch können vom Nebengerät auch die bereits im Hauptgerät oder Server generierten Datensätze ausgewertet werden. Durch Beschränkung auf nur für das Nebengerät aufbereiteter komprimierter Datensätze kann der Vergleich vereinfacht und beschleunigt werden.

[0153] Im Haupt- und/oder Nebengerät und/oder Server kann ein Webserver und/oder Webbrowser ausgeführt werden.

[0154] Dadurch können mittels eines standardisierten Webbrowser der Gegenstelle, des Servers, des Hauptgeräts oder des Nebengeräts Daten vom Server, Haupt- und/oder Nebengerät empfangen oder in dieses eingegeben werden sowie Strukturen der Einrichtung dargestellt werden.

[0155] Der Webbrowser nutzt hier die Infrastruktur der vernetzten Einrichtung um Zugriff auf Haupt-, Nebengeräte oder Server über die in den Geräten vorhandenen Webserver zu erhalten.

[0156] In der Regel kann vom Webbrowser eines Nebengerätes nur auf den Webserver des Nebengerätes zugegriffen werden, vom Webbrowser eines Hauptgerätes nur auf die Webbrowser des Hauptgerätes und der angeschlossenen Nebengeräte und vom Webbrowser eines Servers auf die Webbrowser der Hauptgeräte und der direkt angeschlossenen Nebengeräte.

[0157] Durch erweiterte Zugriffsrechte können aber auch Webbrowser wahlweise die Gesamthierarchie der Einrichtung oder einzelne Ebenen oder Komponenten aus der Menge Server, Hauptgerät, Nebengerät, Peripherieanlage Peripheriegerät darstellen.

[0158] Dadurch lassen sich unterstützt durch eine grafische Oberfläche sämtliche Wartungs- und Aktualisierungsarbeiten von einem Ort aus durchführen.

[0159] Nachfolgend wird die Erfindung anhand von Ausführungsbeispielen erläutert, die in der Zeichnung dargestellt sind.

[0160] In der Zeichnung zeigen:

Fig. 1 eine schematische Übersicht der erfindungsgemäßen Einrichtung,

Fig. 2 ein Blockschaltbild eines Hauptgeräts oder Nebengeräts,

Fig. 3 eine schematische Darstellung einer Verbindungsmöglichkeit zwischen einem Haupt- und einem Nebengerät,

Fig. 4 eine schematische Darstellung einer Anbindung zusätzlicher Anlagen, Sensoren, Melder und Geber und

Fig. 5 eine schematische Darstellung von Verbindungsmöglichkeiten zwischen Haupt-, Nebengerät und Server.

[0161] Fig. 1 zeigt eine schematische Übersicht der erfindungsgemäßen Einrichtung. Über ein IP-Netzwerk 10 sind mehrere Hauptgeräte 12, 12', 12'' ständig oder temporär mit einem Server 14 verbunden. Die Hauptgeräte 12, 12', 12'' enthalten sämtliche zur Überwachung und Kontrolle eines Zugangsbegehrens für einen geschützten Bereich erforderlichen Komponenten und umfassen hier zusätzlich einen Webserver 16, 16', 16" und Webklient 18, 18', 18''. Die Hauptgeräte 12, 12', 12''arbeiten Zugangsbegehren autark ab, können aber auch vom Nutzer generierte Identifikationsdaten zum Server 14 übertragen oder aktualisierte Zugangsdaten und Steuerungssoftware vom Server 14 erhalten.

[0162] Bei dem IP-Netzwerk 10 handelt es sich um ein das Internetprotokoll nutzendes Netzwerk. Dies kann ein öffentliches Netzwerk, wie das Internet oder auch ein privates Netzwerk, wie das Intranet sein. Auch Funknetzwerke sind möglich, wie zum Beispiel WLAN, Bluetooth oder ZigBee.

[0163] Fig. 2 zeigt ein Blockschaltbild eines Hauptgerätes 12 oder Nebengerätes 54. Das Hauptgerät 12 oder Nebengerät 54 umfasst ein Steuergerät 20 mit einem Hauptprozessor, einem Speicher 22 und einem Signal- und Datenübertragungsgerät 24. An das Steuergerät sind ein Identifikationskarten-Lesegerät 25, ein Lesegerät 26 für biometrische Merkmale, ein Bildschirm 28, eine Kamera 30, ein Mikrofon 32, ein Lautsprecher 34 sowie Funktionstasten und/oder eine Tastatur 36 angeschlos-

sen. Das Identifikationskarten-Lesegerät 25, das Lesegerät 26 für biometrische Merkmale, der Bildschirm 28, die Kamera 30, das Mikrofon 32, und der Lautsprecher 34 können auch mehrfach vorhanden und vom Hauptgerät 12 oder Nebengerät 54 abgesetzt oder abweichend von Fig. 2 nur abgesetzt sein. Dabei kann zum Beispiel das Hauptgerät 12 oder Nebengerät 54 in einem geschützten Bereich angeordnet sein, während die abgesetzten Komponenten in einem ungeschützten Bereich installiert sind.

[0164] Das Signal- und Datenübertragungsgerät 24 ist über eine IP-Schnittstelle 44, 68 mit einem IP-Netzwerk verbunden, bei dem es sich um ein öffentliches Netzwerk WAN oder ein lokales Netzwerk LAN handeln kann. Weiterhin sind an das Signal- und Datenübertragungsgerät 24 Funkmodule angeschlossen, die im Hauptgerät 12 und Nebengerät 68 integriert sind. Es handelt sich hier um ein GSM-Funkmodul 38, ein WLAN-Funkmodul 40 sowie ein ISM-Funkmodul 42. An das Signal- und Datenübertragungsgerät 24 ist außerdem eine weitere Schnittstelle 46, 56, 70 angeschlossen zur Anbindung an ein weiteres IP-Netzwerk, aber auch einen Datenbus, eine Datenleitung oder unmittelbar an eine externe Komponente.

[0165] An die weitere Schnittstelle 46, 56, 70 ist hier ein applikationsspezifisches Modul 48 angeschlossen, über das gebäudetechnische Anlagen, Sensoren Melder oder Aktoren angeschlossen werden können. Als Beispiel ist hier ein Funkmodul 50 dargestellt, das vom applikationsspezifischen Modul 48 gesteuert wird und über Funk ein Türöffnungssystem freigibt.

[0166] Alternativ kann das Türöffnungssystem auch über Funk durch das ISM-Funkmodul 42 gesteuert werden.

[0167] Im Speicher 22 sind Zugangsdaten zur Überprüfung von Zugangsbegehren und Steuerprogramme zur Steuerung des Steuergeräts 20 gespeichert. Ferner können auch Codecs für Sprachsignale, Bewegtbild- und Standbildsignale gespeichert sein. Darüber hinaus können auch vom Identifikationskarten-Lesegerät 25 gelesene Ausweisnummern oder vom Lesegerät 26 für biometrische Merkmale gelesenen biometrische Merkmale, über die Tastatur 36 eingegebene PINs sowie von der Kamera 30 aufgenommene Stand- oder Bewegtbilder und vom Mikrofon 32 aufgenommene Sprachsignale zwischengespeichert werden.

[0168] Zur Erhöhung der Sicherheit können sämtliche Daten und Programme in verschlüsselter Form gespeichert werden. Das Signal- und Datenübertragungsgerät 24 verwaltet die IP-Schnittstelle 44, 68, die weitere Schnittstelle 46, 56, 70 und steuert das Senden und Empfangen von Daten über diese Schnittstelle. Ferner werden auch die Funkmodule 38, 40 und 42 gesteuert.

[0169] In der Darstellung nach Fig. 2 sind das Identifikationskarten-Lesegerät 25 und das Lesegerät 26 für biometrische Merkmale, der Bildschirm 28, die Kamera 30, das Mikrofon 32, der Lautsprecher 34 und Funktionstasten oder die Tastatur 36 im Gehäuse des Hauptgerätes 12 oder Nebengerätes 54 integriert. Es ist jedoch auch möglich, einzelne oder mehrere Komponenten außerhalb des Gehäuses des Hauptgerätes 12 oder Nebengerätes 54anzuordnen. So können mittels einer oder auch mehrerer Kameras 30 Bilder aus weiteren Perspektiven oder Räumen erfasst werden. Auch der Lautsprecher 34 kann aus einem einzelnen oder mehreren Lautsprechern bestehen, um zum Beispiel Durchsagen in anderen Bereichen oder Räumen hörbar zu machen.

[0170] Während im Speicher 22 des Hauptgerätes 12 ein Betriebssystem-unabhängig übergreifendes Steuerprogramm, nämlich JAVA, gespeichert ist und durch den Hauptprozessor des Steuergerätes 20 ausgeführt wird, ist im Speicher 22 des Nebengerätes 54 ein abstrahiertes aber funktionsgleiches Steuerprogramm gespeichert und wird durch den Hauptprozessor des Steuergerätes 20 ausgeführt.

[0171] Fig. 3 zeigt eine schematische Darstellung einer Verbindungsmöglichkeit zwischen einem Hauptgerät und einem Nebengerät.

[0172] Das Hauptgerät 12 ist über die zusätzliche Schnittstelle 46 und einen Datenbus 52 mit Nebengeräten 54, 54' über deren Schnittstellen 56, 56' verbunden. Wenn die Nebengeräte 54, 54' vom Hauptgerät 12 aus verwaltet werden, können sie mit einfacheren und preisgünstigeren Komponenten im Vergleich zum Hauptgerät 12 ausgestattet werden.

[0173] In diesem Fall besteht lediglich vom Hauptgerät 12 aus eine Verbindung über ein IP-Netzwerk 10 zu einem Server 14, während die Nebengeräte 54, 54' Zugangsdaten und Programmdaten vom Hauptgerät 12 aufbereitet über den Datenbus 52 erhalten.

[0174] Fig. 4 zeigt eine schematische Darstellung einer weiteren Verbindungsmöglichkeit zwischen Hauptgerät 12 und Nebengerät 54. In diesem Fall sind an dem Datenbus 52 zwischen dem Hauptgerät 12 und dem Nebengerät 54 applikationsspezifische Module 48, 48', 48'' über deren Schnittstellen 60, 60', 60'' angeschlossen. Die applikationsspezifischen Module 48, 48', 48'' dienen dazu, gebäudetechnische Anlagen sowie Sensoren. Melder und Aktoren einzubinden. Die applikationsspezifischen Module 48, 48', 48'' dienen ebenfalls zur Umsetzung von Schnittstellen und Protokollen.

[0175] So ist in der Darstellung an eine Schnittstelle 62 des applikationsspezifischen Moduls 48 eine Einbruchmeldeanlage 64 und an eine Schnittstelle 62' des applikationsspezifischen Moduls 48' eine Brandmeldeanlage 66 angeschlossen. Sensoren, Melder und Aktoren können über entsprechende Schnittstellen 62'', 62''', 62'''' an das applikationsspezifische Modul 58'' angeschlossen werden. Beispiele hierfür sind Bewegungsmelder, Brandmelder, Temperatursensoren als Sensoren bzw. Melder oder Schaltelemente oder elektromechanische Bauelemente als Aktoren.

[0176] Fig. 5 zeigt eine schematische Darstellung von Verbindungsmöglichkeiten zwischen Hauptgerät 12, Nebengeräten 54, 54', 54'' und Server 14. An die Schnittstelle 46 eines Hauptgerätes sind zwei Nebengeräte 54,

54' und ein applikationsspezifisches Modul 48 angeschlossen. Das Hauptgerät kann über eine IP-Schnittstelle 44 über ein IP-Netzwerk 10 mit einem Server 14 kommunizieren. Zusätzlich ist noch die Möglichkeit dargestellt, dass ein Nebengerät 54'' ebenfalls eine IP-Schnittstelle 68 aufweisen kann und über ein IP-Netzwerk 10 direkt mit dem Server 14 oder einem Hauptgerät 12 kommuniziert. Das Nebengerät 54'' kann seinerseits über eine weitere Schnittstelle 70 mit einem Datenbus 72 mit einem applikationsspezifischen Modul 48 über dessen Schnittstelle 60 kommunizieren.

[0177] Nachfolgend werden einige Einsatzszenarien für die erfindungsgemäße Einrichtung beschrieben.

[0178] Wenn ein Nutzer Zugang zu einem gesicherten Bereicht wünscht, hält er eine Identifikationskarte, auf der eine Ausweisnummer gespeichert ist, vor das Lesegerät 25. Auf der Karte kann ein Transponder mit einem Speicher angeordnet sein, so dass die Ausweisnummer berührungslos vom Lesegerät 25 gelesen werden kann. Der Prozessor des Steuergerätes 20 vergleicht daraufhin die gelesene Ausweisnummer mit im Speicher 22 abgelegten Zugangsdaten. Ist der Vergleich positiv, wird Zugang gewährt, indem das Steuergerät 20 über das Signal- und Datenübertragungsgerät 24 ein verschlüsseltes Türöffnungssignal generiert, das zu einem applikationsspezifischen Modul 48 und weiter zu einem Funkmodul 50 übertragen wird. Das Funkmodul 50 wiederum gibt ein funkgesteuertes Türöffnungssystem eine damit verbundene Tür. Die Übertragung zum funkgesteuerten Türöffnungssystem kann auch über ein mit dem Signal- und Datenübertragungsgerät 24 verbundenes ISM-Funkmodul 42 erfolgen.

[0179] Um zu verhindern, dass Unberechtigte mit einer gestohlenen oder geliehenen Identifikationskarte Zugang erhalten, können auch biometrische Merkmale, wie zum Beispiel ein Fingerabdruck, angefordert und durch ein weiteres Lesegerät 26 gelesen werden. Das Steuergerät 20 vergleicht dann zusätzlich die auf der Identifikationskarte oder im Speicher 22 gespeicherten biometrischen Merkmale mit vom Lesegerät 26 gelesenen biometrischen Merkmalen.

[0180] Nach positiver Authentifizierung der Identifikationskarte und des damit verbundenen Nutzers vergleicht das Steuergerät 20 dann diese Identifikationsmerkmale mit Zugangsdaten und generiert ein bei Übereinstimmung Türöffnungssignal.

[0181] Alternativ oder zusätzlich zu den biometrischen Daten kann auch eine PIN abgefragt werden, die vom Nutzer über eine Tastatur 36 eingegeben wird. In dem Fall wird vom Steuergerät 20 zusätzlich die Übereinstimmung der eingegebenen PIN mit einer auf der Identifikationskarte oder im Speicher 22 gespeicherten PIN verglichen.

[0182] Für eine spätere Protokollierung und Überprüfung können die gelesenen oder eingegebenen Daten, also die Identifikationsdaten, biometrischen Daten und PINs auch im Speicher 22 zwischengespeichert werden. Verknüpft mit diesen gespeicherten Daten, werden auch Ereignisdaten, zum Beispiel Tageszeit und Datum mitgespeichert. Zusätzlich können auch von der Kamera 30 erfasste Bilder der zugangsbegehrenden Personen erfasst und als wenigstens ein Standbild in komprimierter Form zusammen mit den anderen Daten zwischengespeichert werden.

[0183] Neben den Zugangsdaten können auch Zugangsprofile im Speicher 22 gespeichert sein und beim Vergleich berücksichtigt werden. Solche Zugangsprofile können zum Beispiel Hierarchiestufen der Nutzer sowie Sicherheitsstufen der geschützten Bereiche kennzeichnen. So kann festgelegt werden, dass Benutzer nur zu bestimmten gesicherten Bereichen Zugang haben, während ein Zugangswunsch zu anderen Bereichen abgewiesen wird.

[0184] Alternativ oder zusätzlich zu den Zugangsprofilen können auch Zeitprofile gespeichert sein, die ebenfalls zusätzlich zu den Zugangsdaten verglichen werden. Mithilfe dieser Zeitprofile können Tageszeiten, Wochenprogramme und Datumszeiten festgelegt werden, zu denen Nutzern ein Zugang gewährt wird oder ein Zugangswunsch abgewiesen wird.

[0185] Die in einem oder mehreren Hauptgeräten 12 und/oder Nebengeräten 54 gespeicherten Zugangsdaten, Zugangsprofile und Zeitprofile werden in einem Server 14 verwaltet, zu dem eine dauerhafte oder eine temporäre Verbindung über ein IP-Netzwerk 10 besteht. Von diesem Server 14 werden die verbundenen Hauptgeräte 12 und/oder Nebengeräte 54 erstmalig mit Zugangsdaten, Zugangsprofilen und Zeitprofilen geladen.

[0186] Wenn auf dem Server 14 Änderungen dieser Daten vorgenommen werden, können aktualisierte Daten an die von den Änderungen betroffenen Haupt- und/oder Nebengeräte übertragen und dort gespeichert werden. Zur Verminderung von Manipulationen an den Haupt- und/oder Nebengeräten können sämtliche Daten in den betreffenden Speichern 22 verschlüsselt gespeichert werden. Neben den Zugangsdaten, Berechtigungsprofilen und Zeitprofilen können auch Programmdateien sowie Codecs vom Server über das IP-Netzwerk 10 zu den Hauptgeräten 12 und/oder Nebengeräten 54 übertragen und dort verschlüsselt oder unverschlüsselt gespeichert werden.

[0187] Umgekehrt können auch zwischengespeicherte Nutzerdaten, das heißt Identifikationsdaten, biometrische Daten, PINs, Standbilddaten der Kamera zusammen mit Ereignisdaten, wie Zeit, Datum, Zugang gewährt, Zugangswunsch abgewiesen, Kamerabild nicht erfasst, zum Server 14 übertragen und dort gespeichert werden, um eine zentrale Datensicherung zu Protokoll- und Überwachungszwecken durchzuführen.

[0188] Während Hauptgeräte 12 und Nebengerät 54 generell über eine IP-Netzwerkverbindung zu einem Server 14 verfügen, können Nebengeräte 54 auch ausschließlich nur über eine weitere Schnittstelle 56 über einen Datenbus 52 oder eine Datenleitung mit einem zugeordneten Hauptgerät 12 kommunizieren. In diesem Fall werden vom Hauptgerät 12 neben den eigenen Zu-

gangsdaten, Zugangsprofilen und Zeitprofilen auch die Zugangsdaten, Zugangsprofile und Zeitprofile sowie Steuerprogramme der angeschlossenen Nebengeräte 54 verwaltet und bedarfsweise über die weitere Schnittstelle 46; 56 aktualisiert.

[0189] Wenn im Speicher 22 des Hauptgerätes 12 ein in einer Hochsprache verfasstes Programm ausgeführt wird, kann dieses automatisch in ein abstrahiertes aber funktionsgleiches Steuerprogramm übersetzt werden, das auf dem Nebengerät 54 läuft. Weiterhin kann automatisch eine auf dem Hauptgerät 12 ausgeführte Datenbank aus standardisierten Datensätzen in eine Datenbank aus komprimierten Datensätzen konvertiert werden, die auf dem Nebengerät 54 ausgeführt wird. Die Programm- und Datenbankkonvertierung kann auch vom Server 14 durchgeführt werden, wenn, Nebengeräte 54 direkt mit dem Server 14 kommunizieren. Aufgrund einer maschinennäheren Programmierung und einem schnelleren Zugriff auf die Datensätze kommt das Nebengerät 54 bei gleicher Ablaufgeschwindigkeit im Vergleich zum Hauptgerät 12 mit einer geringerer Prozessorleistung aus. Auch die Speicherkapazität des Nebengerätes 54 kann im Vergleich zum Hautgerät 12 geringer bemessen sein.

[0190] Zusätzlich kann das Hauptgerät 12 oder auch das Nebengerät 54, sofern es mit den zusätzlichen Komponenten Bildschirm, Kamera, Mikrofon und Lautsprecher ausgestattet ist, auch mit einer Gegenstelle in Videotelefonie kommunizieren. Dazu werden im Steuergerät 20 mittels im Speicher 22 gespeicherter Codecs die empfangenen und gesendeten Video- und Sprachdaten in ein Protokoll übersetzt, das als Livestream über das IP-Netzwerk 10 übertragen werden kann. Die Gegenstellen können andere Hauptgeräte, Nebengeräte, PCs oder IP-Telefone sein, die den SIP-Standard beherrschen.

[0191] Für den Verbindungsaufbau betätigt der Nutzer eine Funktionstaste 36 am Hauptgerät 12 oder Nebengerät 54, die dann einen vorprogrammierten Verbindungsaufbau startet. Zeitgesteuert können auch andere Verbindungen aktiviert werden.

[0192] An die weitere Schnittstelle 46; 56 des Haupt- und/oder Nebengerätes können auch gebäudetechnische Anlagen, Sensoren, Melder und Geber angeschlossen werden. Um eine Kompatibilität zwischen der weiteren Schnittstelle 46; 56 und den Anlagen, Meldern, Sensoren und Aktoren zu ermöglichen, sind diese über ein applikationsspezifisches Modul 48; 58 mit der weiteren Schnittstelle 46; 56; 70 oder einem an die Schnittstelle angeschlossenen Datenbus 52; 72 oder Datenleitung verbunden. Das applikationsspezifische Modul 48 fungiert dann als Protokollumsetzer, Schnittstellenumsetzer oder D/A- oder A/D-Wandler. In diesem Fall wird die Infrastruktur der erfindungsgemäßen Einrichtung für die Verwaltung, Steuerung und Weiterleitung von Signalen und Daten der gebäudetechnischen Anlage, Melder, Sensoren oder Aktoren mitverwendet.

[0193] Zusätzlich kann auch in den Haupt- und/oder Nebengeräten ein Wartungs- und Einrichtungsprogramm gespeichert und aufrufbar sein. Dabei lassen sich zum Beispiel die einzelnen Komponenten einstellen und auf Funktionen überprüfen. So ist es zum Beispiel möglich, das Kamerabild auf den eigenen Bildschirm umzulenken, um so gezielt die Ausrichtung der Kamera auf einen Nutzer vorzunehmen.

[0194] Auf den Haupt- und/oder Nebengeräten und/oder dem Server können auch Webserver und Webclients gespeichert und bedarfsweise ausgeführt werden. Dadurch kann die Infrastruktur und Hardware genutzt werden, um auf einer grafischen Oberfläche die Struktur und Verknüpfung in unterschiedlichen Ebenen darzustellen, zu verwalten oder auch an einzelnen Haupt- oder Nebengeräten zu verwalten. Dazu erzeugt der entsprechende Webserver Daten in einem über ein IP-Netzwerk übertragbares Protokoll, während der Webclient als Browser die Daten auf einer grafischen Oberfläche darstellt.

Patentansprüche

1. Zugangs-, Überwachungs- und Kommunikationseinrichtung für wenigstens einen geschützten örtlichen Bereich von Gebäuden, Räumen oder Grundstücken mit wenigstens einem Hauptgerät, wobei das Hauptgerät als Komponenten einen Bildschirm, eine Kamera, einen Lautsprecher, ein Mikrofon, wenigstens eine Funktionstaste, ein Steuergerät, einen Speicher und ein Signal- und Datenübertragungsgerät mit einer Netzwerkschnittstelle zur Signalübertragung zu und von wenigstens einer Gegenstelle über ein IP-Netzwerk umfasst, **dadurch gekennzeichnet, dass** das Hauptgerät als zusätzliche Komponente ein Lesegerät zum Lesen von auf Identifikationskarten gespeicherten Ausweisnummern als Bestandteil von Identifikationsmerkmalen umfasst.

2. Zugangs-, Überwachungs- und Kommunikationseinrichtung nach Anspruch 1, **dadurch gekennzeichnet, dass** ein Server zur Datenübertragung zu und von dem wenigstens einen Hauptgerät über eine Netzwerkschnittstelle ebenfalls an das IP-Netzwerk angeschlossen ist, wobei das IP-Netzwerk ein Internet-Protokoll nutzendes Netzwerk aus der Menge Internet-Netzwerk, Lokal Area Netzwerk (LAN), drahtloses Lokal Area Netzwerk (WLAN), Bluetooth-Netzwerk, ZigBee ist.

3. Zugangs-, Überwachungs- und Kommunikationseinrichtung nach Anspruch 1 oder 2, **dadurch gekennzeichnet, dass** das wenigstens eine Hauptgerät wenigstens eine weitere Schnittstelle zur Daten- und Signalübertragung oder Datenübertragung oder Signalübertragung zu und von wenigstens einem Nebengerät umfasst.

4. Zugangs-, Überwachungs- und Kommunikationseinrichtung nach Anspruch 3, **dadurch gekennzeichnet, dass** wenigstens ein Nebengerät mit dem Hauptgerät verbunden ist, wobei das Nebengerät als Komponenten ein Steuergerät mit einem Prozessor, einen Speicher und ein Signal- und Datenübertragungsgerät mit einer Schnittstelle zum Hauptgerät und ein Lesegerät zum Lesen von Identifikationsmerkmalen umfasst.

5. Zugangs-, Überwachungs- und Kommunikationseinrichtung nach Anspruch 3 oder 4, **dadurch gekennzeichnet, dass** das Nebengerät zusätzlich eine Netzwerkschnittstelle zur Signal- und Datenübertragung zu und von wenigstens einer Einrichtung aus der Menge Server und Gegenstelle über das IP-Netzwerk umfasst.

6. Zugangs-, Überwachungs- und Kommunikationseinrichtung nach einem der Ansprüche 1 bis 5, **dadurch gekennzeichnet, dass** das Haupt- oder Nebengerät zusätzlich wenigstens eine weitere Schnittstelle zur Signal- und Datenübertragung zu und von der wenigstens einer Einrichtung aus der Menge Server und Gegenstelle über wenigstens ein weiteres Netzwerk aus der Menge Mobilfunkwählnetz, insbesondere GSM-Netz, und Festwählnetz, insbesondere ISDN-Netz, Analog-Netz umfasst.

7. Zugangs-, Überwachungs- und Kommunikationseinrichtung nach einem der Ansprüche 1 bis 6, **dadurch gekennzeichnet, dass** das Haupt- oder Nebengerät als zusätzliche Komponente ein Lesegerät zum Lesen biometrischer Merkmale als Bestandteil von Identifikationsmerkmalen umfassen.

8. Zugangs-, Überwachungs- und Kommunikationseinrichtung nach einem der Ansprüche 1 bis 7, **dadurch gekennzeichnet, dass** das Haupt- oder Nebengerät als zusätzliche Komponente eine Tastatur zur Eingabe einer PIN als Bestandteil von Identifikationsmerkmalen umfassen.

9. Zugangs-, Überwachungs- und Kommunikationseinrichtung nach einem der Ansprüche 1 bis 8, **dadurch gekennzeichnet, dass** im Speicher des Hauptgeräts wenigstens die dem Hauptgerät zugeordneten Zugangsdaten für einen Vergleich mit vom Lesegerät gelesenen Identifikationsmerkmalen unverschlüsselt oder verschlüsselt gespeichert sind.

10. Zugangs-, Überwachungs- und Kommunikationseinrichtung nach einem der Ansprüche 1 bis 9, **dadurch gekennzeichnet, dass** im Speicher des Haupt- oder Nebengeräts Zugangsprofile als Bestandteile von Zugangsdaten unverschlüsselt oder verschlüsselt gespeichert sind.

11. Zugangs-, Überwachungs- und Kommunikationseinrichtung nach einem der Ansprüche 1 bis 10, **dadurch gekennzeichnet, dass** im Speicher des Haupt- oder Nebengeräts Zeitprofile als Bestandteile von Zugangsdaten unverschlüsselt oder verschlüsselt gespeichert sind.

12. Zugangs-, Überwachungs- und Kommunikationseinrichtung nach einem der Ansprüche 1 bis 11, **dadurch gekennzeichnet, dass** im Speicher des Hauptgeräts die dem Hauptgerät zugeordneten Zugangsdaten und die den angeschlossenen Nebengeräten zugeordneten Zugangsdaten für einen Vergleich mit vom Lesegerät gelesenen Identifikationsmerkmalen unverschlüsselt oder verschlüsselt gespeichert sind.

13. Zugangs-, Überwachungs- und Kommunikationseinrichtung nach einem der Ansprüche 4 bis 12, **dadurch gekennzeichnet, dass** im Speicher des Nebengeräts nur die dem Nebengerät lokal zugeordneten Zugangsdaten für einen Vergleich mit vom Lesegerät gelesenen Identifikationsmerkmalen unverschlüsselt oder verschlüsselt gespeichert sind.

14. Zugangs-, Überwachungs- und Kommunikationseinrichtung nach einem der Ansprüche 1 bis 13, **dadurch gekennzeichnet, dass** das Haupt- oder Nebengerät mit dem Server über das IP-Netzwerk dauerhaft oder temporär zur Aktualisierung und unverschlüsselten oder verschlüsselten Speicherung der Betriebssoftware oder der im Speicher des Hauptgeräts unverschlüsselt oder verschlüsselt gespeicherten Zugangsdaten verbunden ist.

15. Zugangs-, Überwachungs- und Kommunikationseinrichtung nach einem der Ansprüche 1 bis 14, **dadurch gekennzeichnet, dass** im Speicher des Haupt- oder Nebengeräts Identifikationsmerkmale verknüpft mit Ereignissen und optional weiter verknüpft mit Standbilddaten oder Sprachdaten oder Standbild- und Sprachdaten als Historiedaten unverschlüsselt oder verschlüsselt zwischengespeichert sind.

16. Zugangs-, Überwachungs- und Kommunikationseinrichtung nach einem der Ansprüche 4 bis 15, **dadurch gekennzeichnet, dass** das Nebengerät weitere Komponenten aus der Menge von Bildschirm, Kamera, Lautsprecher, Mikrofon, Funktionstaste umfasst.

17. Zugangs-, Überwachungs- und Kommunikationseinrichtung nach einem der Ansprüche 1 bis 16, **dadurch gekennzeichnet, dass** das Haupt- oder Nebengerät einen Türöffnertreiber zur unverschlüsselten oder verschlüsselten Generierung von Türöffnungssignalen an ein abgesetztes Türöffnerschalt-

modul umfasst.

18. Zugangs-, Überwachungs- und Kommunikationseinrichtung nach einem der Ansprüche 1 bis 16, **dadurch gekennzeichnet, dass** an eine der Schnittstellen des Haupt- oder Nebengeräts wenigstes ein applikationsspezifisches Modul mit einer Schnittstelle zum Haupt- oder Nebengerät und wenigstens einer weiteren Schnittstelle zu einer Peripherieanlage aus der Menge Einbruchmeldeanlage, Brandmeldeanlage, Alarmanlage, Heizung-, Lüftung-, Klimaanlage, Beleuchtungsanlage, Aufzugsanlage und/oder einem Peripheriegerät aus der Menge Feuermelder, Rauchmelder, Gasmelder, Wassermelder, Feuchtemelder, Temperaturmelder, Bewegungsmelder, Öffnungsmelder, Glasbruchmelder, Dämmerungsmelder als Eingabegeräte und optische Alarmgeber, akustische Alarmgeber, Wählgeräte, Schaltelemente, Heizung-, Lüftung-, Klimasteuerungen, Beleuchtungssteuerungen, Aufzugssteuerungen als Ausgabegeräten umfasst.

19. Zugangs-, Überwachungs- und Kommunikationseinrichtung nach Anspruch 18, **dadurch gekennzeichnet, dass** das applikationsspezifische Modul ein Protokollumsetzer ist.

20. Zugangs-, Überwachungs- und Kommunikationseinrichtung nach Anspruch 18, **dadurch gekennzeichnet, dass** das applikationsspezifische Modul ein Wandler aus der Menge Analog/Digital-Wandler, Digital/Analogwandler, Impedanzwandler und Schnittstellenwandler ist.

21. Zugangs-, Überwachungs- und Kommunikationseinrichtung nach einem der Ansprüche 1 bis 20, **dadurch gekennzeichnet, dass** das Steuergerät des Haupt- oder Nebengeräts einen Hauptprozessor zur Datenverarbeitung aus der Menge Codierung, Dekodierung von Zugangs-, Sprach- und Bilddaten zum Beschreiben oder Lesen des Speichers; Senden oder Empfangen von Daten über das IP-Netzwerk oder wenigstens ein weiteres Netzwerk oder wenigstes eine Schnittstelle; Auswerten von Daten, die über das IP-Netzwerk oder das wenigstens eine weitere Netzwerk oder die wenigstens Schnittstelle empfangen werden; Auswerten von empfangenen Daten von Peripherieanlagen oder Peripheriegeräten; Steuern von Peripherieanlagen oder Peripheriegeräten; autarkes Steuern von Peripherieanlagen oder Peripheriegeräten auf Basis von von Peripherieanlagen oder Peripheriegeräten empfangener Daten, Generierung von Türöffnungssignalen jeweils unverschlüsselt oder verschlüsselt umfasst.

22. Zugangs-, Überwachungs- und Kommunikationseinrichtung nach einem der Ansprüche 1 bis 21, **dadurch gekennzeichnet, dass** das den Hauptprozessor im Steuergerät des Hauptgeräts steuernde und im Speicher unverschlüsselt oder verschlüsselt gespeicherte Steuerprogramm ein Betriebssystem-unabhängig übergreifendes Programm ist.

23. Zugangs-, Überwachungs- und Kommunikationseinrichtung nach Anspruch 22, **dadurch gekennzeichnet, dass** das Betriebssystem-unabhängig übergreifende Programm JAVA ist.

24. Zugangs-, Überwachungs- und Kommunikationseinrichtung nach einem der Ansprüche 1 bis 23, **dadurch gekennzeichnet, dass** im Speicher des Haupt- oder Nebengeräts Codecs aus der Menge Sprachsignale, Standbildsignale und Bewegtbildsignale zur Ausführung durch den Hauptprozessor unverschlüsselt oder verschlüsselt gespeichert sowie ladbar und damit aktualisierbar sind.

25. Zugangs-, Überwachungs- und Kommunikationseinrichtung nach einem der Ansprüche 1 bis 24, **dadurch gekennzeichnet, dass** im Speicher des Haupt- oder Nebengerät eine Menü-geführte Bedienanweisung unverschlüsselt oder verschlüsselt gespeichert ist.

26. Zugangs-, Überwachungs- und Kommunikationseinrichtung nach einem der Ansprüche 1 bis 25, **dadurch gekennzeichnet, dass** im Speicher des Haupt- oder Nebengerät Steuerprogramme zur Ausführung von Programmen aus der Menge von Inbetriebnahme-, Einstell- und Wartungsarbeiten durch den Hauptprozessor unverschlüsselt oder verschlüsselt gespeichert sind.

27. Zugangs-, Überwachungs- und Kommunikationseinrichtung nach einem der Ansprüche 3 bis 26, **dadurch gekennzeichnet, dass** die dem Haupt- oder Nebengerät zugeordneten Komponenten aus der Menge Lesegerät zum Lesen von Ausweisnummern, Lesegerät zum Lesen von biometrischen Merkmalen, Tastatur zur Eingabe einer PIN außerhalb des Hauptgeräts oder des Nebengeräts in einem ungeschützten Bereich angeordnet sind.

28. Zugangs-, Überwachungs- und Kommunikationseinrichtung nach einem der Ansprüche 3 bis 27, **dadurch gekennzeichnet, dass** im Speicher des Nebengeräts vom Hauptgerät zum Nebengerät übertragene Zugangsdaten unverschlüsselt oder verschlüsselt gespeichert sind.

29. Zugangs-, Überwachungs- und Kommunikationseinrichtung nach einem der Ansprüche 3 bis 28, **dadurch gekennzeichnet, dass** im Speicher des Hauptgeräts ein Steuerprogramm zur Steuerung eines selektiven Datentransfers der lokal benötigten Zugangsdaten zum jeweiligen Nebengerät unver-

schlüsselt oder verschlüsselt gespeichert ist.

30. Zugangs-, Überwachungs- und Kommunikationseinrichtung nach einem der Ansprüche 3 bis 29, **dadurch gekennzeichnet, dass** im Speicher des Nebengeräts ein Steuerprogramm zur Abfrage und eigenen Speicherung der lokal benötigten Zugangsdaten vom Speicher des Hauptgerätes unverschlüsselt oder verschlüsselt gespeichert ist.

31. Zugangs-, Überwachungs- und Kommunikationseinrichtung nach einem der Ansprüche 3 bis 30, **dadurch gekennzeichnet, dass** im Speicher des Hauptgeräts oder Servers ein Steuerprogramm zur automatischen Übersetzung eines in einer Hochsprache verfassten Steuerprogramms in ein abstrahiertes, aber funktionsgleiches Steuerprogramm eines Nebengeräts und zur Übertragung auf das Nebengerät unverschlüsselt oder verschlüsselt gespeichert ist.

32. Zugangs-, Überwachungs- und Kommunikationseinrichtung nach einem der Ansprüche 3 bis 31, **dadurch gekennzeichnet, dass** im Speicher des Hauptgeräts oder Servers ein Konvertierungsprogramm zur Konvertierung von standardisierten Datensätzen von Zugangsdaten in komprimierte Datensätze mit komprimierten Feldinhalten aus den Zugangsdaten und Übertragung der komprimierten Zugangsdaten zum Nebengerät unverschlüsselt oder verschlüsselt gespeichert ist.

33. Zugangs-, Überwachungs- und Kommunikationseinrichtung nach einem der Ansprüche 3 bis 31, **dadurch gekennzeichnet, dass** im Speicher des Nebengeräts ein Konvertierungsprogramm zur Konvertierung von aus vom Hauptgerät oder vom Server aufbereiteten und zum Nebengerät übertragenen standardisierten Datensätzen von Zugangsdaten in komprimierte Datensätze mit komprimierten Feldinhalten aus den Zugangsdaten unverschlüsselt oder verschlüsselt gespeichert ist.

34. Zugangs-, Überwachungs- und Kommunikationseinrichtung nach einem der Ansprüche 1 bis 33, **dadurch gekennzeichnet, dass** im Speicher des Haupt-, oder Nebengeräts oder Servers ein durch den Hauptprozessor im Haupt-, Nebengerät oder Servers ausgeführter Webserver oder Webbrowser unverschlüsselt oder verschlüsselt gespeichert ist.

35. Zugangs-, Überwachungs- und Kommunikationsverfahren für wenigstens einen geschützten Bereich mit einer Zugangs-, Überwachungs- und Kommunikationseinrichtung nach einem der Ansprüche 1 bis 34, **dadurch gekennzeichnet, dass** nach Lesen von Identifikationsmerkmalen diese mit im Speicher des Haupt- oder Nebengeräts unverschlüsselt oder verschlüsselt gespeicherten und dem Haupt- oder Nebengerät zugeordneten Zugangsdaten verglichen werden.

36. Zugangs-, Überwachungs- und Kommunikationsverfahren nach Anspruch 35, **dadurch gekennzeichnet, dass** vor dem Vergleich die verschlüsselt gespeicherten Zugangsdaten entschlüsselt werden.

37. Zugangs-, Überwachungs- und Kommunikationsverfahren nach Anspruch 35 oder 36, **dadurch gekennzeichnet, dass** vom Server die dem Haupt- oder Nebengerät zugeordneten Zugangsdaten verwaltet und bei Änderungen aktualisierte Zugangsdaten über das IP-Netzwerk oder eines der weiteren Netzwerke zum Haupt- oder Nebengerät übertragen und im Speicher des Haupt- oder Nebengeräts unverschlüsselt oder verschlüsselt gespeichert werden.

38. Zugangs-, Überwachungs- und Kommunikationsverfahren nach Anspruch 37, **dadurch gekennzeichnet, dass** eine IP-Netzwerkverbindung und eine über eines der weiteren Netzwerk bestehende Verbindung oder eine IP-Netzwerkverbindung oder eine über eines der weiteren Netzwerk bestehende Verbindung zwischen dem Server und dem Hauptgerät vom Server oder vom Hauptgerät überwacht wird und nach einem Ausfall und anschließender Wiederherstellung der IP-Netzwerkverbindung und der weiteren Netzwerkverbindung oder der IP-Netzwerkverbindung oder der weiteren Netzwerkverbindung vom Server direkt oder vom Server auf Anforderung durch das Hauptgerät eine Prüfung auf geänderte Zugangsdaten durchgeführt wird und bei zwischenzeitlicher Änderung der dem Hauptgerät zugeordneten Zugangsdaten während des Ausfalls der IP-Netzwerkverbindung und der weiteren Netzwerkverbindung oder der IP-Netzwerkverbindung oder der weiteren Netzwerkverbindung aktualisierte Zugangsdaten über das IP-Netzwerk und das weitere Netzwerk oder das IP-Netzwerk oder das weitere Netzwerks zum Hauptgerät übertragen und im Speicher des Hauptgerätes unverschlüsselt oder verschlüsselt gespeichert werden.

39. Zugangs-, Überwachungs- und Kommunikationsverfahren nach einem der Ansprüche 35 bis 38, **dadurch gekennzeichnet, dass** Historiedaten im Speicher des Haupt- oder Nebengeräts unverschlüsselt oder verschlüsselt zwischengespeichert, zum Server übertragen und in einem Speicher des Servers gespeichert werden.

40. Zugangs-, Überwachungs- und Kommunikationseinrichtung nach einem der Ansprüche 35 bis 39, **dadurch gekennzeichnet, dass** Historiedaten zwischen dem Haupt- oder Nebengerät und der wenig-

stens einen Einrichtung aus der Menge Server und Gegenstelle wahlweise oder zusätzlich über ein weiteres Übertragungsmedium aus der Menge Schnittstelle, Netzwerk aus der Menge Internet-Netzwerk, Lokal Area Netzwerk (LAN), drahtloses Lokal Area Netzwerk (WLAN), Bluetooth-Netzwerk, Mobilfunkwählnetz, insbesondere GSM-Netz, oder Festwählnetz, insbesondere ISDN-Netz oder Analog-Netz generell oder bedarfsweise übertragen werden.

41. Zugangs-, Überwachungs- und Kommunikationsverfahren nach einem der Ansprüche 35 bis 40, **dadurch gekennzeichnet, dass** vom Haupt- oder Nebengerät zusätzlich oder alternativ biometrischen Merkmale als Bestandteil von Identifikationsmerkmalen erfasst und ausgewertet werden.

42. Zugangs-, Überwachungs- und Kommunikationsverfahren nach einem der Ansprüche 35 bis 41, **dadurch gekennzeichnet, dass** vom Haupt- oder Nebengerät zusätzlich oder alternativ Tastatureingaben einer PIN als Bestandteil von Identifikationsmerkmalen erfasst und ausgewertet werden.

43. Zugangs-, Überwachungs- und Kommunikationsverfahren nach einem der Ansprüche 35 bis 42, **dadurch gekennzeichnet, dass** vom Haupt- oder Nebengerät die dem Haupt- oder Nebengerät zugeordneten Zugangsdaten für einen Vergleich mit vom Lesegerät gelesenen Identifikationsmerkmalen unverschlüsselt oder verschlüsselt gespeichert und ausgewertet werden.

44. Zugangs-, Überwachungs- und Kommunikationsverfahren nach einem der Ansprüche 35 bis 43, **dadurch gekennzeichnet, dass** vom Haupt- oder Nebengerät Berechtigungsprofile als Bestandteil von Zugangsdaten unverschlüsselt oder verschlüsselt gespeichert und ausgewertet werden.

45. Zugangs-, Überwachungs- und Kommunikationsverfahren nach einem der Ansprüche 35 bis 44, **dadurch gekennzeichnet, dass** vom Haupt- oder Nebengerät Zeitprofile als Bestandteil von Zugangsdaten unverschlüsselt oder verschlüsselt gespeichert und ausgewertet werden.

46. Zugangs-, Überwachungs- und Kommunikationsverfahren nach einem der Ansprüche 35 bis 45, **dadurch gekennzeichnet, dass** vom Hauptgerät die dem Hauptgerät zugeordneten Zugangsdaten und die den angeschlossenen Nebengeräten zugeordneten Zugangsdaten für einen Vergleich mit Identifikationsmerkmalen unverschlüsselt oder verschlüsselt gespeichert und ausgewertet werden.

47. Zugangs-, Überwachungs- und Kommunikationsverfahren nach einem der Ansprüche 35 bis 46, **dadurch gekennzeichnet, dass** vom Nebengerät nur die dem Nebengerät lokal zugeordneten Zugangsdaten für einen Vergleich mit Identifikationsmerkmalen unverschlüsselt oder verschlüsselt gespeichert und ausgewertet werden.

48. Zugangs-, Überwachungs- und Kommunikationsverfahren nach einem der Ansprüche 35 bis 47, **dadurch gekennzeichnet, dass** das Haupt- oder Nebengerät mit dem Server über das IP-Netzwerk dauerhaft oder temporär zur Aktualisierung der Betriebssoftware oder der im Speicher des Haupt- oder Nebengeräts gespeicherten Zugangsdaten verbunden wird.

49. Zugangs-, Überwachungs- und Kommunikationsverfahren nach einem der Ansprüche 35 bis 48, **dadurch gekennzeichnet, dass** im Speicher des Haupt- oder Nebengeräts Identifikationsmerkmale verknüpft mit Ereignissen und optional weiter verknüpft mit Standbilddaten oder Sprachdaten oder Standbild- und Sprachdaten als Historiedaten unverschlüsselt oder verschlüsselt zwischengespeichert werden.

50. Zugangs-, Überwachungs- und Kommunikationsverfahren nach einem der Ansprüche 35 bis 49, **dadurch gekennzeichnet, dass** mittels eines Türöffnertreibers im Haupt- oder Nebengerät unverschlüsselte oder verschlüsselte Türöffnungssignale generiert und an ein abgesetztes Türöffnerschaltmodul drahtlos oder drahtgebunden übertragen werden.

51. Zugangs-, Überwachungs- und Kommunikationsverfahren nach einem der Ansprüche 35 bis 50, **dadurch gekennzeichnet, dass** über eine der Schnittstellen des Haupt- oder Nebengeräts wenigstes ein applikationsspezifisches Modul mit einer Schnittstelle zum Haupt- oder Nebengerät und wenigstens einer weiteren Schnittstelle zu einer Peripherie aus der Menge Peripherieanlage aus der Menge Einbruchmeldeanlage, Brandmeldeanlage, Alarmanlage, Heizung-, Lüftung-, Klimaanlage, Beleuchtungsanlage, Aufzugsanlage und einem Peripheriegerät aus der Menge Feuermelder, Rauchmelder, Gasmelder, Wassermelder, Feuchtemelder, Temperaturmelder, Bewegungsmelder, Öffnungsmelder, Glasbruchmelder, Dämmerungsmelder, Sensor als Eingabegeräte und optische Alarmgeber, akustische Alarmgeber, Wählgeräte, Schaltelemente, Heizung-, Lüftung-, Klimasteuerungen, Beleuchtungssteuerungen, Aufzugssteuerungen als Ausgabegeräten gesteuert wird.

52. Zugangs-, Überwachungs- und Kommunikationsverfahren nach Anspruch 51, **dadurch gekennzeichnet, dass** durch das applikationsspezifische Modul Protokolle zwischen den Schnittstellen um-

gesetzt werden..

53. Zugangs-, Überwachungs- und Kommunikationsverfahren nach Anspruch 51, **dadurch gekennzeichnet, dass** durch das applikationsspezifische Modul eine Signalwandlung aus der Menge Analog/Digital-Wandlung, Digital/Analogwandlung, Impedanzwandlung, Schnittstellenwandlung, vorgenommen wird.

54. Zugangs-, Überwachungs- und Kommunikationsverfahren nach einem der Ansprüche 35 bis 53, **dadurch gekennzeichnet, dass** durch einen Hauptprozessor des Steuergeräts des Haupt- oder Nebengeräts eine Datenverarbeitung aus der Menge Codierung oder Dekodierung von Zugangs-, Sprach- und Bilddaten zum Beschreiben oder Lesen des Speichers; Senden oder Empfangen von Daten über das IP-Netzwerk oder wenigstens ein weiteres Netzwerk oder wenigstes eine Schnittstelle; Auswerten von Daten, die über das IP-Netzwerk oder das wenigstens eine weitere Netzwerk oder die wenigstens Schnittstelle empfangen werden; Auswerten von empfangenen Daten von Peripherieanlagen oder Peripheriegeräten; Steuern von Peripherieanlagen oder Peripheriegeräten; autarkes Steuern von Peripherieanlagen oder Peripheriegeräten auf Basis von Peripherieanlagen oder Peripheriegeräten empfangener Daten, Generierung von verschlüsselten oder unverschlüsselten Türöffnungssignalen durchgeführt wird.

55. Zugangs-, Überwachungs- und Kommunikationsverfahren nach einem der Ansprüche 35 bis 54, **dadurch gekennzeichnet, dass** im Hauptprozessor im Steuergerät des Hauptgerätes ein ein Betriebssystem-unabhängig übergreifendes Steuerprogramm ausgeführt wird.

56. Zugangs-, Überwachungs- und Kommunikationsverfahren nach Anspruch 55, **dadurch gekennzeichnet, dass** als Betriebssystem-unabhängig übergreifendes Steuerprogramm JAVA ausgeführt wird.

57. Zugangs-, Überwachungs- und Kommunikationsverfahren nach einem der Ansprüche 35 bis 56, **dadurch gekennzeichnet, dass** im Haupt- oder Nebengerätgeräte Codecs für aus der Menge Sprachsignale, Standbildsignale und Bewegtbildsignale unverschlüsselt oder verschlüsselt gespeichert, bedarfsweise aktualisiert und durch den Hauptprozessor ausgeführt werden.

58. Zugangs-, Überwachungs- und Kommunikationsverfahren nach einem der Ansprüche 35 bis 57, **dadurch gekennzeichnet, dass** im Haupt- oder Nebengerät eine Menü-geführte Bedienanweisung unverschlüsselt oder verschlüsselt gespeichert und ausgeführt wird.

59. Zugangs-, Überwachungs- und Kommunikationsverfahren nach einem der Ansprüche 35 bis 58, **dadurch gekennzeichnet, dass** im Haupt- oder Nebengerät Steuerprogramme zur Durchführung von aus der Menge Inbetriebnahme-, Einstell- und Wartungsarbeiten unverschlüsselt oder verschlüsselt gespeichert und ausgeführt werden.

60. Zugangs-, Überwachungs- und Kommunikationsverfahren nach einem der Ansprüche 35 bis 59, **dadurch gekennzeichnet, dass** vom Hauptgerät oder vom Server zum Nebengerät Zugangsdaten übertragen und im Speicher des Nebengeräts unverschlüsselt oder verschlüsselt gespeichert werden.

61. Zugangs-, Überwachungs- und Kommunikationsverfahren nach einem der Ansprüche 35 bis 61, **dadurch gekennzeichnet, dass** im Hauptgerät ein Steuerprogramm zur Steuerung eines selektiven Datentransfers der lokal benötigten Zugangsdaten zum jeweiligen Nebengerät unverschlüsselt oder verschlüsselt gespeichert und ausgeführt wird.

62. Zugangs-, Überwachungs- und Kommunikationsverfahren nach einem der Ansprüche 35 bis 61, **dadurch gekennzeichnet, dass** im Nebengerät ein Steuerprogramm zur Abfrage und eigenen Speicherung der lokal benötigten Zugangsdaten vom Speicher des Hauptgerätes unverschlüsselt oder verschlüsselt gespeichert und ausgeführt wird.

63. Zugangs-, Überwachungs- und Kommunikationsverfahren nach einem der Ansprüche 35 bis 61, **dadurch gekennzeichnet, dass** im Hauptgerät oder Server ein Steuerprogramm zur automatischen Übersetzung eines in einer Hochsprache verfassten Steuerprogramms des Hauptgerätes in ein abstrahiertes aber funktionsgleiches Steuerprogramm des jeweiligen Nebengerätes und zur Übertragung auf das Nebengerät unverschlüsselt oder verschlüsselt gespeichert und ausgeführt wird.

64. Zugangs-, Überwachungs- und Kommunikationsverfahren nach einem der Ansprüche 35 bis 63, **dadurch gekennzeichnet, dass** im Hauptgerät oder Server ein Steuerprogramm zur Konvertierung einer Datenbank mit standardisierten Datensätzen aus dem Hauptgerät oder dem Server in eine Datenbank mit komprimierten Datensätzen des jeweiligen Nebengeräts und zur Übertragung auf das jeweilige Nebengerät unverschlüsselt oder verschlüsselt gespeichert und ausgeführt wird.

65. Zugangs-, Überwachungs- und Kommunikationsverfahren nach einem der Ansprüche 35 bis 64, **da-**

durch gekennzeichnet, dass im Nebengerät ein Konvertierungsprogramm zur Konvertierung von aus vom Hauptgerät oder vom Server aufbereiteten und zum Nebengerät übertragenen standardisierten Datensätzen von Zugangsdaten in komprimierte Datensätze mit komprimierten Feldinhalten aus den Zugangsdaten unverschlüsselt oder verschlüsselt gespeichert und ausgeführt wird.

66. Zugangs-, Überwachungs- und Kommunikationsverfahren nach einem der Ansprüche 35 bis 65, **dadurch gekennzeichnet, dass** im Haupt- oder Nebengerät oder Server ein Webserver unverschlüsselt oder verschlüsselt gespeichert und ausgeführt wird.

67. Zugangs-, Überwachungs- und Kommunikationsverfahren nach einem der Ansprüche 35 bis 66, **dadurch gekennzeichnet, dass** im Haupt- oder Nebengerät oder Server ein Webbrowser ausgeführt wird.

68. Zugangs-, Überwachungs- und Kommunikationsverfahren nach einem der Ansprüche 35 bis 67, **dadurch gekennzeichnet, dass** mittels des Webbrowser wahlweise die Gesamthierarchie der Einrichtung oder einzelne Ebenen oder Komponenten aus der Menge Server, Hauptgerät, Nebengerät, Peripherieanlage Peripheriegerät dargestellt werden.

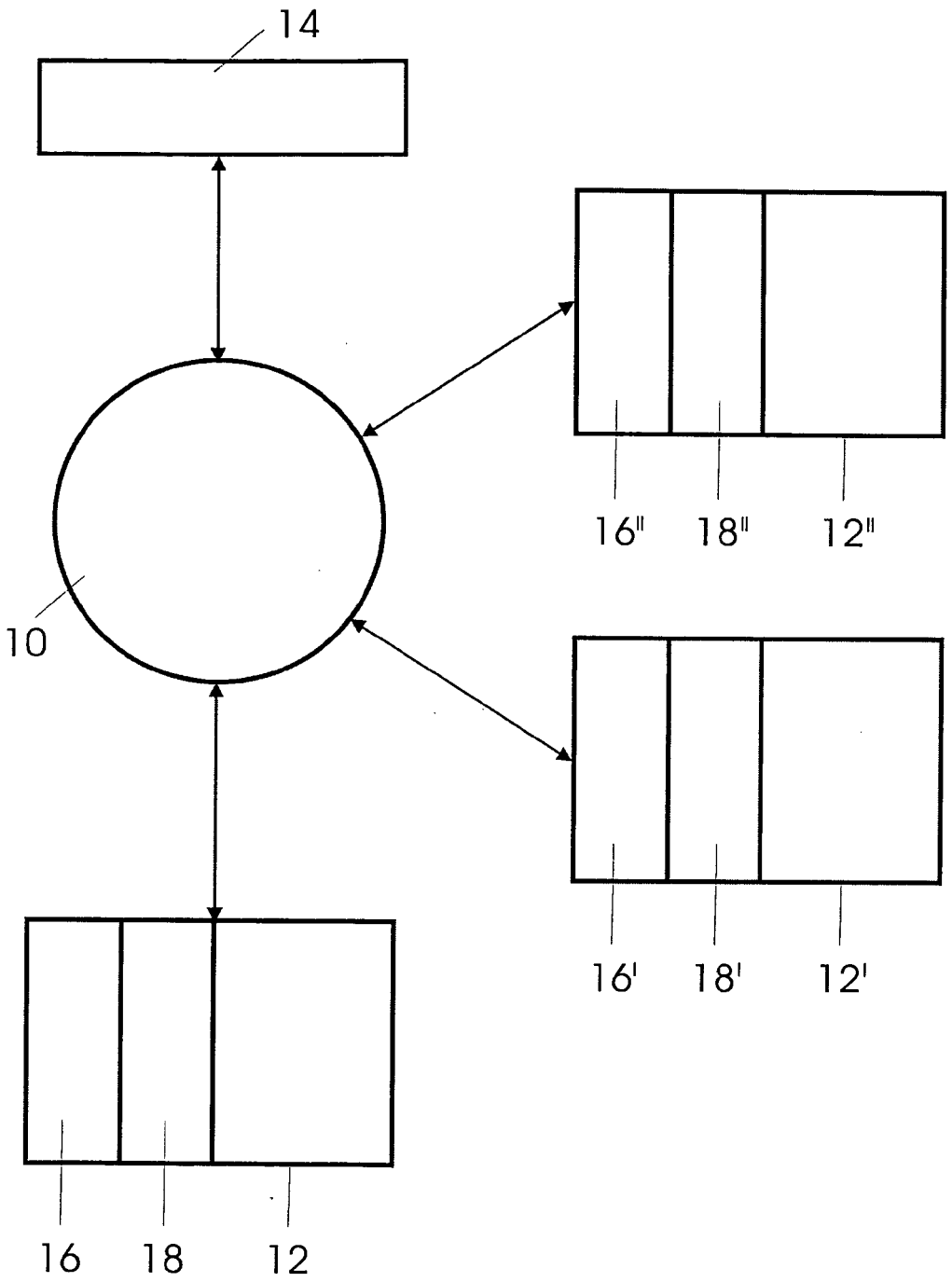

Fig.1

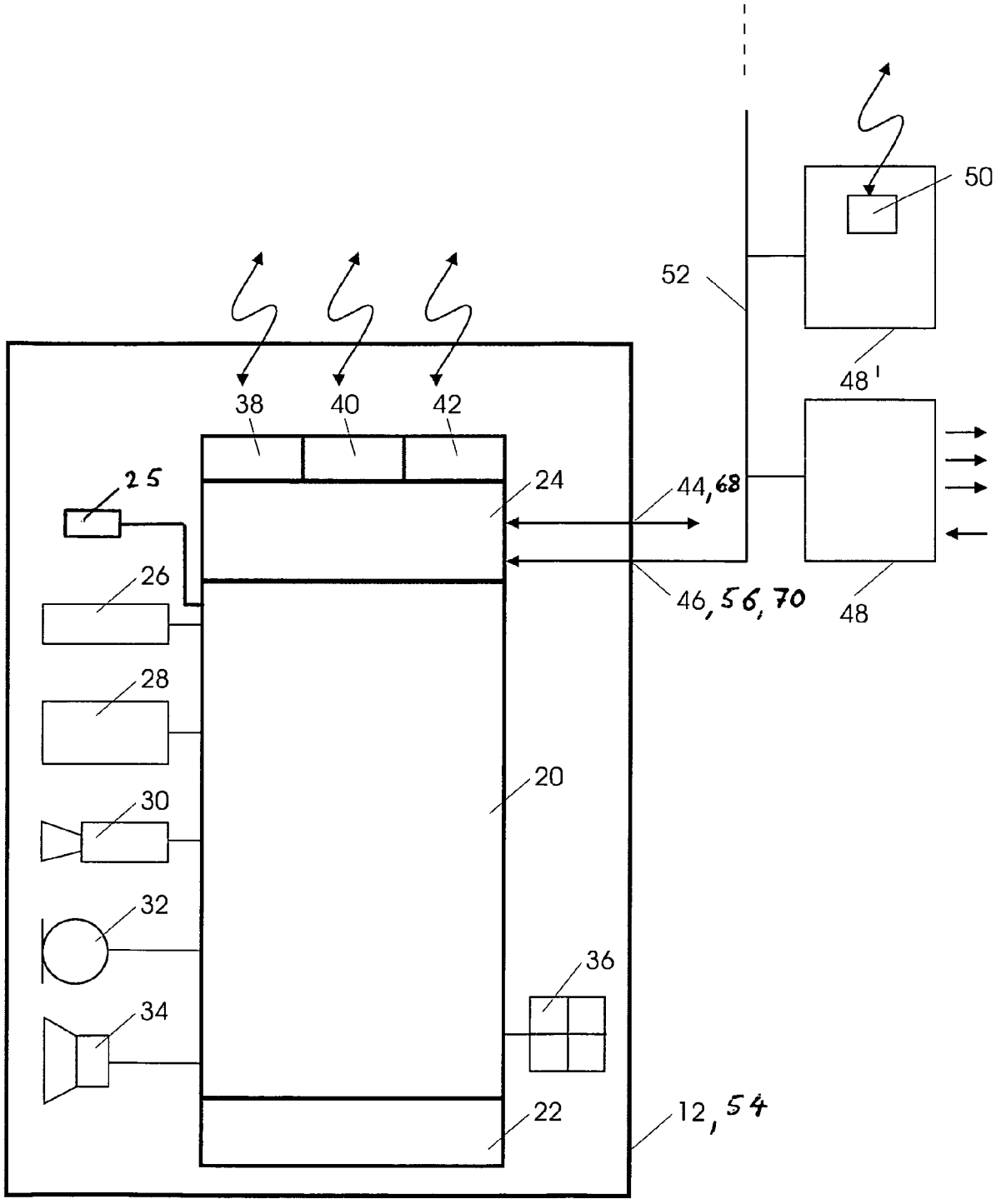

Fig.2

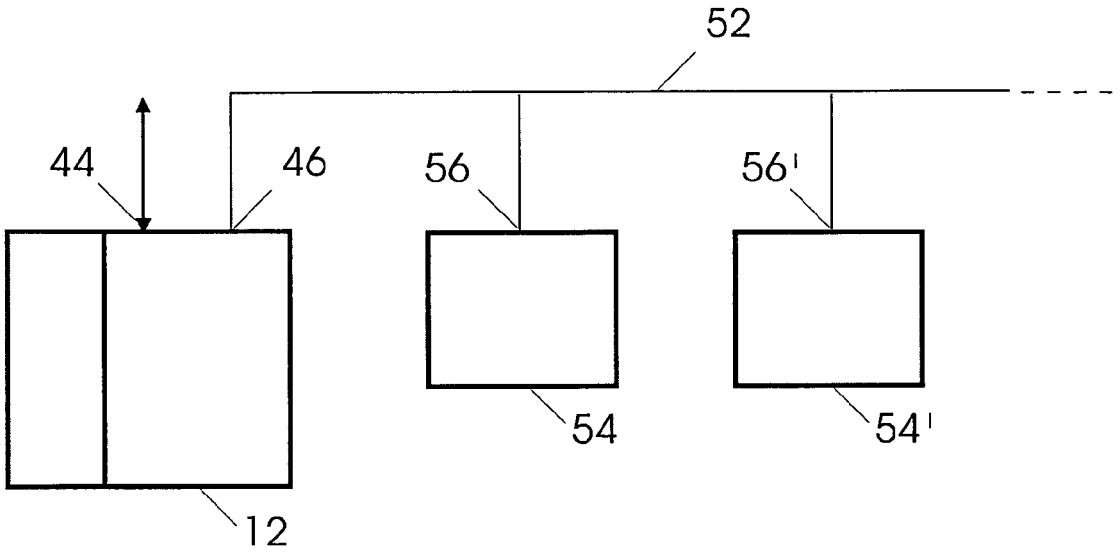

Fig.3

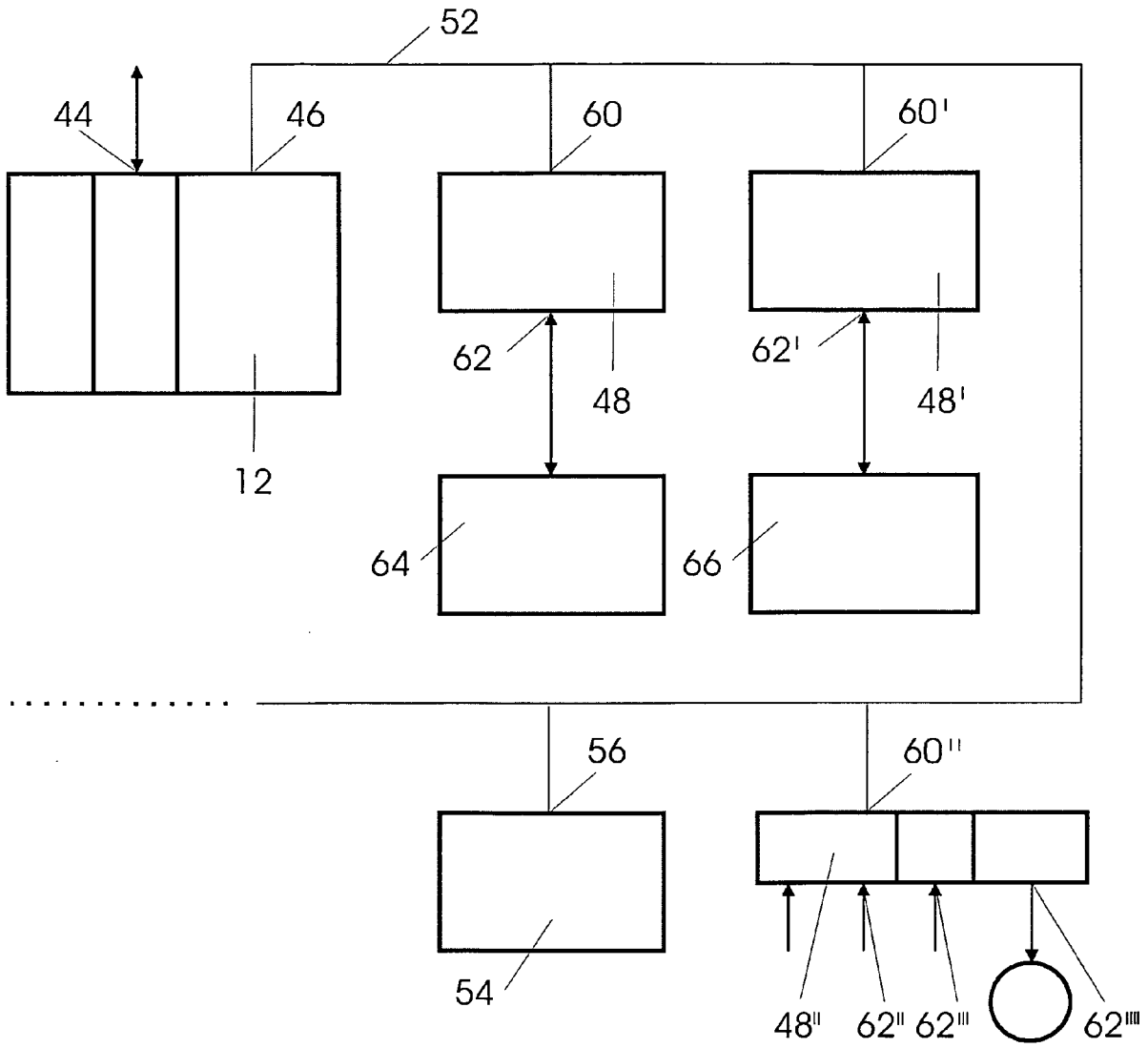

Fig.4

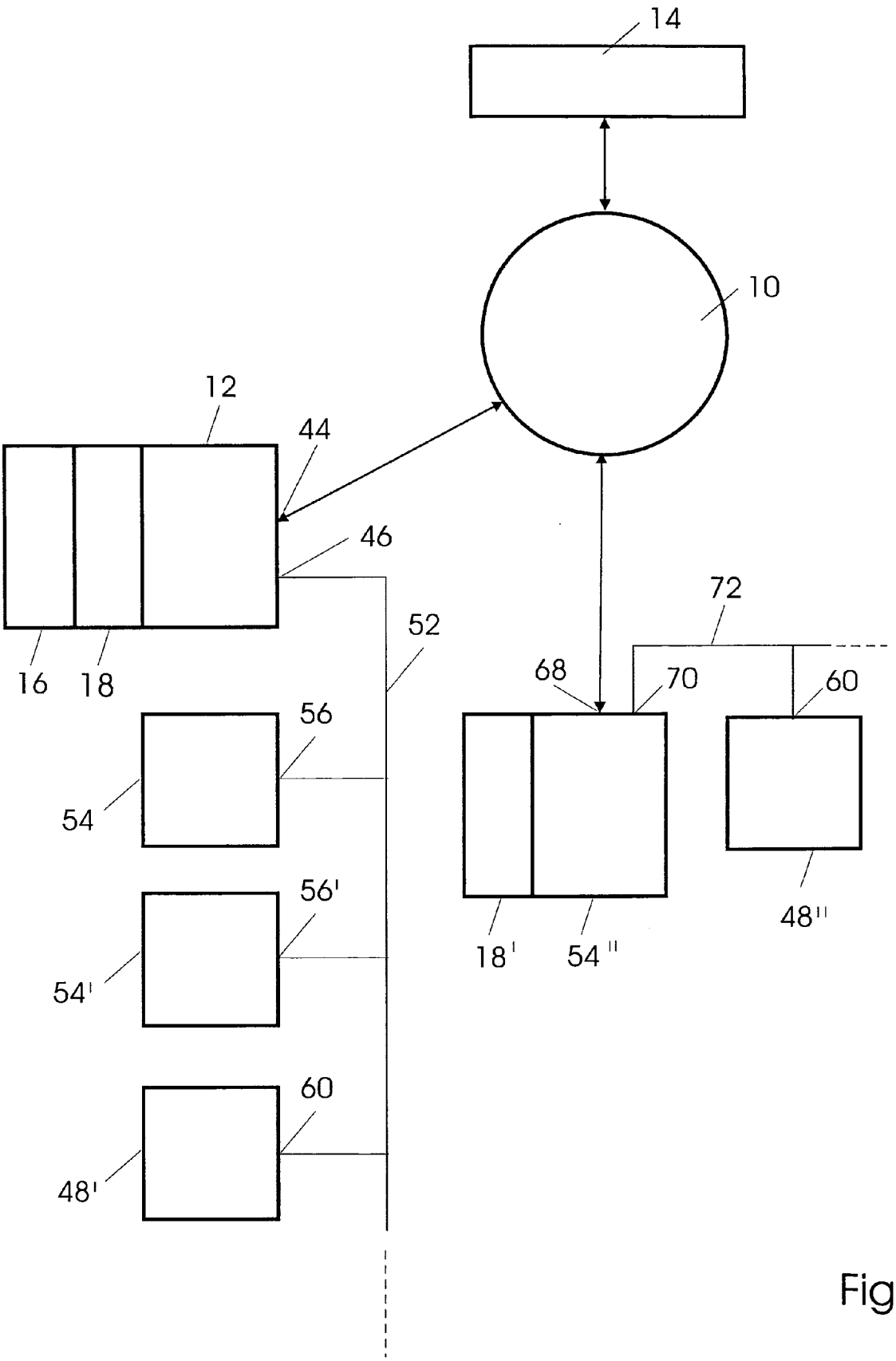

Fig.5