(19) Deutsches Patent- und Markenamt

(10) **DE 10 2012 213 155 A1** 2014.02.13

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2012 213 155.8**
(22) Anmeldetag: **26.07.2012**
(43) Offenlegungstag: **13.02.2014**

(51) Int Cl.: ***G06F 21/00*** (2013.01)

(71) Anmelder:
Siemens Aktiengesellschaft, 80333, München, DE

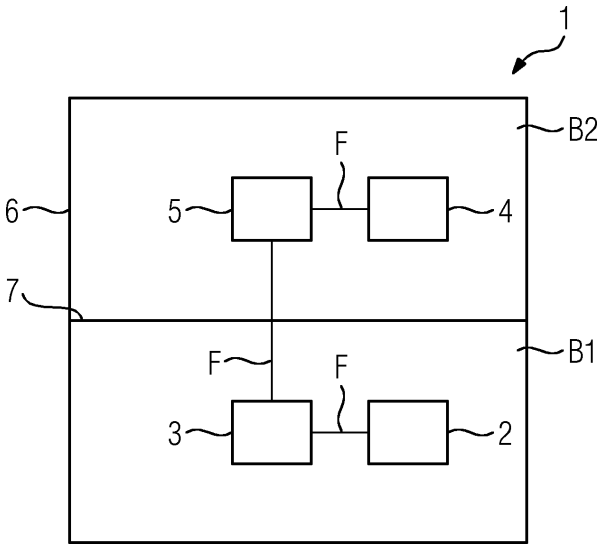
(72) Erfinder:
Falk, Rainer, Dr., 85586, Poing, DE; Fries, Steffen, 85598, Baldham, DE

Prüfungsantrag gemäß § 44 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Vorrichtung mit Sicherheitseinheiten in unterschiedlich geschützten Bereichen**

(57) Zusammenfassung: Es wird eine Vorrichtung mit Sicherheitseinheiten in unterschiedlich geschützten Bereichen vorgeschlagen. Dabei weisen ein stärker geschützter Bereich eine erste Sicherheitseinheit zur Ausführung einer Anzahl von ersten Sicherheitsfunktionen für eine zugeordnete erste Datenverarbeitungseinheit und ein schwächer geschützter Bereich eine zweite Sicherheitseinheit zur Ausführung einer Anzahl von zweiten Sicherheitsfunktionen für eine zugeordnete zweite Datenverarbeitungseinheit auf. Die zweiten Sicherheitsfunktionen umfassen zumindest eine freizuschaltende Sicherheitsfunktion, wobei die erste Sicherheitseinheit dazu eingerichtet ist, die zumindest eine freizuschaltende Sicherheitsfunktion der zweiten Sicherheitseinheit mittels eines vorbestimmten Freischaltsignals freizuschalten.
Dadurch, dass die zumindest eine freizuschaltende Sicherheitsfunktion der zweiten Sicherheitseinheit in dem schwächer geschützten Bereich durch die erste Sicherheitseinheit des stärker geschützten Bereichs freigeschaltet werden muss, wird der höhere Schutz des stärker geschützten Bereiches für die in dem schwächer geschützten Bereich angeordnete zweite Sicherheitseinheit mitgenutzt. Damit wird die Sicherheit der Vorrichtung insgesamt erhöht.



Beschreibung

[0001] Die vorliegende Erfindung betrifft eine Vorrichtung mit Sicherheitseinheiten in unterschiedlich geschützten Bereichen.

[0002] Vorrichtungen, wie eingebettete Systeme (Embedded Systems), wie z.B. Steuergeräte, intelligente Zähler (Smart Meter) oder Feldgeräte, realisieren häufig kryptographische Sicherheitsfunktionen. Dazu muss ein kryptographischer Schlüssel auf der Vorrichtung so gespeichert werden, dass er auch bei direktem Zugriff auf die Vorrichtung nicht bzw. nicht mit praktikablem Aufwand auslesbar ist. Gleichermaßen besteht häufig der Wunsch nach einer modularen Vorrichtung, bei welcher z.B. ein Kommunikationsmodul wechselbar ist. Durch einen Tausch des Kommunikationsmoduls können unterschiedliche Kommunikationsstandards, wie z.B. Ethernet, Power Line Communication (PLC), WLAN (Wireless Local Area Network) oder UMTS (Universal Mobile Telecommunications System), unterstützt werden.

[0003] Ferner sind intelligente Zähler (Smart Meter) bekannt, die insbesondere aus einem eichpflichtigen Modul und aus einem wechselbaren Kommunikationsmodul bestehen.

[0004] Bei solchen intelligenten Zählern kann auch ein Zusatzmodul mittels eines Plug-and-Play-Protokolls an ein Basismodul angebunden werden. Dabei speichert das Zusatzmodul die IP-Adresse des Basismoduls als Datenquelle für die Messwerte.

[0005] Ferner kann ein solches Smart Meter auch mehrere Plomben aufweisen, insbesondere eine Eichplombe und eine Betriebsplombe. Nach Brechen der jeweiligen Plombe sind unterschiedliche Funktionalitäten zugänglich. Das Basismodul kann kryptographische Operationen durchführen, z.B. eine Signatur eines Messwertes berechnen. Ebenso kann das Zusatzmodul andere kryptographische Operationen durchführen, z.B. die Verschlüsselung der Datenkommunikation.

[0006] Es ist durch das derzeit entstehende Schutzprofil (Protection Profile) und die dazugehörige technische Richtlinie des Bundesamtes für Sicherheit in der Informationstechnik (BSI) Deutschlands bekannt, dass ein Smart Meter ein Sicherheitsmodul aufweist, welches für die kryptographische Sicherung einer WAN-Verbindung (WAN, Wide Area Network) über SSL/TLS vorgesehen ist. Die Messeinheit des Smart Meters, welche dem Kommunikationsmodul Messwerte bereitstellt, kann die Messwerte signieren. Ferner ist bekannt, dass das Sicherheitsmodul des Kommunikationsmoduls die digitale Signatur empfangener Messdaten prüft und die Daten erneut signiert, bevor diese an ein Back-End-System oder einen Back-End-Server übertragen werden.

[0007] Des Weiteren sind Hardware-Security-ICs bekannt, die ähnlich wie eine Chipkarte kryptographische Schlüssel speichern und kryptographische Operationen durchführen können. Solche Hardware-Security-ICs verfügen herkömmlicherweise über einen Schutz gegen unbefugten Eingriff (Tamperschutz) des ICs selbst. Beispiele hierfür sind die Verwendung einer Passivierungsschicht und Sensoren auf dem IC, um ein Öffnen des ICs zu erkennen.

[0008] Insgesamt sind typische Maßnahmen eines Security-ICs der Einsatz von Sensoren, um ungewöhnliche Betriebszustände zu erfassen, z.B. über Licht- oder Temperaturerfassung, fehlererkennende bzw. fehlerkorrigierende Schutzmaßnahmen für Speicher und Buskommunikation, redundante Ausführungen von Befehlen, verschlüsselte Daten und Buskommunikation, unregelmäßige Verdrahtungsmasken, Passivierung oder Schutzschichten auf der Chipoberfläche oder modifizierte Fertigungsverfahren, bei denen sensitive Daten in "tieferen" Schichten des Halbleiterbausteins liegen.

[0009] Bei herkömmlichen Personalcomputern (PCs) ist bekannt, dass durch einen Schalter ein Öffnen des Gehäuses des PCs detektiert wird. Dadurch kann z.B. eine Alarmnachricht an einen Nutzer oder einen Administrator erzeugt werden. Eine solche Alarmnachricht ist auch als Case Opening Warning bekannt.

[0010] Bei Feuermeldern oder Diebstahls-/Einbruchmeldern sind Schalter bekannt, die ein Öffnen des Gehäuses erkennen oder ein Entfernen des Meldegerätes, z.B. Abschrauben von einer Wand.

[0011] Des Weiteren sind tampergeschützte Sicherheitsmodule (Hardware Security Module, HSM) bekannt. Solche tampergeschützten Sicherheitsmodule speichern kryptographische Schlüssel und führen kryptographische Operationen aus. Diese Sicherheitsmodule können über physikalische Tamperschutzsensoren verfügen. So können beispielsweise Licht, Ionenstrahlung und Temperatur durch Sensoren überwacht werden. Ferner kann ein mechanisches Eindringen durch eine Tamperschutzfolie (Wire Mesh) oder Schalter erkannt werden. Bei einem unbefugten Eingriff können gespeicherte Schlüssel gelöscht werden.

[0012] Ferner bietet die Firma Maxim sichere Speicherbausteine an, an welche Tampersensoren anschließbar sind. Bei einem erkannten unbefugten Eingriff (Tamper-Event) werden gespeicherte Daten gelöscht. Dabei wird allerdings eine Backup-Batterie benötigt, damit auch ohne externe Stromversorgung gespeicherte Daten gelöscht werden können. Im Betrieb werden Speicherwerte laufend gewechselt, um ein physikalisches "Einbrennen" der Schlüsselbits in den Halbleiter zu verhindern. Ein solcher

sicherer Speicher kann z.B. innerhalb eines vergossenen, durch ein Tamper-Mesh-geschütztes Sicherheitsmodul (Security Module) zur sicheren Schlüsselspeicherung verwendet werden. Ein Beispiel hier ist das Produkt Maxim DS3645.

[0013] Ferner ist es bekannt, ein Messgerät oder einen intelligenten Zähler zu verplomben. Bei einer Ablesung kann anhand der Plombe erkannt werden, ob eine Manipulation innerhalb des verplombten Bereichs erfolgte. Auch ist bekannt, Sicherheitssiegel oder Sicherheits-Label aufzukleben, mit denen ein Öffnen eines Gehäuses erkannt werden kann.

[0014] Der intelligente Zähler selbst kann vor Manipulationen durch spezielle Tamperschutzmaßnahmen geschützt werden. Dazu können z.B. speziell verschlossene, nicht öffnen- und wiederverschließbare Gehäuse verwendet werden. Beispielsweise werden bei solchen nicht öffnen- und wiederverschließbaren Gehäusen keine Schrauben, verklebte Gehäuseschalen oder nicht zu öffnende Snap-in-Einrastungen verwendet. Auch ist bekannt, dass durch Sensoren eine Bewegung oder Neigung eines intelligenten Zählers sowie ein Entfernen von einer Befestigung detektiert werden kann. Auch ein GPS-Empfänger kann eingebaut werden, so dass der intelligente Zähler anhand der mit Hilfe des GPS-Satelliten-Navigationssystems ermittelten Position erkennen kann, ob es sich noch am vorgesehenen Ort befindet. Dies wird auch als Location-Lock bezeichnet.

[0015] Weiter können in einem intelligenten Zähler auch Sicherheitsbausteine (ICs) verwendet werden, um Programmcode, Konfigurationsdaten und Messwerte manipulationsgeschützt zu speichern. Auch können einzelne Bausteine oder ein ganzer intelligenter Zähler mit einem physikalischen Manipulationsschutz versehen werden, z.B. indem sie in Epoxydharz vergossen werden. Ebenfalls ist es möglich, die Platine oder einen Teil der Platine des intelligenten Zählers mit Metallhüllen abzudecken, die als Kondensator wirken. Werden diese Platten entfernt, so ändert sich die Kapazität und ein Tamperalarm kann ausgelöst werden.

[0016] Das Dokument US 2007/103334 A beschreibt die Erkennung einer Bewegung eines intelligenten Zählers von mehr als einer vorgegebenen Entfernung als Tamper-Event. In diesem Dokument wird auch erwähnt, dass bei einer Stromunterbrechung durch Vergleich des Stromverbrauchsprofils vor und nach der Stromunterbrechung ein Vertauschen eines Stromzählers erkannt werden kann, so dass eine Tampermeldung erzeugt wird.

[0017] Weiterhin ist bekannt, einen Stromdiebstahl dadurch zu erkennen, dass mehrere Messgeräte installiert werden, z.B. im Haushalt und in der Verteilstation, um einen Stromdiebstahl auf der dazwischen liegenden Stromübertragungsstrecke anhand einer Abweichung der gemessenen Strommenge zu erkennen. Ein intelligenter Zähler zur Stromverbrauchsmessung kann durch Sensoren Strom, Spannung und Phase messen, um den Stromverbrauch zu ermitteln. Dabei kann es abweichende Messgrößen als Manipulationsversuche erkennen. So kann z.B. bei einer Stromverbrauchsmessung ein rückwärts fließender Strom erkannt werden, oder auch eine offene Kabelverbindung kann erkannt werden. Ferner ist bekannt, bei fernauslesbaren Zellen die erfassten Messdaten kryptographisch geschützt zu einem Messwerte-Erfassungsserver zu übertragen.

[0018] Demzufolge ist es eine Aufgabe der vorliegenden Erfindung, eine verbesserte Vorrichtung mit Sicherheitseinheiten in unterschiedlich geschützten Bereichen zu schaffen.

[0019] Demgemäß wird eine Vorrichtung mit Sicherheitseinheiten in unterschiedlich geschützten Bereichen vorgeschlagen. Dabei weist ein stärker geschützter Bereich eine erste Sicherheitseinheit zur Ausführung einer Anzahl von ersten Sicherheitsfunktionen für eine zugeordnete erste Datenverarbeitungseinheit und ein schwächer geschützter Bereich eine zweite Sicherheitseinheit zur Ausführung einer Anzahl von zweiten Sicherheitsfunktionen für eine zugeordnete zweite Datenverarbeitungseinheit auf. Die zweiten Sicherheitsfunktionen umfassen zumindest eine freizuschaltende Sicherheitsfunktion, wobei die erste Sicherheitseinheit dazu eingerichtet ist, die zumindest eine freizuschaltende Sicherheitsfunktion der zweiten Sicherheitseinheit mittels eines vorbestimmten Freischaltsignals freizuschalten.

[0020] Dadurch, dass die zumindest eine freizuschaltende Sicherheitsfunktion der zweiten Sicherheitseinheit in dem schwächer geschützten Bereich durch die erste Sicherheitseinheit des stärker geschützten Bereichs freigeschaltet werden muss, wird der höhere Schutz des stärker geschützten Bereiches für die in dem schwächer geschützten Bereich angeordnete zweite Sicherheitseinheit mitgenutzt. Damit wird die Sicherheit der Vorrichtung insgesamt erhöht.

[0021] Insbesondere sind alle Sicherheitsfunktionen der zweiten Sicherheitseinheit freizuschaltende Sicherheitsfunktionen. Dann kann die in dem schwächer geschützten Bereich angeordnete zweite Sicherheitseinheit nur zusammen mit der stärker geschützten Sicherheitseinheit des stärker geschützten Bereiches genutzt werden. Der Schutz der unterschiedlich geschützten Bereiche ist relativ zueinander zu sehen, d.h. der stärker geschützte Bereich hat einen stärkeren Schutz als der schwächer geschützte Bereich. Der Schutz umfasst insbesondere den physikalischen Schutz vor unbefugtem Eingriff.

[0022] Die freizuschaltende Sicherheitsfunktion ist ohne eine Freischaltung durch das Freischaltsignal nicht aktiviert und kann demnach nicht ausgeführt werden. Die freizuschaltende Sicherheitsfunktion wird durch das Freischaltsignal freigeschalten und somit aktiviert.

[0023] Die jeweilige Sicherheitseinheit ist insbesondere eine kryptographische Sicherheitseinheit. Damit sind die von den Sicherheitseinheiten ausführbaren Sicherheitsfunktionen insbesondere kryptographische Sicherheitsfunktionen, welche insbesondere Verschlüsselung und digitale Signatur umfassen.

[0024] Bei einer Ausführungsform umfasst das vorbestimmte Freischaltsignal zum Freischalten der zumindest einen freizuschaltenden Sicherheitsfunktion der zweiten Sicherheitseinheit zumindest einen Sicherheitsparameter. Der Sicherheitsparameter ist insbesondere ein Passwort, eine Persönliche Identifikationsnummer oder ein kryptographischer Parameter.

[0025] Durch die Verwendung des Sicherheitsparameters als Teil des Freischaltsignals wird das Freischalten der zweiten Sicherheitseinheit gesichert. Des Weiteren kann das Freischaltsignal auch verschlüsselt übertragen werden, so dass die Sicherheit weiter erhöht wird.

[0026] Bei einer weiteren Ausführungsform ist die Vorrichtung als ein intelligenter Zähler, insbesondere als ein intelligenter Stromzähler ausgebildet.

[0027] Bei einer weiteren Ausführungsform ist die Vorrichtung als ein intelligenter Gaszähler ausgebildet.

[0028] Bei einer weiteren Ausführungsform ist die Vorrichtung als ein Feldgerät, insbesondere für eine Ampelsteuerung, ausgebildet.

[0029] Bei einer weiteren Ausführungsform ist die Vorrichtung als ein Steuergerät, insbesondere für ein Kraftfahrzeug, ausgebildet.

[0030] Bei einer weiteren Ausführungsform ist die erste Sicherheitseinheit dazu eingerichtet, einen Zustand der zweiten Sicherheitseinheit zu überwachen und die zumindest eine freizuschaltende Sicherheitsfunktion der zweiten Sicherheitseinheit in Abhängigkeit des überwachten Zustands freizuschalten.

[0031] Somit wird das Freischalten der zweiten Sicherheitseinheit ereignisgetriggert durchgeführt. Somit muss die freizuschaltende Sicherheitsfunktion der zweiten Sicherheitseinheit nicht bei einer jeden Anwendung freigeschaltet werden.

[0032] Bei einer weiteren Ausführungsform ist die erste Sicherheitseinheit dazu eingerichtet, die zumindest eine freizuschaltende Sicherheitsfunktion der zweiten Sicherheitseinheit bei zumindest einem der folgenden Ereignisse mittels des vorbestimmten Freischaltsignals freizuschalten:

– Hochfahren der zweiten Sicherheitseinheit,
– Batteriewechsel einer Batterie der zweiten Sicherheitseinheit,
– jeweils nach Ablauf einer vorbestimmten Zeitdauer im Betrieb der zweiten Sicherheitseinheit,
– bei einem Aufbau einer Datenverbindung der zweiten Sicherheitseinheit zu einer externen Einrichtung.

[0033] Bei einer weiteren Ausführungsform ist der stärker geschützte Bereich verplombt oder vergossen. Der stärker geschützte Bereich ist insbesondere mittels eines Epoxydharzes vergossen.

[0034] Verplomben oder Vergießen sind technisch einfach realisierbare Möglichkeiten, einen Bereich der Vorrichtung stärker zu schützen als andere.

[0035] Bei einer weiteren Ausführungsform sind der stärker geschützte Bereich und der schwächer geschützte Bereich getrennt.

[0036] Durch die Trennung des stärker geschützten Bereiches und des schwächer geschützten Bereiches können diese auch zueinander modular aufgebaut sein. Durch den modularen Aufbau kann beispielsweise ein eichpflichtiger Messsystem-Teil in dem stärker geschützten Bereich mit unterschiedlichen Kommunikationsmodulen in dem schwächer geschützten Bereich kombiniert werden. Durch die Verwendung unterschiedlicher Kommunikationsmodule können auch unterschiedliche Kommunikationsstandards, wie beispielsweise WLAN, WiFi, Ethernet und dergleichen, eingesetzt werden.

[0037] Bei einer weiteren Ausführungsform integriert ein Gehäuse der Vorrichtung den stärker geschützten Bereich und den schwächer geschützten Bereich, wobei eine Gehäusetrennwand den stärker geschützten Bereich und den schwächer geschützten Bereich trennt.

[0038] Bei einer weiteren Ausführungsform sind die erste Sicherheitseinheit und die zweite Sicherheitseinheit dazu eingerichtet, dass die zweite Sicherheitseinheit eine Anfrage-Antwort-Authentisierung (Challenge-Response-Authentication) der ersten Sicherheitseinheit durchführt, wobei die zweite Sicherheitseinheit ferner dazu eingerichtet ist, das Freischaltsignal aus der Antwort der ersten Sicherheitseinheit zu extrahieren.

[0039] Bei dieser Ausführungsform muss das Freischaltsignal nicht extra zu der zweiten Sicherheits-

einheit übertragen werden, da das Freischaltsignal aus der Antwort der ersten Sicherheitseinheit extrahierbar ist. Beispielsweise wird dann die digitale Signatur einer Nachricht mit Messdaten nicht nur dazu verwendet, dass ein mit dem schwächer geschützten Bereich verbundener Back-End-Server eine empfangene Energieverbrauchsinformation in Abhängigkeit der Messwerte prüfen kann, sondern innerhalb der Vorrichtung selbst durch die zweite Datenverarbeitungseinheit, um die zweite Sicherheitseinheit freizuschalten oder deren Freischaltung aufrechtzuerhalten.

[0040] In einer anderen Variante kann die zweite Sicherheitseinheit auch als ein eingebettetes Modul ausgebildet sein, welches einen sicheren Boot-Vorgang durch Signieren einer Attestation eines PCR-Registers (PCR, Platform Configuration Register) attestiert. Diese Attestation wird dann der zweiten Sicherheitseinheit bereitgestellt und durch diese geprüft.

[0041] Bei einer weiteren Ausführungsform sind die erste Sicherheitseinheit und die zweite Sicherheitseinheit dazu eingerichtet, dass die erste Sicherheitseinheit die Identität der zweiten Sicherheitseinheit authentisiert und in Abhängigkeit der authentisierten Identität der zweiten Sicherheitseinheit ein Bestätigungssignal zur Bestätigung einer Verbindung zwischen der ersten Sicherheitseinheit und der zweiten Sicherheitseinheit generiert. Zur Authentisierung wird insbesondere eine Anfrage-Antwort-Authentisierung (Challenge-Response-Authentication) eingesetzt.

[0042] Dabei ist das generierte Bestätigungssignal zumindest Teil des Freigabesignals oder das Freigabesignal ist zumindest teilweise aus dem generierten Bestätigungssignal ableitbar.

[0043] Durch das Bestätigungssignal kann vorteilhafterweise eine vorhandene Verbindung zwischen der ersten Sicherheitseinheit und der zweiten Sicherheitseinheit bestätigt und verifiziert werden. Liegt eine solche Verbindung vor, so kann ein unbefugter Eingriff auf die Verbindung zwischen der ersten Sicherheitseinheit und der zweiten Sicherheitseinheit ausgeschlossen werden.

[0044] Das Bestätigungssignal ist insbesondere ein kryptographisch geschütztes Bestätigungssignal und kann auch als Assertion bezeichnet werden. Die Assertion ist eine Datenstruktur, welche mittels einer kryptographischen Prüfsumme der ersten Sicherheitseinheit geschützt ist. Dazu kann eine digitale Signatur oder ein Message-Authentication-Code eingesetzt werden. Die Datenstruktur der Assertion umfasst vorzugsweise eine Identifizierungsinformation der ersten Sicherheitseinheit, eine Identifizierungsinformation der zweiten Sicherheitseinheit sowie eine Zeitinformation, beispielsweise einen Zähler oder einen Zeitstempel.

[0045] Die Prüfung der Assertion erfolgt vorzugsweise durch eine dritte Stelle, z.B. durch die CPU (Central Processing Unit) der zweiten Datenverarbeitungseinheit des schwächer geschützten Bereiches, oder durch einen Back-End-Server, z.B. einen Web-Server. Dazu authentisiert sich die CPU der zweiten Datenverarbeitungseinheit gegenüber dem Back-End-Server unter Verwendung einer ersten Sicherheitsinformation der ersten Sicherheitseinheit und einer zweiten Sicherheitsinformation der zweiten Sicherheitseinheit. Eine Authentisierung der zweiten Sicherheitseinheit mit einem Schlüssel der zweiten Sicherheitseinheit wird nur dann akzeptiert, wenn zusätzlich eine Assertion der ersten Sicherheitseinheit vorliegt.

[0046] In einer Variante kann die Authentisierung der zweiten Sicherheitseinheit vorläufig oder temporär akzeptiert werden. Dabei muss innerhalb einer vorgegebenen Zeitspanne über die durch die erste Sicherheitseinheit authentisierte Kommunikationsverbindung eine Assertion der ersten Sicherheitseinheit übertragen werden. Vorteilhafterweise ist in beiden oben beschriebenen Varianten die zweite Sicherheitseinheit alleine, d.h. ohne die erste Sicherheitseinheit, nicht nutzbar oder nur eingeschränkt nutzbar. Die beiden Sicherheitseinheiten sind dadurch funktional aneinander gebunden. Der physikalische starke Tamperschutz der ersten Sicherheitseinheit wirkt somit auf die zweite Sicherheitseinheit.

[0047] Das Bestätigungssignal kann eingeschränkt gültig sein, z.B. für eine vorgegebene Zeitdauer, z.B. eine Minute, eine Stunde oder einen Tag, oder bis zu einem vorgebbaren Ereignis, z.B. Stromunterbrechung, Verbindungsaufbau oder Verbindungsabbau.

[0048] Bei einer weiteren Ausführungsform ist zumindest ein mit der ersten Sicherheitseinheit gekoppelter Sensor zum Erkennen eines unbefugten Eingriffs in die zweite Sicherheitseinheit vorgesehen. Dabei ist die erste Sicherheitseinheit dazu eingerichtet ist, die zweite Sicherheitseinheit bei einem durch den zumindest einen Sensor erkannten unbefugten Eingriff zu sperren.

[0049] Dabei kann bei einem unbefugten Eingriff in oder auf die zweite Sicherheitseinheit diese sofort gesperrt werden. Diese Sperrung übernimmt vorteilhafterweise eine andere Einrichtung, nämlich die erste Sicherheitseinheit.

[0050] Bei einer weiteren Ausführungsform ist die erste Sicherheitseinheit als ein Trusted-Platform-Modul ausgebildet.

[0051] Bei einer weiteren Ausführungsform ist die zweite Sicherheitseinheit als ein M2M-Security-Module (M2M, Machine To Machine) ausgebildet.

[0052] Bei einer weiteren Ausführungsform sind die erste Sicherheitseinheit und die erste Datenverarbeitungseinheit als eine erste integrierte Baugruppe ausgebildet.

[0053] Bei einer weiteren Ausführungsform sind die zweite Sicherheitseinheit und die zweite Datenverarbeitungseinheit als eine zweite integrierte Baugruppe ausgebildet.

[0054] Durch die Ausbildung der integrierten Baugruppen kann ein modularer Aufbau der Vorrichtung bewerkstelligt werden, insbesondere hinsichtlich einer modularen Trennung des stärker geschützten Bereiches und des schwächer geschützten Bereiches.

[0055] Bei einer weiteren Ausführungsform ist die erste Datenverarbeitungseinheit als eine Steuereinheit eines Messsystems ausgebildet.

[0056] Bei einer weiteren Ausführungsform ist die zweite Datenverarbeitungseinheit als ein Kommunikationsmodul zur Kommunikation mit einer externen Einrichtung ausgebildet.

[0057] Durch das Kommunikationsmodul können die Messwerte des intelligenten Zählers insbesondere digital signiert an die externe Einrichtung, beispielsweise einen Back-End-Server, übertragen werden.

[0058] Die jeweilige Einheit, Sicherheitseinheit und Datenverarbeitungseinheit, kann hardwaretechnisch und/oder auch softwaretechnisch implementiert sein. Bei einer hardwaretechnischen Implementierung kann die jeweilige Einheit als Vorrichtung oder als Teil einer Vorrichtung, zum Beispiel als Computer oder als Mikroprozessor ausgebildet sein. Bei einer softwaretechnischen Implementierung kann die jeweilige Einheit als Computerprogrammprodukt, als eine Funktion, als eine Routine, als Teil eines Programmcodes oder als ausführbares Objekt ausgebildet sein.

[0059] Die oben beschriebenen Eigenschaften, Merkmale und Vorteile dieser Erfindung sowie die Art und Weise, wie diese erreicht werden, werden klarer und deutlicher verständlich im Zusammenhang mit der folgenden Beschreibung der Ausführungsbeispiele, die im Zusammenhang mit den Zeichnungen näher erläutert werden.

[0060] Dabei zeigen:

[0061] **Fig.** 1 ein Blockschaltbild eines ersten Ausführungsbeispiels einer Vorrichtung mit Sicherheitseinheiten in unterschiedlich geschützten Bereichen;

[0062] **Fig.** 2 ein Blockschaltbild eines zweiten Ausführungsbeispiels einer Vorrichtung mit Sicherheitseinheiten in unterschiedlich geschützten Bereichen;

[0063] **Fig.** 3 ein Blockschaltbild eines dritten Ausführungsbeispiels einer Vorrichtung mit Sicherheitseinheiten in unterschiedlich geschützten Bereichen;

[0064] **Fig.** 4 ein Blockschaltbild eines vierten Ausführungsbeispiels einer Vorrichtung mit Sicherheitseinheiten in unterschiedlich geschützten Bereichen; und

[0065] **Fig.** 5 ein erstes Beispiel eines Kommunikationsdiagramms einer Vorrichtung mit Sicherheitseinheiten in unterschiedlich geschützten Bereichen mit einem Server.

[0066] In den Figuren sind gleiche oder funktionsgleiche Elemente mit denselben Bezugszeichen versehen worden, sofern nichts anderes angegeben ist.

[0067] In **Fig.** 1 ist ein Blockschaltbild eines ersten Ausführungsbeispiels einer Vorrichtung **1** mit Sicherheitseinheiten **2**, **4** in unterschiedlich geschützten Bereichen B1, B2 dargestellt.

[0068] Die Vorrichtung **1** ist beispielsweise ein intelligenter Zähler, insbesondere ein intelligenter Stromzähler oder ein intelligenter Gaszähler. Die Vorrichtung **1** kann aber auch als ein Feldgerät oder als ein Steuergerät ausgebildet sein.

[0069] Ohne Einschränkung der Allgemeinheit ist die Vorrichtung **1** der **Fig.** 1 in zwei getrennte, unterschiedlich geschützte Bereiche B1, B2 aufgeteilt. Geschützt bezieht sich hier insbesondere auf den Schutz gegen unbefugten Eingriff (Tamperschutz).

[0070] Der stärker geschützte Bereich B1 weist eine erste Sicherheitseinheit **2** auf. Die erste Sicherheitseinheit **2** ist zur Ausführung einer Anzahl von ersten Sicherheitsfunktionen für eine zugeordnete erste Datenverarbeitungseinheit **3** eingerichtet. Der schwächer geschützte Bereich B2 hat eine zweite Sicherheitseinheit **4** zur Ausführung einer Anzahl von zweiten Sicherheitsfunktionen für eine zugeordnete zweite Datenverarbeitungseinheit **5**.

[0071] Beispielsweise ist der stärker geschützte Bereich B1 verplombt oder vergossen. Hierzu kann beispielsweise ein Epoxydharz verwendet werden. Der stärker geschützte Bereich B1 und der schwächer geschützte Bereich B2 sind voneinander getrennt. Beispielsweise integriert ein Gehäuse **6** der Vorrichtung **1** den stärker geschützten Bereich B1 und den schwächer geschützten Bereich B2, wobei eine Gehäusetrennwand **7** den stärker geschützten Bereich B1 und den schwächer geschützten Bereich B2 trennt. Die erste Sicherheitseinheit **2** ist beispiels-

weise ein Trusted-Platform-Modul (TPM). Die zweite Sicherheitseinheit **4** ist beispielsweise ein M2M-Security-Modul. Die erste Sicherheitseinheit **2** und die erste Datenverarbeitungseinheit **3** sind beispielsweise als eine erste integrierte Baugruppe ausgebildet. Entsprechend können die zweite Sicherheitseinheit **4** und die zweite Datenverarbeitungseinheit **5** als eine zweite integrierte Baugruppe ausgebildet sein.

[0072] Die jeweilige Datenverarbeitungseinheit **3**, **5** ist zum Verarbeiten von Daten, insbesondere solchen Daten von der jeweiligen zugeordneten Sicherheitseinheit **2**, **4**, eingerichtet. Insbesondere ist die erste Datenverarbeitungseinheit **3** eine Steuereinheit eines Messsystems der Vorrichtung **1**. Die zweite Datenverarbeitungseinheit **5** ist insbesondere ein Kommunikationsmodul zur Kommunikation der Vorrichtung **1** mit einer externen Einrichtung, beispielsweise einem Server oder einem Back-End-Server.

[0073] Die zweiten Sicherheitsfunktionen der zweiten Sicherheitseinheit **4** umfassen zumindest eine freizuschaltende Sicherheitsfunktion. Erst nach einem Freischalten der freizuschaltenden Sicherheitsfunktion ist diese aktiviert. Dabei ist die erste Sicherheitseinheit **2** dazu eingerichtet, die zumindest eine freizuschaltende Sicherheitsfunktion der zweiten Sicherheitseinheit **4** mittels eines vorbestimmten Freischaltsignals F freizuschalten. Mit Bezug zu **Fig.** 1 wird das Freischaltsignal F von der ersten Sicherheitseinheit **2** generiert. Das generierte Freischaltsignal F wird an die zweite Sicherheitseinheit **4** über die erste Datenverarbeitungseinheit **3** und die zweite Datenverarbeitungseinheit **5** übertragen. Diese Datenübertragung des Freischaltsignals F der **Fig.** 1 ist nur beispielhaft.

[0074] Das vorbestimmte Freischaltsignal F zum Freischalten der zumindest einen freizuschaltenden Sicherheitsfunktion der zweiten Sicherheitseinheit **4** umfasst zumindest einen Sicherheitsparameter. Beispiele für solche Sicherheitsparameter sind ein Passwort, eine PIN und ein kryptographischer Parameter.

[0075] Vorzugsweise ist die erste Sicherheitseinheit **2** dazu eingerichtet, einen Zustand der zweiten Sicherheitseinheit **4** zu überwachen und die zumindest eine freizuschaltende Sicherheitsfunktion der zweiten Sicherheitseinheit **4** in Abhängigkeit des überwachten Zustands freizuschalten. Bei den beispielhaften folgenden Zuständen der zweiten Sicherheitseinheit **4** kann die erste Sicherheitseinheit **2** diese oder zumindest die eine freizuschaltende Sicherheitsfunktion dieser freischalten: Hochfahren der zweiten Sicherheitseinheit **4**, Batteriewechsel einer Batterie der zweiten Sicherheitseinheit **4**, jeweils nach Ablauf einer vorbestimmten Zeitdauer im Betrieb der zweiten Sicherheitseinheit **4**, und beim Aufbau einer Datenverbindung der zweiten Sicherheitseinheit **4** zu einer externen Einrichtung, beispielsweise einem Server.

[0076] Hinsichtlich der Generierung und Übertragung des Freischaltsignals F von der ersten Sicherheitseinheit **2** zu der zweiten Sicherheitseinheit **4** sind weitere Alternativen denkbar:
Beispielsweise können die erste Sicherheitseinheit **2** und die zweite Sicherheitseinheit **4** dazu eingerichtet werden, dass die zweite Sicherheitseinheit **4** eine Anfrage-Antwort-Authentisierung (Challenge-Response-Authentication) der ersten Sicherheitseinheit **2** durchführt. Dabei ist die zweite Sicherheitseinheit **4** ferner dazu eingerichtet, das Freischaltsignal F aus der Antwort (Response) der ersten Sicherheitseinheit **2** zu extrahieren.

[0077] Des Weiteren können die erste Sicherheitseinheit **2** und die zweite Sicherheitseinheit **4** dazu eingerichtet werden, dass die erste Sicherheitseinheit **2** die Identität der zweiten Sicherheitseinheit **4** authentisiert und in Abhängigkeit der authentisierten Identität der zweiten Sicherheitseinheit **4** ein Bestätigungssignal (Assertion) zur Bestätigung einer Verbindung zwischen der ersten Sicherheitseinheit **2** und der zweiten Sicherheitseinheit **4** generiert. Dabei ist das generierte Bestätigungssignal beispielsweise Teil des Freigabesignals F. Alternativ kann das Freigabesignal F zumindest teilweise aus dem generierten Bestätigungssignal abgeleitet werden.

[0078] **Fig.** 2 zeigt ein Blockschaltbild eines zweiten Ausführungsbeispiels einer Vorrichtung **1** mit Sicherheitseinheiten **2**, **4** in unterschiedlich geschützten Bereichen B1, B2. Das zweite Ausführungsbeispiel der **Fig.** 2 basiert auf dem ersten Ausführungsbeispiel der **Fig.** 1. Die Vorrichtung **1** der **Fig.** 2 weist ferner einen Sensor **8** auf. Der Sensor **8** ist dazu eingerichtet, einen unbefugten Eingriff in dem schwächer geschützten Bereich B2 oder in die zweite Sicherheitseinheit **4** zu detektieren. Ferner ist der Sensor **8** mit der ersten Sicherheitseinheit **2** gekoppelt. Dabei ist die erste Sicherheitseinheit **2** dazu eingerichtet, die zweite Sicherheitseinheit **4** bei einem durch den Sensor **8** erkannten unbefugten Eingriff zu sperren.

[0079] In **Fig.** 3 ist ein Blockschaltbild eines dritten Ausführungsbeispiels einer Vorrichtung **1** mit Sicherheitseinheiten **2**, **4** in unterschiedlich geschützten Bereichen B1, B2 dargestellt. Die Vorrichtung **1** der **Fig.** 3 basiert auf der Ausführungsform der **Fig.** 1 und ist als ein Smart Meter **1** ausgebildet.

[0080] Der stärker beschützte Bereich B1 kann auch als tampergeschützter Bereich oder tampergeschützte Zone bezeichnet werden. Dabei ist der stärker geschützte Bereich B1 als ein vergossener Bereich ausgestaltet. Die Trennwand **7** kann beispielsweise als eine verplombte interne Trennwand **7** ausgestaltet sein. Der stärker geschützte Bereich B1 hat neben der Sicherheitseinheit **2** und der Datenverarbeitungseinheit **3**, welche als Steuereinheit des Messsystems ausgebildet ist, Sensoren **13**, welche den über En-

ergietransportträger **11**, **12** transportierten Energieverbrauch erfassen. Hierbei kann beispielsweise verbrauchter Strom, verbrauchtes Wasser, verbrauchte Wärme oder verbrauchtes Gas erfasst werden.

[0081] Der von den Sensoren **13** bereitgestellte Messwert wird durch die Steuereinheit **3** des Messsystems verarbeitet. Dazu hat die Steuereinheit **3** insbesondere eine CPU (Central-Processing-Unit). In einem der Steuereinheit **3** zugeordneten Speicher **8** sind Programmcode, Eichdaten, Messdaten und dergleichen ablegbar. Die Sicherheitseinheit **2** ist beispielsweise als ein Sicherheitsmodul ausgebildet, welches beispielsweise dazu verwendet wird, die erfassten Messwerte oder Verbrauchswerte digital zu signieren.

[0082] In dem schwächer geschützten Bereich B2, welcher über einen abnehmbaren Deckel **17** des Gehäuses **6** zugänglich bzw. einfacher zugänglich ist als der stärker geschützte Bereich B1, befinden sich die Datenverarbeitungseinheit **5**, die hier als Kommunikationsmodul ausgebildet ist, und die zweite Sicherheitseinheit **4**. Das Kommunikationsmodul **5** ist über eine Datenschnittstelle **14** dazu eingerichtet, mit einer externen Einrichtung, beispielsweise einem Server **16** (siehe **Fig.** 5), zu kommunizieren. Hierzu kann Ethernet, UMTS, GPRS, LTE, WLAN oder dergleichen eingesetzt werden.

[0083] Die zweite Sicherheitseinheit **4** des schwächer geschützten Bereichs **B2** ist mit dem Kommunikationsmodul **5** gekoppelt und ist beispielsweise als eine M2M-SIM-Karte oder als ein festverdrahteter Chipkarten-Controller ausgebildet. Die zweite Sicherheitseinheit **4** wird dazu eingesetzt, um eine kryptographisch gesicherte Kommunikationsverbindung zu einem Mobilfunknetz oder zu einem Back-End-Server **16** aufzubauen. Darüber hinaus hat der schwächer geschützte Bereich B2 noch einen Bildschirm **15**, über welchen insbesondere die erfassten Messwerte oder Stromwerte angezeigt werden können.

[0084] **Fig.** 4 zeigt eine alternative Ausführungsform zu der **Fig.** 3. Bei der Ausführungsform der **Fig.** 4 weist das Gehäuse **6** der Vorrichtung **1** nur einen intern vergießbaren Bereich B1 auf, in welchen die erste Sicherheitseinheit **4** vergossen ist. Für diesen Verguss wird beispielsweise Epoxydharz oder Kunststoff eingesetzt. Der Vorteil dieser Ausführungsform liegt darin, dass nur dieser kleinere Bereich vergossen werden muss. Hierbei wird Material eingespart. Es sind weitere Varianten denkbar, welche Baugruppen in dem intern vergießbaren Bereich B1 angeordnet sind. So kann z.B. auch ein oder mehrere der Sensoren **13** und/oder der Speicher **8** und/oder die Messsystem-Steuereinheit **3** im vergießbaren Bereich B1 angeordnet sein.

[0085] **Fig.** 5 zeigt ein erstes Beispiel eines Kommunikationsdiagramms einer Vorrichtung **1** mit Sicherheitseinheiten **2**, **4** in unterschiedlich geschützten Bereichen B1, B2 mit einem Server **16**. Ferner ist in **Fig.** 5 dargestellt, dass die Vorrichtung **1** ein Kommunikationsmodul **5** umfasst.

[0086] Zu Beginn der Kommunikation zwischen der Vorrichtung **1** und dem Server **16** wird in Schritt **501** zwischen dem Kommunikationsmodul **5** der Vorrichtung **1** und dem Server **16** eine Verbindung über ein Kommunikationsnetz, z.B. Internet oder einem Mobilfunknetz, aufgebaut. Hierzu wird beispielsweise TCP/IP eingesetzt, welches insbesondere durch ein TLS-Protokoll geschützt ist.

[0087] In Schritt **502** überträgt der Server **16** eine Authentisierungsaufforderung, welche eine Challenge enthält, an das Kommunikationsmodul **5**.

[0088] Um sich zu authentisieren, muss die passende Antwortnachricht mittels einer HMAC-Funktion oder einer digitalen Signaturfunktion berechnet werden. In Schritt **503** überträgt das Kommunikationsmodul **5** dazu die empfangene Challenge an die erste Sicherheitseinheit **4**, welche dem Kommunikationsmodul **5** zugeordnet ist.

[0089] Die erste Sicherheitseinheit **4** hat einen kryptographischen Schlüssel gespeichert. Der kryptographische Schlüssel ist beispielsweise ein symmetrischer Schlüssel eines symmetrischen kryptographischen Verfahrens, wie AES, DES, IDEA, HMAC, oder ein privater Schlüssel eines asymmetrischen kryptographischen Verfahrens, wie RSA, DSA oder ECC.

[0090] Technisch kann die zweite Sicherheitseinheit **4** diese Berechnung durchführen. Bevor diese Berechnung allerdings durchgeführt wird, authentisiert die zweite Sicherheitseinheit **4** zunächst die erste Sicherheitseinheit **2**, welche sich im stärker geschützten Bereich B1 der Vorrichtung **1** befindet. Dazu wählt die zweite Sicherheitseinheit **4** eine zufällige Nonce in Schritt **504** und stellt diese der ersten Sicherheitseinheit **2** in Schritt **505** bereit.

[0091] In Schritt **506** wird eine Antwort oder Response mittels eines kryptografischen Authentisierungsalgorithmus oder einer physikalischen PUF berechnet.

[0092] In Schritt **507** wird die generierte Response von der ersten Sicherheitseinheit **2** an die zweite Sicherheitseinheit **4** übertragen. In Schritt **508** prüft die zweite Sicherheitseinheit **4** die empfangene Response.

[0093] Nur wenn diese gültig ist (Schritt **509**), wird die Benutzung des auf der zweiten Sicherheitseinheit **4** gespeicherten Schlüssels durch die zweite Sicherheitseinheit **4** freigegeben (Schritt **510**).

[0094] In Schritt **511** wird eine kryptographische Prüfsumme der Challenge unter Verwendung des Schlüssels berechnet und dem Kommunikationsmodul **5** bereitgestellt. In Schritt **513** verwendet das Kommunikationsmodul **5** diese Information, beispielsweise indem es diesen direkt oder einen damit bestimmten weiteren Authentisierungsparameter an den Server **16** zur Prüfung überträgt.

[0095] Vielfältige Varianten des mit Bezug zu **Fig.** 5 beschriebenen Ablaufs sind denkbar. Beispielsweise kann die zweite Sicherheitseinheit **4** die erste Sicherheitseinheit **2** direkt nach dem Anlegen der Versorgungsspannung authentisieren, also schon bevor ein Verbindungsaufbau mit dem Server **16** stattfindet.

[0096] In einer weiteren Variante kann die erste Sicherheitseinheit **2** weitere Prüfungen vornehmen, bevor sie sich authentisiert, z.B. indem es Tampersensoren abfragt. Beispiele für solche Tampersensoren sind Schalter, Kontakte, Wire-Mesh-Sensoren, Verplombungsbruch-Sensoren, Sensoren für elektrische, magnetische Felder oder elektromagnetische Strahlung, Lagesensoren oder Lichtsensoren.

[0097] Die erste Sicherheitseinheit **2** kann eine Manipulationserkennung der gemessenen Sensorwerte vornehmen. Ferner kann eine Manipulation der Anschlussverbinder der Energieversorgungsleitung durch die erste Sicherheitseinheit **2** detektiert werden. Die erste Sicherheitseinheit **2** kann ferner prüfen, ob ein Stromfluss stattfindet bzw. ob eine Spannung anliegt. Bei anderen Energiegrößen kann z.B. der Gasfluss, der Gasfluss, der Wasserdruck, der Wasserfluss, die Temperatur eines Wärmemediums, z.B. Wasser oder Dampf, gemessen werden.

[0098] In einer weiteren Variante ist der Schlüssel auf der zweiten Sicherheitseinheit **4** verschlüsselt gespeichert, wobei eine von der ersten Sicherheitseinheit **2** bereitgestellte Information dazu verwendet wird, den gespeicherten Schlüssel durch die zweite Sicherheitseinheit **4** zu entschlüsseln, so dass dieser entschlüsselte Schlüssel nutzbar wird.

[0099] In einer weiteren Variante ist auf der zweiten Sicherheitseinheit **4** nur ein erster Teilschlüssel gespeichert. Ein zweiter Teilschlüssel ist dann auf der ersten Sicherheitseinheit **2** gespeichert. Beide Teilschlüssel werden zur Erstellung einer Signatur verwendet. Hierfür sind verschiedene Ansätze möglich, wie z.B. der von Shoup (www.shoup.net/papers/thsig.pdf).

[0100] Obwohl die Erfindung im Detail durch das bevorzugte Ausführungsbeispiel näher illustriert und beschrieben wurde, so ist die Erfindung nicht durch die offenbarten Beispiele eingeschränkt und andere Variationen können vom Fachmann hieraus abgeleitet werden, ohne den Schutzumfang der Erfindung zu verlassen.

ZITATE ENTHALTEN IN DER BESCHREIBUNG

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

Zitierte Patentliteratur

- US 2007/103334 A [0016]

Zitierte Nicht-Patentliteratur

- DS3645 [0012]
- www.shoup.net/papers/ thsig.pdf [0099]

Patentansprüche

1. Vorrichtung (**1**) mit Sicherheitseinheiten (**2**, **4**) in unterschiedlich geschützten Bereichen (B1, B2), wobei ein stärker geschützter Bereich (B1) eine erste Sicherheitseinheit (**2**) zur Ausführung einer Anzahl von ersten Sicherheitsfunktionen für eine zugeordnete erste Datenverarbeitungseinheit (**3**) und ein schwächer geschützter Bereich (B2) eine zweite Sicherheitseinheit (**4**) zur Ausführung einer Anzahl von zweiten Sicherheitsfunktionen für eine zugeordnete zweite Datenverarbeitungseinheit (**5**) aufweisen, wobei die zweiten Sicherheitsfunktionen zumindest eine freizuschaltende Sicherheitsfunktion umfassen, wobei die erste Sicherheitseinheit (**2**) dazu eingerichtet ist, die zumindest eine freizuschaltende Sicherheitsfunktion der zweiten Sicherheitseinheit (**4**) mittels eines vorbestimmten Freischaltsignals (F) freizuschalten.

2. Vorrichtung nach Anspruch 1, **dadurch gekennzeichnet,** dass das vorbestimmte Freischaltsignal (F) zum Freischalten der zumindest einen freizuschaltenden Sicherheitsfunktion der zweiten Sicherheitseinheit (**4**) zumindest einen Sicherheitsparameter, insbesondere ein Passwort, eine Persönliche Identifikationsnummer und/oder einen kryptographischen Parameter, umfasst.

3. Vorrichtung nach Anspruch 1 oder 2, **dadurch gekennzeichnet,** dass die Vorrichtung (**1**) als ein intelligenter Zähler, insbesondere als ein intelligenter Stromzähler oder als ein intelligenter Gaszähler, als ein Feldgerät, insbesondere für eine Ampelsteuerung, oder als ein Steuergerät, insbesondere für ein Kraftfahrzeug, ausgebildet ist.

4. Vorrichtung nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet,** dass die erste Sicherheitseinheit (**2**) dazu eingerichtet ist, einen Zustand der zweiten Sicherheitseinheit (**4**) zu überwachen und die zumindest eine freizuschaltende Sicherheitsfunktion der zweiten Sicherheitseinheit (**4**) in Abhängigkeit des überwachten Zustands freizuschalten.

5. Vorrichtung nach Anspruch 4, **dadurch gekennzeichnet,** dass die erste Sicherheitseinheit (**2**) dazu eingerichtet ist, die zumindest eine freizuschaltende Sicherheitsfunktion der zweiten Sicherheitseinheit (**4**) bei einem Hochfahren der zweiten Sicherheitseinheit (**4**), bei einem Batteriewechsel einer Batterie der zweiten Sicherheitseinheit (**4**), jeweils nach Ablauf einer vorbestimmten Zeitdauer im Betrieb der zweiten Sicherheitseinheit (**4**), und/oder bei einem Aufbau einer Datenverbindung der zweiten Sicherheitseinheit (**4**) zu einer externen Einrichtung mittels des vorbestimmten Freischaltsignals (F) freizuschalten.

6. Vorrichtung nach einem der Ansprüche 1 bis 5, **dadurch gekennzeichnet,** dass der stärker geschützte Bereich (B1) verplombt oder vergossen ist, insbesondere mittels eines Epoxydharzes vergossen ist.

7. Vorrichtung nach einem der Ansprüche 1 bis 5, **dadurch gekennzeichnet,** dass der stärker geschützte Bereich (B1) und der schwächer geschützte Bereich (B2) getrennt sind.

8. Vorrichtung nach Anspruch 7, **dadurch gekennzeichnet,** dass ein Gehäuse (**6**) den stärker geschützten Bereich (B1) und den schwächer geschützten Bereich (B2) integriert, wobei eine Gehäusetrennwand (**7**) den stärker geschützten Bereich (B1) und den schwächer geschützten Bereich (B2) trennt.

9. Vorrichtung nach einem der Ansprüche 1 bis 8, **dadurch gekennzeichnet,** dass die erste Sicherheitseinheit (**2**) und die zweite Sicherheitseinheit (**4**) dazu eingerichtet sind, dass die zweite Sicherheitseinheit (**4**) eine Anfrage-Antwort-Authentisierung der ersten Sicherheitseinheit (**2**) durchführt, wobei die zweite Sicherheitseinheit (**4**) ferner dazu eingerichtet ist, das Freischaltsignal (F) aus der Antwort der ersten Sicherheitseinheit (**2**) zu extrahieren.

10. Vorrichtung nach einem der Ansprüche 1 bis 8, **dadurch gekennzeichnet,** dass die erste Sicherheitseinheit (**2**) und die zweite Sicherheitseinheit (**4**) dazu eingerichtet sind, dass die erste Sicherheitseinheit (**2**) die Identität der zweiten Sicherheitseinheit (**4**) authentisiert und in Abhängigkeit der authentisierten Identität der zweiten Sicherheitseinheit (**4**) ein Bestätigungssignal zur Bestätigung einer Verbindung zwischen der ersten Sicherheitseinheit (**2**) und der zweiten Sicherheitseinheit (**4**) generiert, wobei das generierte Bestätigungssignal zumindest Teil des Freigabesignals (F) ist oder das Freigabesignal (F) zumindest teilweise aus dem generierten Bestätigungssignal ableitbar ist.

11. Vorrichtung nach einem der Ansprüche 1 bis 10, gekennzeichnet durch:
zumindest einen mit der ersten Sicherheitseinheit (**2**) gekoppelten Sensor (**8**) zum Erkennen eines unbefugten Eingriffs in die zweite Sicherheitseinheit (**4**), wobei die erste Sicherheitseinheit (**2**) dazu eingerichtet ist, die zweite Sicherheitseinheit (**4**) bei einem durch den zumindest einen Sensor (**8**) erkannten unbefugten Eingriff zu sperren.

12. Vorrichtung nach einem der Ansprüche 1 bis 11, **dadurch gekennzeichnet,** dass die erste Sicherheitseinheit (**2**) als ein Trusted-Platform-Module (TPM) ausgebildet ist.

13. Vorrichtung nach einem der Ansprüche 1 bis 12, **dadurch gekennzeichnet,** dass die zweite Sicherheitseinheit (**4**) als ein M2M-Security-Module ausgebildet ist.

14. Vorrichtung nach einem der Ansprüche 1 bis 13, **dadurch gekennzeichnet,** dass die erste Sicherheitseinheit (**2**) und die erste Datenverarbeitungseinheit (**3**) als eine erste integrierte Baugruppe ausgebildet sind und/oder dass die zweite Sicherheitseinheit (**4**) und die zweite Datenverarbeitungseinheit (**5**) als eine zweite integrierte Baugruppe ausgebildet sind.

15. Vorrichtung nach einem der Ansprüche 1 bis 14, **dadurch gekennzeichnet,** dass die erste Datenverarbeitungseinheit (**3**) als eine Steuereinheit eines Messsystems ausgebildet ist und/oder dass die zweite Datenverarbeitungseinheit (**5**) als ein Kommunikationsmodul zur Kommunikation mit einer externen Einrichtung ausgebildet ist.

Es folgen 3 Seiten Zeichnungen

Anhängende Zeichnungen

FIG 1

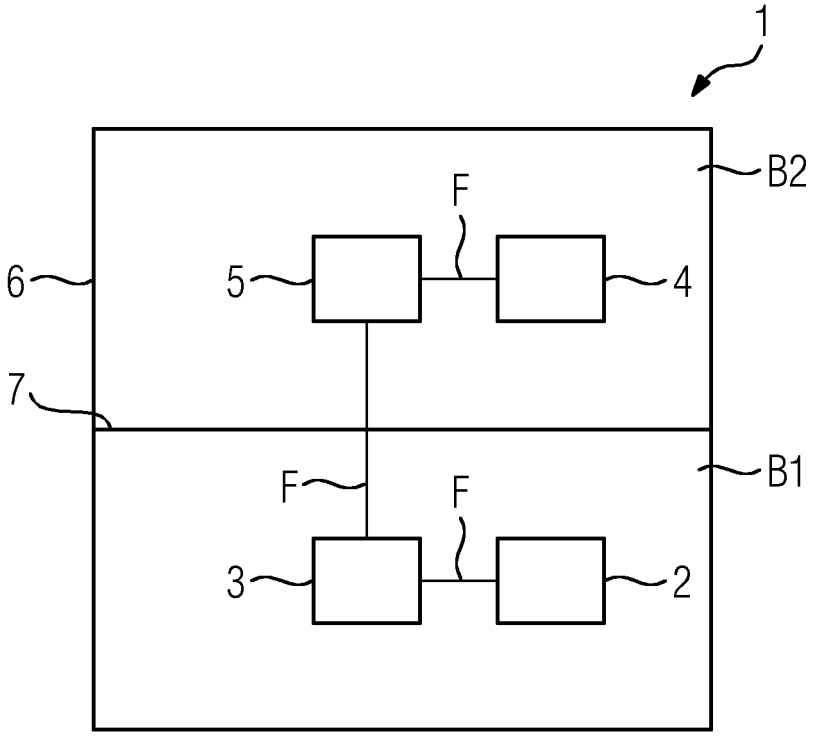


FIG 2

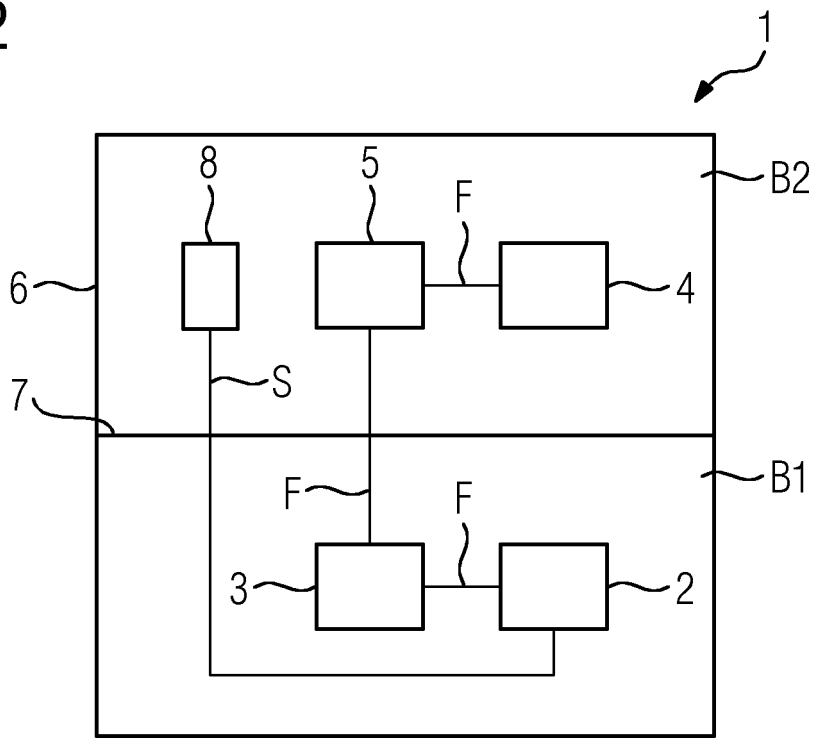


FIG 3

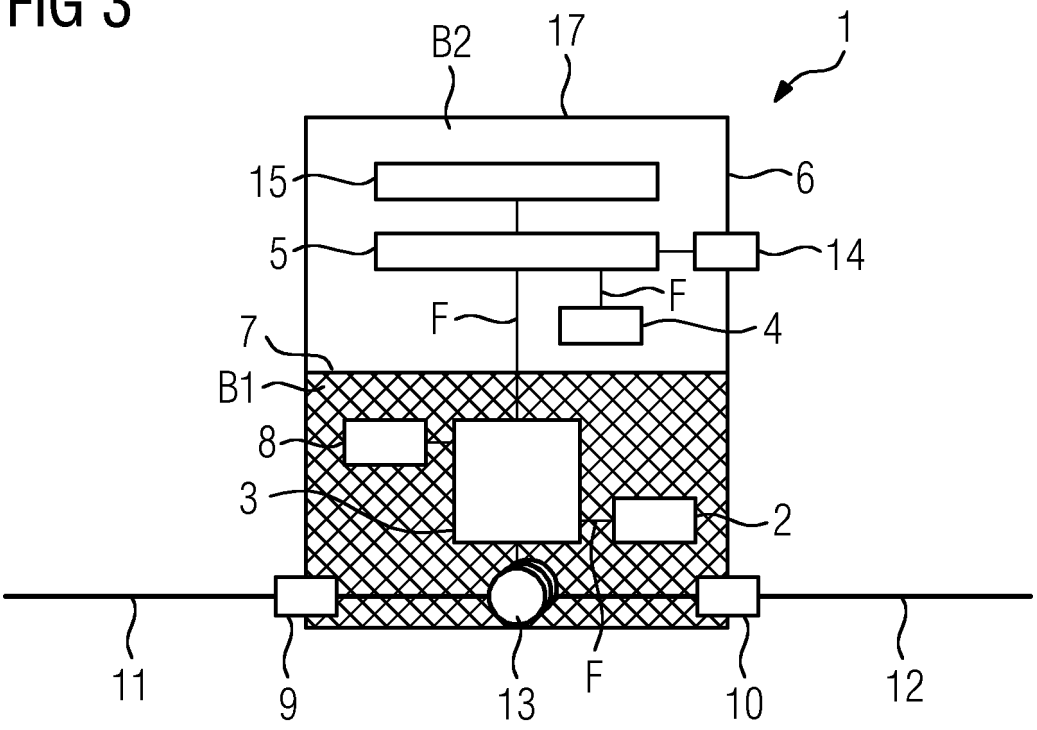

B2
17
1
15
6
5
14
F
F
4
7
B1
8
3
2
11
9
13
F
10
12

FIG 4

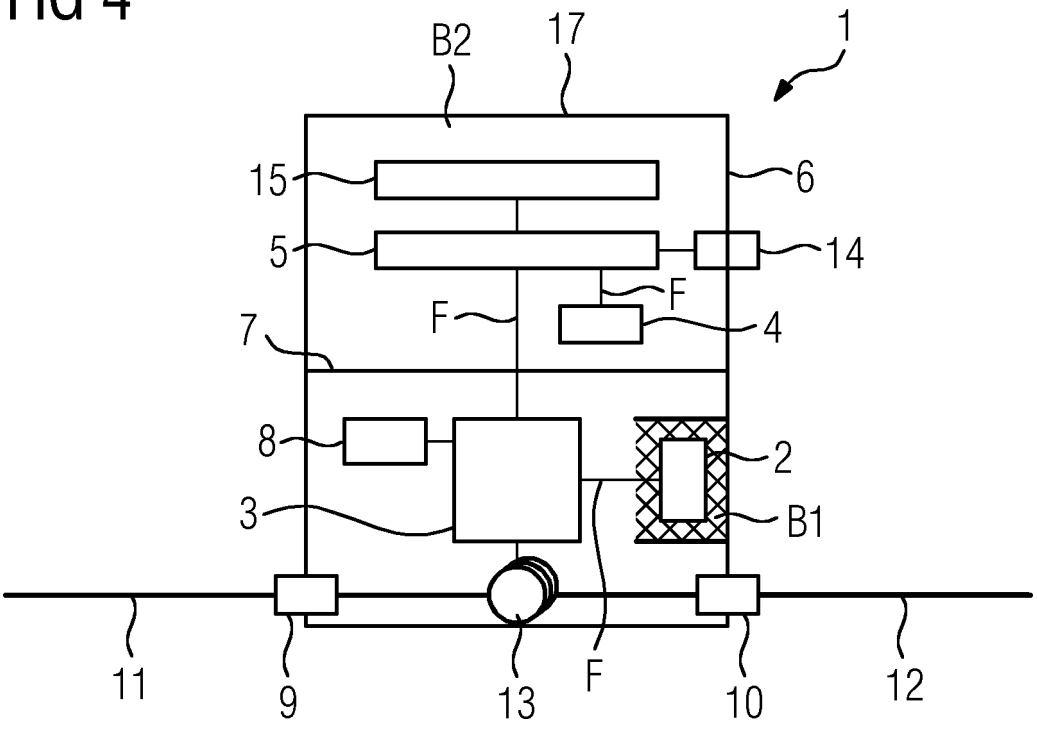

B2
17
1
15
6
5
14
F
F
4
7
8
2
3
B1
11
9
13
F
10
12

FIG 5