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

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
26. Oktober 2012 (26.10.2012)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2012/143270 A1

(51) Internationale Patentklassifikation:
G06F 21/06 (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2012/056516

(22) Internationales Anmeldedatum:
11. April 2012 (11.04.2012)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2011 007 571.2
18. April 2011 (18.04.2011) DE

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

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: **FALK, Rainer** [DE/DE]; Parkstraße 43, 85435 Erding (DE).

(74) Gemeinsamer Vertreter: **SIEMENS AKTIENGESELLSCHAFT**; Postfach 22 16 34, 80506 München (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

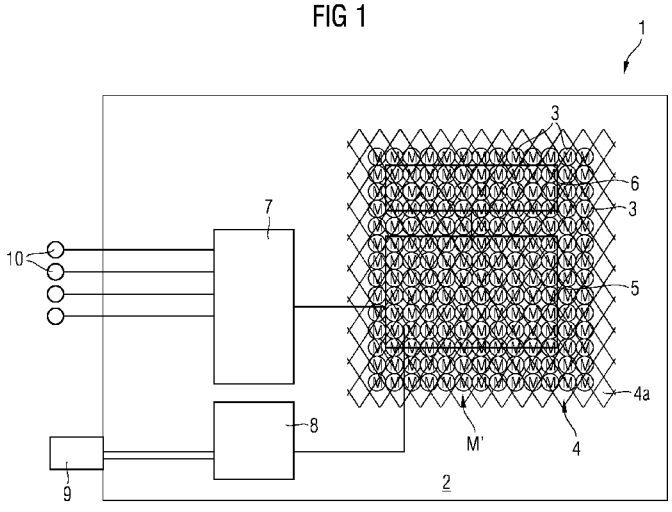
Veröffentlicht:

— *mit internationalem Recherchenbericht (Artikel 21 Absatz 3)*

(54) **Title**: TAMPER PROTECTION DEVICE FOR PROTECTING A FIELD DEVICE AGAINST TAMPERING

(54) **Bezeichnung** : TAMPERSCHUTZVORRICHTUNG ZUM TAMPERSCHUTZ EINES FELDGERÄTS

FIG 1



(57) **Abstract**: The invention relates to a tamper protection device for protecting a field device against tampering, comprising a carrier and at least one electronic memory, wherein the at least one electronic memory is disposed in at least one partial area on the carrier, and the at least one electronic memory stores at least one predefinable security information item, and wherein the at least one electronic memory is designed in such a way as to modify the predefinable security information item in the event of at least partial damage to the tamper protection device. The invention further relates to a method for producing a field device having a tamper protection device, to a field device comprising a tamper protection device, to a tamper protection system, and to the use of a tamper protection device.

(57) **Zusammenfassung**:

[Fortsetzung auf der nächsten Seite]

WO 2012/143270 A1

Die Erfindung betrifft eine Tamperschutzvorrichtung zum Tamperschutz eines Feldgeräts, umfassend einen Träger und zumindest einen elektronischen Speicher, wobei der zumindest eine elektronische Speicher in zumindest einem Teilbereich auf dem Träger angeordnet ist und der zumindest eine elektronische Speicher zumindest eine vorgebbare Sicherheitsinformation speichert, und wobei der der zumindest eine elektronische Speicher ausgebildet ist, bei einer zumindest teilweisen Beschädigung der Tamperschutzvorrichtung die vorgebbare Sicherheitsinformation zu verändern. Die Erfindung betrifft ebenfalls ein Verfahren zur Herstellung eines Feldgeräts mit einer Tamperschutzvorrichtung, ein Feldgerät umfassend eine Tamperschutzvorrichtung sowie ein Tamperschutzsystem und Verwendungen einer Tamperschutzvorrichtung.

Beschreibung

Tamperschutzvorrichtung zum Tamperschutz eines Feldgeräts

Die Erfindung betrifft eine Tamperschutzvorrichtung zum Tamperschutz eines Feldgeräts, ein Verfahren zur Herstellung eines Feldgeräts mit einem Tamperschutz und ein Tamperschutzsystem sowie Verwendungen einer Tamperschutzvorrichtung.

Feldgeräte werden in vielfältigen Bereichen der Technik verwendet, beispielsweise in Form von Signalanlagen als Ampeln, Bahnsignale oder dergleichen. Feldgeräte sind üblicherweise mit einer Steuervorrichtung, beispielsweise einer Leitstelle oder ähnlichem verbunden, um die Feldgeräte anhand von Steuerungssignalen zu steuern. Ein derartiges Feldgerät kann dabei insbesondere zur Verarbeitung der Steuersignale einen Steuerrechner umfassen, an dem ein Konfigurationsspeicher angeschlossen ist. Diese beiden Komponenten sind somit wesentlich für die Steuerung des Feldgeräts. Der Steuerrechner kann weiter mit einer Eingabe-/Ausgabeeinheit des Feldgeräts verbunden sein, über die Sensorsignale zusätzlicher Sensoren übermittelt werden können, beispielsweise Sensoren, die eine Drehzahl eines Aktors des Feldgeräts erfassen oder dergleichen. Darüber hinaus umfasst das Feldgerät auch eine Kommunikationsschnittstelle zur Kommunikation mit der Leitstelle.

Um Manipulationen an dem Feldgerät und insbesondere an dem Steuerrechner und dem Konfigurationsspeicher zu vermeiden, ist es der Anmelderin bekannt geworden, dass diese beiden Komponenten mit einer Vergussmasse, beispielsweise ein Epoxidharz oder dergleichen, versehen werden. Dadurch wird die Zugänglichkeit zu den beiden Komponenten erschwert und ein gewisser Tamperschutz erreicht.

Durch den Tamperschutz des Steuerrechners und des Konfigurationsspeichers sind die im Konfigurationsspeicher abgelegten Konfigurationsdaten, beispielsweise insbesondere kryp-

tographische Schlüssel zur Kommunikation mit der Leitstelle vor Manipulationen geschützt oder deren Manipulation zumindest erschwert.

Ein integrierter Schaltkreis, der über einen Tamperschutz verfügt, ist beispielsweise der ATMEL AT98, dessen Daten unter http//www.datasheetarchive.com/AT98SC008CT-datasheet.html abrufbar sind.

Darüber hinaus ist es der Anmelderin bekannt geworden, Sensoren am Feldgerät anzuordnen, um eine Manipulation des Steuerrechners oder des Konfigurationsspeichers zu erkennen. Diese Sensoren können beispielsweise innerhalb eines Tamper-geschützten Bereichs angeordnet werden oder auch außerhalb. So ist es der Anmelderin beispielweise bekannt geworden, ein Drahtgeflecht im Tamper-geschützten Bereich anzuordnen, welches mit einem entsprechenden Sensor zur Beaufschlagung des Drahtgeflechtes mit elektrischen Signalen verbunden ist. Sollte nun ein Angreifer eine Manipulation am Steuerrechner oder am Konfigurationsspeicher des Feldgeräts vornehmen, beispielsweise durch Anbohren der Vergussmasse, um eine Kontaktierung des Steuerrechners und/oder des Konfigurationsspeichers zum Auslesen von Daten zu erreichen, um diesen manipulieren zu können, wird mit einer bestimmten hohen Wahrscheinlichkeit das Drahtgeflecht dabei zerstört. Um einen effektiven Tamperschutz zu erreichen, ist hierzu eine kontinuierliche Überwachung des Drahtgeflechts durch den entsprechenden Sensor nötig. Andernfalls könnte ein Angreifer das Drahtgeflecht, beispielsweise bei einem ausgeschalteten Gerät, entfernen, das Drahtgeflecht analysieren und ein elektrisch gleichwertiges Drahtgeflecht nachbauen, bevor er das Feldgerät wieder in Betrieb nimmt und sich dieses mit der Leitstelle verbindet. Das Feldgerät selbst und auch die Leitstelle, könnten dann nicht erkennen, ob oder inwieweit das Feldgerät manipuliert wurde.

Eine dauerhafte Überwachung erfordert auch eine entsprechende Energieversorgung, welche zusätzliche Kosten verursacht. Darüber hinaus ist es notwendig, den Zustand der Energieversorgung laufend zu überprüfen, um einen zuverlässigen Tamperschutz des Feldgeräts zu ermöglichen.

Aus der US 7,685,438 ist es bekannt geworden, in eine Schutzschicht einer integrierten Schaltung magnetische Partikel einzubringen. Die magnetischen Partikel können durch Sensoren erfasst und ein kryptographischer Schlüssel anhand der erfassten Informationen über die magnetischen Partikel erstellt werden. Wird die Schutzschicht der integrierten Schaltung entfernt, wird damit auch die zur Generierung des kryptographischen Schlüssels benötigte Information zerstört.

Aus der US 2008/192240 ist es weiter bekannt geworden, eine charakteristische Eigenschaft eines Lichtwellenleiters auszuwerten, um eine physikalische Manipulation des Lichtwellenleiters zu detektieren.

Eine Aufgabe der vorliegenden Erfindung ist es daher, eine einfache und kostengünstige Tamperschutzvorrichtung bereitzustellen, welche insbesondere auch ohne eine ununterbrochene Überwachung zuverlässig eine physikalische Manipulation eines mit der Tamperschutzvorrichtung versehenen Feldgeräts ermöglicht.

Diese Aufgabe wird durch eine Tamperschutzvorrichtung zum Tamperschutz eines Feldgeräts gelöst, umfassend einen Tamperschutzträger und zumindest einen elektronischen Speicher, wobei der zumindest eine elektronische Speicher in zumindest einem Teilbereich auf dem Tamperschutzträger angeordnet ist und der zumindest eine elektronische Speicher zumindest eine vorgebbare Sicherheitsinformation speichert und wobei der zumindest eine elektronische Speicher ausgebildet ist, bei einer zumindest teilweisen Beschädigung der Tamperschutzvorrichtung die vorgebbare Sicherheitsinformation zu verändern.

Die Aufgabe wird ebenfalls durch ein Verfahren zur Herstellung eines Feldgeräts mit einer Tamperschutzvorrichtung gemäß zumindest einem der Ansprüche 1 bis 6 gelöst, umfassend die Schritte Herstellen des Feldgeräts, Herstellen der Tamperschutzvorrichtung, Anordnen der Tamperschutzvorrichtung an dem Feldgerät, und Verbinden der Tamperschutzvorrichtung mit einer Überwachungseinrichtung zum Überwachen der Tamperschutzvorrichtung.

Die Aufgabe wird ebenfalls durch ein Feldgerät, umfassend eine Tamperschutzvorrichtung gemäß zumindest einem der Ansprüche 1 bis 6 gelöst.

Die Aufgabe wird ebenfalls durch ein Tamperschutzsystem gelöst, umfassend zumindest ein Feldgerät, zumindest eine Tamperschutzvorrichtung gemäß zumindest einem der Ansprüche 1-6, zumindest eine Überwachungsvorrichtung, wobei die Tamperschutzvorrichtung an dem Feldgerät zum Tamperschutz angeordnet ist und wobei die Überwachungsvorrichtung mit der Tamperschutzvorrichtung verbunden ist.

Schließlich wird die Aufgabe auch durch die Verwendung einer Tamperschutzvorrichtung gemäß zumindest einem der Ansprüche 1-6 in/oder an einem Feldgerät sowie die Verwendung einer Tamperschutzvorrichtung gemäß zumindest einem der Ansprüche 1-6 als Sicherheitssiegel gelöst.

Der erzielte Vorteil dabei ist, dass damit eine Tamperschutzvorrichtung bereitgestellt wird, welche bei einer physikalischen Manipulation, beispielsweise einem Anbohren, Aufbrechen oder dergleichen irreparabel zerstört wird. Die Sicherheitsinformation in dem durch die physikalische Manipulation zumindest teilweise zerstörten elektronischen Speicher der Tamperschutzvorrichtung kann so nicht mehr rekonstruiert werden. Auf diese Weise ist eine physikalische Manipulation eines Feldgeräts mit einer derartigen Tamperschutzvorrichtung an-

hand der zerstörten Sicherheitsinformation erkennbar. Ein weiterer Vorteil ist, dass eine kontinuierliche oder laufende Überwachung des Tamperschutzes nicht notwendig ist, da eine physikalische Manipulation auch später anhand des modifizierten oder zerstörten Speicherinhalts und damit einer veränderten Sicherheitsinformation erkennbar ist. Ein weiterer Vorteil ist schließlich, dass dabei keine aufwändige Sensorik, wie beispielsweise Drucksensoren, Strahlungssensoren, Temperatursensoren oder ähnliches bereitgestellt werden müssen, was die Herstellungskosten reduziert.

Weitere Merkmale und Vorteile der Erfindung sind in den Unteransprüchen beschrieben.

Vorteilhafterweise ist der Tamperschutzträger als Folie, insbesondere als Kunststofffolie ausgebildet. Der damit erzielte Vorteil ist, dass damit auf einfache und kostengünstige Weise der zumindest eine elektronische Speicher auf dem Tamperschutzträger angeordnet werden kann und gleichzeitig eine einfache Anordnung der Folie, beispielsweise auf einer Leiterplatte, ermöglicht wird. Der zumindest eine elektronische Speicher kann dabei beispielsweise als auf die Folie gedruckte elektronische Schaltung ausgebildet sein. Der Speicher kann insbesondere flächig auf der Folie aufgedruckt sein, und so zumindest einen Teilbereich der Folie abdecken. Weiterhin kann der Speicher in mehreren, voneinander isolierten Schichten übereinander aufgedruckt ausgebildet sein.

Die Folie kann weiter auf einen Träger, beispielsweise eine Leiterplatte geklebt sein. Auch kann die Folie um die Leiterplatte herumgeschlagen werden und verklebt oder verschweißt sein. Eine mit der Leiterplatte stoffschlüssig verbundene Folie kann weiterhin durch aufgebrachtes Epoxyd-Harz geschützt sein und/oder in Epoxyd-Harz vergossen sein.

Zweckmäßigerweise ist der zumindest eine elektronische Speicher ausgebildet, die Sicherheitsinformation permanent oder

veränderbar zu speichern. Der erzielte Vorteil dabei ist, dass bei einem permanenten Speichern der Sicherheitsinformation in dem elektronischen Speicher diese direkt beim Herstellen des Speichers, beispielsweise mittels des genannten Aufdruckens der elektronischen Schaltung, in diesem gespeichert werden kann, so dass eine einfache und kostengünstige Speicherung der Sicherheitsinformation ermöglicht wird. Ist die Sicherheitsinformation in dem zumindest einem elektronischen Speicher veränderbar, beispielsweise während eines Betriebs des Feldgeräts, so kann die Sicherheitsinformation, täglich, stündlich, minütlich oder dergleichen neu erstellt und/oder überschrieben werden. Darüber hinaus ist auch ein kontinuierliches Überschreiben des elektronischen Speichers mit neuen Sicherheitsinformationen möglich. Auf diese Weise kann die Sicherheit noch weiter erhöht werden, da nun anhand des im Wesentlichen ständigen Aktualisierens des zumindest einen elektronischen Speichers auch festgestellt werden kann, wann die jeweilige Sicherheitsinformation in dem zumindest einem elektronischen Speicher gespeichert wurde und wann eine physikalische Manipulation des zumindest einen elektronischen Speichers erfolgt ist: Nach einer physikalischen Manipulation der Tamperschutzvorrichtung kann die Sicherheitsinformation nicht mehr weiter verändert werden, da der zumindest eine elektronische Speicher ganz oder teilweise zerstört wurde. Ist gleichzeitig bekannt, welche Sicherheitsinformationen wann in den zumindest einen elektronischen Speicher geschrieben wurde, kann dann der Zeitpunkt der physikalischen Manipulation ermittelt werden.

Vorteilhafterweise ist der zumindest eine elektronische Speicher ausgebildet, eine von der Sicherheitsinformation abhängige und von ihr verschiedene zweite Information bereitzustellen. Auf diese Weise kann beispielsweise anhand der Sicherheitsinformation ein kryptographischer Schlüssel direkt und/oder mittels einer Schlüsselableitungsfunktion und/oder einer kryptographischen Hash-Funktion, insbesondere SHA-1, SHA256, HMAC-SHA-1, HMAC-SHA256 erzeugt werden. Diese kann

beispielsweise dazu verwendet werden, um eine Entschlüsselung von Daten des Feldgeräts durchzuführen und alternativ oder zusätzlich kann bei der Erstellung des kryptographischen Schlüssels ein Fehlererkennungs- und/oder ein Fehlerkorrekturverfahren angewendet werden, sodass veränderte Inhalte eines Konfigurationsspeichers des Feldgeräts erkennbar und insbesondere zumindest teilweise korrigierbar sind.

Die Sicherheitsinformation kann als eine digital codierte Bitfolge ausgebildet sein.

Zweckmäßigerweise weist die Sicherheitsinformationsdichte der Sicherheitsinformation eine Größe von zumindest 32 Bit, insbesondere zumindest 64 Bit, vorzugsweise zumindest 128 Bit, zweckmäßigerweise zumindest 256 Bit, insbesondere zumindest 512 Bit, besonders vorzugsweise zumindest 1024 Bit auf, insbesondere pro einer Einheitsfläche, wobei die Einheitsfläche weniger als 5 cm^2, insbesondere weniger als 2,5 cm^2, vorzugsweise weniger als 1 cm^2, zweckmäßigerweise weniger als 5 mm^2, besonders vorzugsweise weniger als 1 mm^2 beträgt. Dadurch ist zum einen die in dem zumindest in einem elektronischen Speicher gespeicherte Sicherheitsinformation nicht praktikabel erratbar. Darüber hinaus wird ein noch höherer Schutz gegen physikalische Manipulation erreicht, da bei einer räumlich kleinen physikalischen Manipulation der Tamperschutzvorrichtung bereits viele Bits der Sicherheitsinformation durch die physikalische Manipulation des elektronischen Speichers modifiziert oder zerstört werden.

Vorteilhafterweise ist eine Mehrzahl von elektronischen Speichern angeordnet, die ausgebildet sind, eine gemeinsame Sicherheitsinformation bereitzustellen. Auf diese Weise kann der Speicherbedarf der elektronischen Speicher erheblich reduziert werden, sodass diese noch kostengünstiger und zuverlässiger hergestellt werden können.

Zweckmäßigerweise ist bei dem Tamperschutzsystem die Überwachungsvorrichtung ausgebildet, eine Sicherheitsinformation der Tamperschutz-Überwachungsvorrichtung zu prüfen und in Abhängigkeit des Ergebnisses des Prüfers das Feldgerät zu inaktivieren oder zu aktivieren.

Der damit erzielte Vorteil ist, dass insbesondere wenn die Überwachungsvorrichtung in Feldgerät selbst angeordnet ist, das Feldgerät selbst von einem aktiven in einen inaktiven Zustand wechseln kann, so dass einem Angreifer ein weiterer Zugriff auf das Feldgerät weiter erschwert wird, falls die Prüfung eine Manipulation der Sicherheitsinformation ergibt. Das Feldgerät kann dann selbsttätig beispielsweise in einem Konfigurationsspeicher gespeicherte Schlüssel löschen oder eine Statusmeldung bereitstellen und/oder an eine Leitstelle übertragen oder mittels eines Kurzschlusses elektronische Komponenten des Feldgerätes permanent zerstören, um einen Zugriff auf diese zu verhindern.

Weitere Merkmale und Vorteile der Erfindung ergeben sich aus der nachfolgenden Beschreibung von Ausführungsbeispielen anhand der Zeichnung.

Dabei zeigen in schematischer Form

Fig. 1 ein Feldgerät mit einer Tamperschutzvorrichtung gemäß einer ersten Ausführungsform der vorliegenden Erfindung; und

Fig. 2 Schritte eines Verfahrens zur Herstellung eines Feldgeräts mit einer Tamperschutzvorrichtung gemäß der ersten Ausführungsform.

Fig. 1 zeigt ein Feldgerät mit einer Tamperschutzvorrichtung gemäß einer ersten Ausführungsform der vorliegenden Erfindung.

In Fig. 1 bezeichnet Bezugszeichen 1 ein Feldgerät. Das Feldgerät 1 umfasst einen Träger 2, beispielsweise in Form einer Leiterplatte. Auf dem Träger 2 ist ein Steuerrechner 5, beispielsweise eine CPU oder dergleichen angeordnet, die mit einem Konfigurationsspeicher 6 zum Austausch von Daten verbunden ist. Weiterhin ist der Steuerrechner 5 über eine Leitung mit einem Netzwerkbaustein 8 verbunden, der wiederum eine Schnittstelle 9 zum Übertragen von Daten zu einer Leitstelle, beispielsweise via Ethernet, bereitstellt.

Der Steuerrechner 5 ist weiter über eine Leitung mit einer Ein-/Ausgabeeinheit 7 verbunden. Die Ein-/Ausgabeeinheit 7 ist mit Sensoren und/oder Aktoren 10, beispielsweise Temperaturfühlern, Stellgliedern, etc. verbunden. Ist beispielsweise das Feldgerät 1 als Signalanlage für Züge ausgebildet, kann die Ein-/Ausgabeeinheit mittels des Steuerrechners 5 entsprechende Befehle an Motoren 10 etc. der Signalanlage übermitteln. Gleichzeitig kann mittels der Sensoren 10 überprüft werden, ob die Signalanlage die vom Steuerrechner 5 erhaltene Anweisung ordnungsgemäß durchgeführt hat.

In Fig. 1 ist weiterhin ein gepunkteter rechteckförmiger Bereich zu erkennen, der im Wesentlichen den Steuerrechner 5 und den Konfigurationsspeicher 6 überdeckt. In diesem Bereich ist eine Tamperschutzvorrichtung 4 angeordnet. Die Tamperschutzvorrichtung 4 umfasst als Tamperschutzträger eine Tamperschutzfolie 4a, auf der insbesondere in regelmäßiger Weise elektronische Speicher 3 angeordnet sind. Die Tamperschutzfolie 4a mit den elektronischen Speichern 3 ist dabei so angeordnet, dass die elektronischen Speicher 3 den Steuerrechner 5 sowie den Konfigurationsspeicher 6 vollständig überdecken und so einen Tamperschutz für diese beiden Komponenten bereitstellen. Nicht dargestellt in Fig. 1 sind jeweilige Verbindungen der einzelnen elektronischen Speicher untereinander sowie zumindest eine Verbindung der elektronischen Speicher 3 zu einer Schnittstelle des Steuerrechners 5 und/oder des Konfigurationsspeichers 6, um die in den elektronischen Spei-

chern gespeicherten Sicherheitsinformation M abrufen oder auslesen zu können. Hierüber kann dann der Konfigurationsspeicher 6 und/oder der Steuerrechner 5 beispielsweise über einen I2C-Bus oder SPI die Sicherheitsinformationen M der elektronischen Speicher 3 auslesen und, beispielsweise in Abhängigkeit der ausgelesenen Sicherheitsinformation M oder der ausgelesenen Sicherheitsinformationen M, einen kryptographischen Schlüssel erstellen, der dazu verwendet werden kann, um im Konfigurationsspeicher 6 verschlüsselt abgelegte Konfigurationsdaten des Feldgeräts 1 zu entschlüsseln.

Es ist weiter möglich, die Tamperschutzvorrichtung 4 derart auszubilden, dass diese nicht den Speicherinhalt der elektronischen Speicher 3 direkt bereitstellt, sondern einen davon abhängigen Wert. So kann beispielsweise die Tamperschutzvorrichtung 4 ausgebildet sein, einen Verarbeitungsschritt zur Verwendung der Sicherheitsinformation M der elektronischen Speicher 3 durchzuführen, wobei dann das Ergebnis dieses Verarbeitungsschrittes als Sicherheitsinformation M' bereitgestellt wird. Auf diese Weise ist es möglich, ein Challenge-Response-Verfahren durchzuführen, wobei die Tamperschutzvorrichtung 4 eine Response bereitstellt, die von in den elektronischen Speichern 3 der Tamperschutzvorrichtung 4 gespeicherten Daten und dem an die Tamperschutzvorrichtung 4 übertragenen Challenge-Wert abhängt. Der Response-Wert kann beispielsweise eine identische Kopie von der Tamperschutzvorrichtung 4 bereitgestellten Sicherheitsinformation M' sein, eine Prüfsumme, insbesondere eine CRC-Prüfsumme oder ein Hash-Wert, beispielsweise SHA-1.

Des Weiteren ist es möglich, dass die in den elektronischen Speichern 3 gespeicherten Sicherheitsinformationen M zufällig oder pseudozufällig erzeugt werden.

Fig. 2 zeigt Schritte eines Verfahrens zur Herstellung eines Feldgeräts mit einer Tamperschutzvorrichtung gemäß der ersten Ausführungsform.

In Fig. 2 bezeichnet Bezugszeichen S1 den Schritt Herstellen des Feldgeräts 1, Bezugszeichen S2 den Schritt Herstellen der Tamperschutzvorrichtung 4, Bezugszeichen S3 Anordnen der Tamperschutzvorrichtung 4 an dem Feldgerät 1 und Bezugszeichen S4 Verbinden der Tamperschutzvorrichtung 4 mit einer Überwachungseinrichtung zum Überwachen der Tamperschutzvorrichtung.

Zusammenfassend weist die Erfindung mehrere Vorteile auf. Die Erfindung ermöglicht die Erkennung einer physikalischen Manipulation eines Feldgeräts, ohne dass eine kontinuierliche Überwachung notwendig ist. Auf diese Weise wird beispielweise keine dauerhafte Stromversorgung benötigt. Darüber hinaus ist die Tamperschutzvorrichtung auch einfach und kostengünstig herstellbar, beispielsweise mittels druckbarer Elektronik und/oder druckbarem Speicher. Ein weiterer Vorteil ist, dass dadurch auch ein grossflächigerer Schutz erreicht werden kann. Ein weiterer Vorteil ist, dass eine aufwändige Sensorik zum Erfassen einer physikalischen Manipulation entfällt. Darüber hinaus ist ein erhöhter Schutz durch die Tamperschutzvorrichtung gegenüber physikalischen Manipulationen über die bereits bekannten Tamperschutzvorrichtungen hinaus gegeben.

Obwohl die vorliegende Erfindung vorstehend anhand bevorzugter Ausführungsbeispiele beschrieben wurde, ist sie nicht darauf beschränkt, sondern auf vielfältige Weise modifizierbar.

Patentansprüche

1. Tamperschutzvorrichtung (4) zum Tamperschutz eines Feldgeräts (1), umfassend
einen Tamperschutzträger (4a) und
zumindest einen elektronischen Speicher (3), wobei
der zumindest eine elektronische Speicher (3) in zumindest einem Teilbereich auf dem Tamperschutzträger (4a) angeordnet ist und
der zumindest eine elektronische Speicher (3) zumindest eine vorgebbare Sicherheitsinformation (M) speichert und wobei
der zumindest eine elektronische Speicher (3) ausgebildet ist, bei einer zumindest teilweisen Beschädigung der Tamperschutzvorrichtung (4) die vorgebbare Sicherheitsinformation (M) zu verändern.

2. Tamperschutzvorrichtung gemäß Anspruch 1,
dadurch gekennzeichnet, dass
der Tamperschutzträger (4a) als Folie, insbesondere als Kunststofffolie, ausgebildet ist.

3. Tamperschutzvorrichtung gemäß zumindest einem der Ansprüche 1-2,
dadurch gekennzeichnet, dass
der zumindest eine elektronische Speicher (3) ausgebildet ist, die Sicherheitsinformation (M) permanent oder veränderbar zu speichern.

4. Tamperschutzvorrichtung gemäß zumindest einem der Ansprüche 1-3,
dadurch gekennzeichnet, dass
der zumindest eine elektronische Speicher (3) ausgebildet ist, eine von der Sicherheitsinformation (M) abhängige und von ihr verschiedene zweite Information bereitzustellen.

5. Tamperschutzvorrichtung gemäß zumindest einem der Ansprüche 1-4,
dadurch gekennzeichnet, dass
die Sicherheitsinformation (M) eine Größe von zumindest 32bit, insbesondere zumindest 64 Bit, vorzugsweise zumindest 128 Bit, zweckmäßigerweise zumindest 256 Bit, insbesondere zumindest 512 Bit, besonders vorzugsweise zumindest 1024 Bit auf, insbesondere pro einer Einheitsfläche, wobei die Einheitsfläche weniger als 5 cm^2, insbesondere weniger als 2,5 cm^2, vorzugsweise weniger als 1 cm^2, zweckmäßigerweise weniger als 5 mm^2, besonders vorzugsweise weniger als 1 mm^2 beträgt.

6. Tamperschutzvorrichtung gemäß zumindest einem der Ansprüche 1-5,
dadurch gekennzeichnet, dass
eine Mehrzahl von elektronischen Speichern (3) angeordnet ist, die ausgebildet sind, eine gemeinsame Sicherheitsinformation (M') bereitzustellen.

7. Verfahren zur Herstellung eines Feldgeräts (1) mit einer Tamperschutzvorrichtung (4) gemäß zumindest einem der Ansprüche 1-6, umfassend die Schritte
   - Herstellen (S1) des Feldgeräts (1)
   - Herstellen (S2) der Tamperschutzvorrichtung (4)
   - Anordnen (S3) der Tamperschutzvorrichtung (4) an dem Feldgerät (1)
   - Verbinden (S4) der Tamperschutzvorrichtung (4) mit einer Überwachungseinrichtung (5,6) zum Überwachen der Tamperschutzvorrichtung (4)

8. Feldgerät (1) umfassend eine Tamperschutzvorrichtung (4) gemäß zumindest einem der Ansprüche 1-6.

9. Tamperschutzsystem, umfassend
zumindest ein Feldgerät (1),

zumindest eine Tamperschutzvorrichtung (4) gemäß zumindest einem der Ansprüche 1-6,
zumindest eine Überwachungsvorrichtung (5,6), wobei
die Tamperschutzvorrichtung (4) an dem Feldgerät (1) zum Tamperschutz angeordnet ist und wobei
die Überwachungsvorrichtung (5,6) mit der Tamperschutzvorrichtung (4) verbunden ist.

10. Tamperschutzsystem gemäß Anspruch 9, dadurch gekennzeichnet, dass die Überwachungsvorrichtung (5,6) ausgebildet ist, eine Sicherheitsinformation (M) der Tamperschutz-Überwachungsvorrichtung (4) zu prüfen und in Abhängigkeit des Ergebnisses des Prüfens das Feldgerät (1) zu inaktivieren oder zu aktivieren.

11. Verwendung einer Tamperschutzvorrichtung (4) gemäß zumindest einem der Ansprüche 1-6 in und/oder an einem Feldgerät (1).

12. Verwendung einer Tamperschutzvorrichtung (4) gemäß zumindest einem der Ansprüche 1-6 als Sicherheitssiegel.

FIG 1

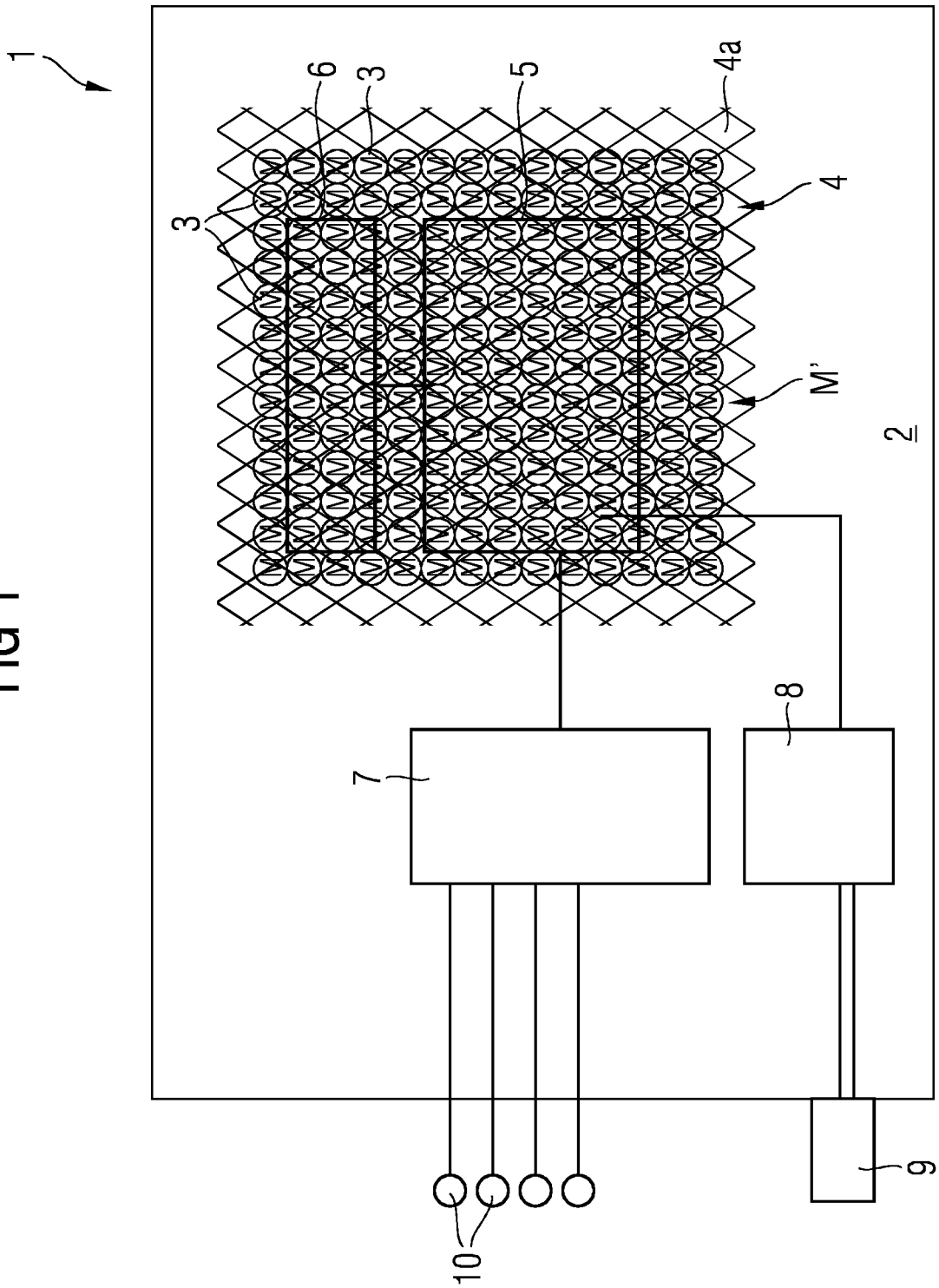
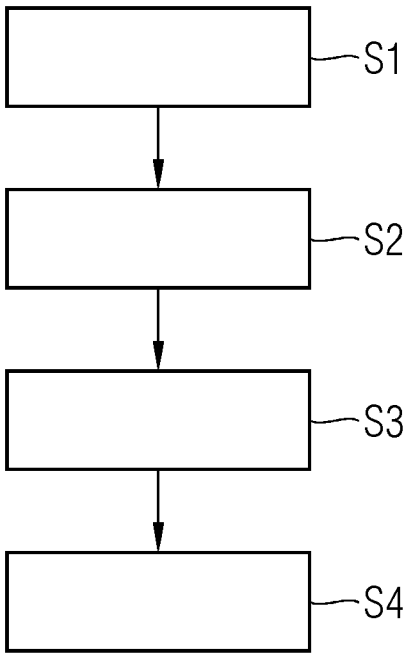


FIG 2



INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2012/056516

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/06
ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2004/055918 A2 (KONINKL PHILIPS ELECTRONICS NV [NL]; KNUDSEN CARL [US]) 1 July 2004 (2004-07-01) the whole document -----	1-12
X	A-R SADEGHI ET AL: "Reconfigurable Physical Unclonable Functions - Enabling technology for tamper-resistant storage", HARDWARE-ORIENTED SECURITY AND TRUST, 2009. HOST '09. IEEE INTERNATIONAL WORKSHOP ON, IEEE, PISCATAWAY, NJ, USA, 27 July 2009 (2009-07-27), pages 22-29, XP031520804, ISBN: 978-1-4244-4805-0 the whole document -----	1-12

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 July 2012	26/07/2012

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Kleiber, Michael

2

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2012/056516

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2004/078787 A1 (CYPAK AB [SE]; EHRENSVAERD JAKOB [SE]; EHRENSVAERD STINA [SE]; ERIKSSO) 16 September 2004 (2004-09-16) the whole document -----	1-12

2

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2012/056516

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2004055918 A2	01-07-2004	AT 460734 T	15-03-2010
		AU 2003288589 A1	09-07-2004
		CN 1729540 A	01-02-2006
		EP 1576614 A2	21-09-2005
		JP 2006514357 A	27-04-2006
		KR 20050089049 A	07-09-2005
		US 2006081497 A1	20-04-2006
		WO 2004055918 A2	01-07-2004
WO 2004078787 A1	16-09-2004	AT 491194 T	15-12-2010
		EP 1599846 A1	30-11-2005
		JP 2006519737 A	31-08-2006
		US 2005011163 A1	20-01-2005
		WO 2004078787 A1	16-09-2004

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2012/056516

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. G06F21/06
ADD.

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
G06F

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

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

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	WO 2004/055918 A2 (KONINKL PHILIPS ELECTRONICS NV [NL]; KNUDSEN CARL [US]) 1. Juli 2004 (2004-07-01) das ganze Dokument -----	1-12
X	A-R SADEGHI ET AL: "Reconfigurable Physical Unclonable Functions - Enabling technology for tamper-resistant storage", HARDWARE-ORIENTED SECURITY AND TRUST, 2009. HOST '09. IEEE INTERNATIONAL WORKSHOP ON, IEEE, PISCATAWAY, NJ, USA, 27. Juli 2009 (2009-07-27), Seiten 22-29, XP031520804, ISBN: 978-1-4244-4805-0 das ganze Dokument -----	1-12
	-/--	

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen [X] Siehe Anhang Patentfamilie

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

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
20. Juli 2012	26/07/2012

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Kleiber, Michael

2

Formblatt PCT/ISA/210 (Blatt 2) (April 2005)

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2012/056516

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	WO 2004/078787 A1 (CYPAK AB [SE]; EHRENSVAERD JAKOB [SE]; EHRENSVAERD STINA [SE]; ERIKSSO) 16. September 2004 (2004-09-16) das ganze Dokument -----	1-12

Formblatt PCT/ISA/210 (Fortsetzung von Blatt 2) (April 2005)

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2012/056516

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 2004055918 A2	01-07-2004	AT 460734 T	15-03-2010
		AU 2003288589 A1	09-07-2004
		CN 1729540 A	01-02-2006
		EP 1576614 A2	21-09-2005
		JP 2006514357 A	27-04-2006
		KR 20050089049 A	07-09-2005
		US 2006081497 A1	20-04-2006
		WO 2004055918 A2	01-07-2004
WO 2004078787 A1	16-09-2004	AT 491194 T	15-12-2010
		EP 1599846 A1	30-11-2005
		JP 2006519737 A	31-08-2006
		US 2005011163 A1	20-01-2005
		WO 2004078787 A1	16-09-2004