

(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
9. September 2016 (09.09.2016)



(10) Internationale Veröffentlichungsnummer
WO 2016/139090 A1

(51) Internationale Patentklassifikation:
G06F 21/57 (2013.01)

(21) Internationales Aktenzeichen: PCT/EP2016/053816

(22) Internationales Anmeldedatum:
24. Februar 2016 (24.02.2016)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
A 50173/2015 5. März 2015 (05.03.2015) AT

(71) Anmelder: **SIEMENS AG ÖSTERREICH** [AT/AT];
Siemensstraße 90, 1210 Wien (AT).

(72) Erfinder: **EPPENSTEINER, Friedrich**; Kremsnerstraße
15, 3620 Spitz (AT). **GHAMESHLU, Majid**; Kopalgasse
40/10, 1110 Wien (AT). **MATSHNIG, Martin**;
Kirschenallee 15, 3430 Tulln (AT). **TAUCHER, Herbert**;
Wiener Straße 9/5, 2340 Mödling (AT).

(74) Anwalt: **MAIER, Daniel**; 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, BN, 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, IR, IS, JP, KE, KG, KN, KP,
KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME,
MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ,
OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA,
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.

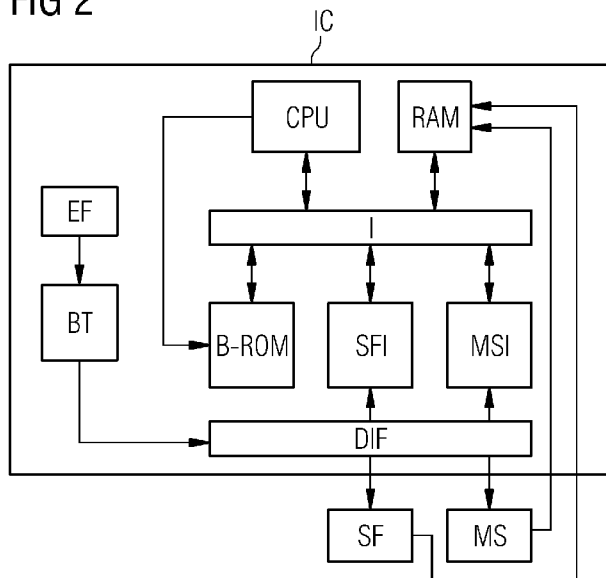
(84) Bestimmungsstaaten (soweit nicht anders angegeben, für
jede verfügbare regionale Schutzrechtsart): ARIPO (BW,
GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST,
SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG,
KZ, RU, TJ, TM), europäisches (AL, AT, BE, BG, CH,
CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, 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, KM, ML, MR, NE, SN, TD, TG).

[Fortsetzung auf der nächsten Seite]

(54) Title: MONITORING THE STARTING OPERATION OF AN INTEGRATED CIRCUIT

(54) Bezeichnung : ÜBERWACHUNG DES STARTVORGANGS EINER INTEGRIERTEN SCHALTUNG

FIG 2



(57) Abstract: The invention relates to a method for
monitoring the starting operation of an integrated
circuit (IC), wherein the starting operation is
performed by using a starting memory (SF), which is
located outside the integrated circuit and is connected
to the integrated circuit by means of a starting
interface (SFI) arranged in the integrated circuit. In
order to reduce the risk of manipulation of the starting
memory, it is provided that an unalterable time period
for the starting operation is prescribed by the
hardware of the integrated circuit (IC) and, if the
prescribed time period is exceeded, the starting
interface (SFI) is disabled.

(57) Zusammenfassung: Die Erfindung betrifft ein
Verfahren zur Überwachung des Startvorgangs einer
integrierten Schaltung (IC), wobei der Startvorgang
unter Verwendung eines außerhalb der integrierten
Schaltung befindlichen Start-Speichers (SF) erfolgt,
der mittels einer in der integrierten Schaltung
angeordneten Start-Schnittstelle (SFI) mit der
integrierten Schaltung verbunden ist. Um die Gefahr
einer Manipulation des Start-Speichers zu verringern,
ist vorgesehen, dass durch die Hardware der
integrierten Schaltung (IC) eine nicht veränderbare
Zeitdauer für den Startvorgang vorgegeben wird und
bei Überschreiten der vorgegebenen Zeitdauer die
Start- Schnittstelle (SFI) gesperrt wird.



Veröffentlicht:

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

Beschreibung

Überwachung des Startvorgangs einer integrierten Schaltung

5

Technisches Gebiet

Die Erfindung betrifft ein Verfahren zur Überwachung des
Startvorgangs (Bootvorgangs) einer integrierten Schaltung,
10 wobei der Startvorgang unter Verwendung eines außerhalb der
integrierten Schaltung befindlichen Start-Speichers erfolgt,
der mittels einer in der integrierten Schaltung angeordneten
Start-Schnittstelle mit der integrierten Schaltung verbunden
ist.

15

Die vorliegende Erfindung liegt auf dem Gebiet der
elektronischen und logischen Schaltungen, insbesondere der so
genannten anwendungsspezifischen, integrierten Schaltungen
oder ASICs.

20

Stand der Technik

Logische bzw. elektronische Schaltungen, welche als
25 integrierte Schaltungen realisiert sind, bilden heutzutage
die Grundlage für jegliche Elektronik, insbesondere in der
Computertechnik. Üblicherweise bestehen derartige
elektronische Schaltungen bzw. Systeme aus auf einem
einzelnen Substrat (z. B. Halbleitersubstrat, etc.)
30 untergebrachten und miteinander verdrahteten elektronischen
Bauelementen bzw. elektronischen Schaltkreisen oder so
genannten Integrated Circuits (ICs). Eine integrierte
Schaltung besteht damit aus einer großen Anzahl von
verschiedenartigen Bauelementen sowie verbindenden
35 Leiterzügen auf oder in einem einkristallinen Substrat. Erst
durch diese Integration ist es möglich, umfangreiche
Funktionalitäten und Anwendungen auf einem kleinen Raum zur
Verfügung zu stellen. Durch integrierte Schaltungen wird eine

Vielzahl von Anwendungen (z. B. in mobilen Geräten, SIM-Karten, RFIDs, Mobiltelefonen, etc.) erst technisch realisierbar, da diese Anwendungen sonst oft zu teuer, zu komplex, zu leistungsintensiv oder zu groß (z.B. für einen
5 Einbau in das jeweilige Gerät, etc.) wären. Werden derartige logische bzw. integrierte Schaltungen für spezielle Anwendungen erstellt, so werden diese Schaltungen auch als anwendungsspezifische, integrierte Schaltungen oder als application-specific integrated circuit bzw. kurz als ASICs
10 bezeichnet.

Eine Verkleinerung von Geräten und ein ständig steigender Integrationsgrad haben dazu geführt, dass mittlerweile ganze Systeme z.B. mit Prozessoren, Controllern, Speicherbausteinen
15 (z. B. RAMs, ROMs, etc.), Power-Management und anderen Komponenten auf einem so genannten Chip oder Die untergebracht werden. Derartige Systeme werden auch als Ein-Chip-Systeme oder System-on-Chip (SoC) bezeichnet und vor allem im Mobilfunkbereich, für Embedded Computer,
20 Smartphones, CD- und DVD-Geräte und überall dort bei Anwendungen eingesetzt, wo kleine Abmessungen bei relativ hoher Leistung und vielfältige Aufgaben gefragt sind.

Bei einem System-on-Chip (SoC) oder Ein-Chip-System sind alle
25 oder ein großer Teil der Funktionen des Systems auf dem Chip integriert - d. h. in einem integrierten Schaltkreis auf einem Halbleiter-Substrat. Üblicherweise werden heutzutage System-on-Chips bzw. Ein-Chip-Systeme nicht mehr komplett neu entwickelt, sondern Entwürfe basieren zumindest teilweise auf
30 bereits vorhandenen und/oder zugekauften Komponenten - so genannten IP-Core-Einheiten oder IP-Blöcken (z. B. Prozessor, Controller-Einheiten, Peripherieblöcke, etc.). Diese IP-Blöcke werden z.B. als fertige Einheit oder mittels Design-Lizenzen erworben und dann in einem neuen Ein-Chip-System
35 direkt oder in angepasster Form verwendet. Fehlende Einheiten für das Ein-Chip-System können dann z.B. für den fertigen ASIC dazu entwickelt werden. Verbunden werden die Einheiten eines derartigen Ein-Chip-Systems intern über ein Bussystem.

Integrierte Schaltungen können durch ein sogenanntes Field Programmable Gate Array (FPGA) verwirklicht werden. Ein FGPA ist ein integrierter Schaltkreis (IC) der Digitaltechnik, in
5 den eine logische Schaltung programmiert werden kann. Programmieren heißt hier, dass dessen Funktionsstruktur definiert wird. Beim Programmieren der Verschaltung der vorgegebenen Elemente wird die Funktionsweise einzelner Blöcke im FPGA und deren Verschaltung untereinander
10 festgelegt. Durch die spezifische Konfiguration interner Strukturen können in einem FPGA verschiedene Schaltungen realisiert werden, bis zu hochkomplexen Schaltungen, wie Mikroprozessoren. FPGAs werden vor allem dort eingesetzt, wo es auf schnelle Signalverarbeitung und flexible Änderung der
15 Schaltung ankommt, um beispielsweise nachträgliche Verbesserungen an den implementierten Funktionen vornehmen zu können, ohne dabei direkt die physische Hardware ändern zu müssen.

20 Die wesensbestimmende Grundstruktur eines FPGA ist ein Feld (engl. Array) aus Basisblöcken mit jeweils einer einfachen programmierbaren Lookup-Tabelle (LUT) und einem 1-Bit-Register (Flipflop). Die Programmierung der gewünschten Funktion erfolgt durch die Hinterlegung der definierenden
25 Wahrheitstabelle in den SRAM-Zellen der LUT, die Funktionsberechnung durch das Auslesen der durch die Eingänge bestimmten Speicheradresse. Neben den LUTs ist auf dem FPGA auch die Verschaltung der Komponenten in großen Freiheitsgraden konfigurierbar. Für Verbindungen über weite
30 Entfernungen liegt zwischen den Basisblöcken ein Gitter aus Busstrukturen, an das Ein- und Ausgänge angeschlossen werden können. Weitere programmierbare Schaltkomponenten in den Kreuzungspunkten des Gitters erlauben die Signalverteilung über den gesamten Chip.

35 Eingangs-/Ausgangs-Blöcke dienen der Kommunikation mit der Außenwelt, über sie werden die Anschlüsse des FPGA mit der Schaltmatrix verbunden. Taktgeneratoren erzeugen ausgehend

von an den Eingängen zur Verfügung gestellten Takten alle für die Anwendung benötigten internen Takte. In komplexen FPGAs sind zusätzliche fest verdrahtete Funktionen enthalten, wie z. B. Speicherblöcke (sog. Block RAM).

5

FPGAs, die im Bereich von System-on-Chip-Anwendung (SoC) finden, besitzen eine Reihe meist komplexer Hard-Cores, um ein komplettes System aufzunehmen. Hard-Cores sind feste und unveränderliche Schaltungen von meist komplexen

10 Funktionsblöcken, wie beispielsweise Mikrocontroller oder Ethernet-Schnittstellen.

Die Programmierung der LUTs eines FGPA und der Verbindungsstrukturen erfolgt typischerweise einmal vor jedem Einsatz, wodurch der FPGA auf eine konkrete Funktion konfiguriert wird. Dies ist notwendig, da der FPGA durch Abschalten der Betriebsspannung seine Konfiguration wieder verliert.

15

20 Unabhängig davon, ob die integrierte Schaltung nun als FPGA verwirklicht ist oder nicht, umfasst diese in der Regel eine eigene Speichereinheit (Boot ROM) mit entsprechendem Programmcode auf dem Chip, um die integrierte Schaltung zu initialisieren. Aus Platzgründen sind jedoch weitere
25 Programme, etwa für das Starten der Funktion der integrierten Schaltung, wie der sogenannte Second Level Boot Code, nicht in der integrierten Schaltung gespeichert, sondern werden in eigenen elektronischen Flash-Speichern, z.B. Flash-Bausteinen, abgelegt, die sich auf der gleichen Platine wie
30 die integrierte Schaltung befinden.

Ein Flash-Speicher, genauer ein Flash-EEPROM, ist ein nichtflüchtiger, elektronischer Speicherbaustein, dessen gespeicherte Information elektrisch gelöscht werden kann,
35 wobei immer bestimmte Blöcke gelöscht und neu programmiert werden können.

Während des Startvorgangs wird das Startprogramm, meist in mehreren Programmteilen, vom Flash-Speicher in den Arbeitsspeicher des integrierten Schaltkreises kopiert und von dort ausgeführt. Durch Fremdeingriffe können die Inhalte des Flash-Speichers manipuliert oder vollständig ausgetauscht werden. Dies hat negative Auswirkungen auf die Sicherheit des integrierten Schaltkreises.

Bisher ist man dieser Gefahr beispielsweise mittels des sogenannten „trusted boot“ Prinzips begegnet. Dabei wird der Startvorgang mit einer Überprüfung der Integrität der Hardware verknüpft. Vor dem eigentlichen Startvorgang überprüft etwa ein sogenanntes „Core Root of Trust Measurement“ (CRTM)-Modul die zugrunde liegende Hardware und speichert einen Signatur-Messwert in einem geschützten Speicherbereich ab. Diese Information wird dann beim Starten verwendet um zu entscheiden, ob das zugrunde liegende System vertrauenswürdig ist.

Diese Überprüfung hat allerdings den Nachteil, dass sie mittels Software erfolgt, die selbst wieder manipuliert werden kann.

Darstellung der Erfindung

Es ist eine Aufgabe der vorliegenden Erfindung, ein Verfahren zur Überwachung des Startvorgangs zur Verfügung zu stellen, welches die Gefahr einer Manipulation des Start-Speichers verringert.

Diese Aufgabe wird durch ein Verfahren mit den Merkmalen des Patentanspruchs 1 gelöst, bei welchem der Startvorgang unter Verwendung eines außerhalb der integrierten Schaltung befindlichen Start-Speichers erfolgt, der mittels einer in der integrierten Schaltung angeordneten Start-Schnittstelle mit der integrierten Schaltung verbunden ist.

Gemäß Anspruch 1 ist bei dem Verfahren zur Überwachung des Startvorgangs einer integrierten Schaltung vorgesehen, dass durch die Hardware der integrierten Schaltung eine nicht veränderbare Zeitdauer für den Startvorgang vorgegeben wird und bei Überschreiten der vorgegebenen Zeitdauer die Start-Schnittstelle gesperrt wird.

Dadurch, dass für den Startvorgang, das Booten oder Initialisieren, nur eine begrenzte Zeit zur Verfügung gestellt wird, nämlich nur jene, die erfahrungsgemäß für den Startvorgang benötigt wird, kann verhindert werden, dass durch Manipulationen des Start-Speichers längere, unzulässige Programme zum Einsatz kommen. Zudem wird verhindert, dass die integrierte Schaltung durch den Einsatz eines CPU-Debuggers ausspioniert wird, weil ein CPU-Debugger in der Regel auch eine Zeit benötigt, die länger ist als jene für den Startvorgang.

Da die erfindungsgemäße Sperre der Start-Schnittstelle unveränderbar in Hardware, und nicht durch Software, realisiert wird, kann sie nicht durch Manipulationsversuche umgangen werden.

Die Zeitdauer, die für den Startvorgang benötigt wird, kann am einfachsten durch einen als Teilschaltung ausgeführten Zeitschalter (Timer) der integrierten Schaltung gemessen werden.

Die Zeitdauer, die für den Startvorgang benötigt wird, wird vorzugsweise im Zeitpunkt der Fertigung der integrierten Schaltung mit zumindest einer elektronischen programmierbaren Sicherung, die in der integrierten Schaltung enthalten ist, eingestellt.

Eine solche elektronische Sicherung wird auch als eFUSE bezeichnet. Für den genannten Zweck sind in der Regel mehrere eFUSES notwendig. Diese Sicherungen sind Hardware-Bauteile, die einmal elektrisch programmiert werden können, diese

Programmierung ist dann aber nicht mehr änderbar. Bei der Programmierung wird die Sicherung mit Hilfe einer zugeführten Fuse-Spannung durchgebrannt.

- 5 Insbesondere kann vorgesehen sein, dass das Entsperren der Start-Schnittstelle ausschließlich durch ein Einschaltrücksetzsignal erfolgt. Wurde also die durch den Zeitschalter vorgegebene Zeitdauer für den Startvorgang überschritten und folglich die Start-Schnittstelle gesperrt,
10 kann ein neuer Startvorgang erst wieder durchgeführt werden, wenn durch einen sogenannten Power-on Reset der Zeitschalter (Timer) wieder neu gestartet wird.

Eine integrierte Schaltung weist in der Regel neben der
15 Start-Schnittstelle weitere Schnittstellen auf. Falls diese bereits zu Beginn des Startvorgangs freigegeben werden, wenn also der Startvorgang (das Booten) noch gar nicht abgeschlossen ist, kann auch über die weiteren Schnittstellen eine unbefugte Änderung von Programmen oder Programmteilen,
20 insbesondere des Startprogramms, erfolgen. Insofern kann vorgesehen werden, dass zumindest eine weitere Schnittstelle der integrierten Schaltung in Abhängigkeit vom Fortschritt des Startvorgangs freigegeben wird. Diese weitere Schnittstelle ist also zu Beginn des Startvorgangs gesperrt.

25 Insbesondere kann vorgesehen sein, dass die weitere Schnittstelle der integrierten Schaltung erst nach Abschluss des Startvorgangs freigegeben wird.

- 30 Der Start-Speicher ist vorzugsweise als serieller Flash-Speicher ausgeführt.

Eine erfindungsgemäße integrierte Schaltung umfasst zumindest eine Start-Schnittstelle, mittels welcher ein Start-Speicher
35 mit der integrierten Schaltung verbunden werden kann, und ist dadurch gekennzeichnet, dass in der integrierten Schaltung eine Hardware-Einheit vorgesehen ist, die so ausgebildet ist, dass nach Ablauf einer für den Startvorgang vorgegeben, nicht

veränderbaren Zeitdauer die Start-Schnittstelle gesperrt wird.

Die bevorzugte Ausführungsform der integrierten Schaltung
5 sieht vor, dass die Hardware-Einheit einen als Teilschaltung
ausgeführten Zeitschalter aufweist sowie zumindest eine
elektronisch programmierbare Sicherung. Die Hardware-Einheit
kann darüber hinaus so ausgebildet sein, dass zumindest eine
10 weitere Schnittstelle der integrierten Schaltung in
Abhängigkeit vom Fortschritt des Startvorgangs freigegeben
wird. Insbesondere kann die weitere Schnittstelle erst nach
Ablauf der für den Startvorgang vorgegeben, nicht
veränderbaren Zeitdauer freigegeben werden.

15 Die Freigabe und Sperrung der Start-Schnittstelle und
gegebenenfalls der weiteren Schnittstelle kann erreicht
werden, indem die Hardware-Einheit so ausgebildet ist, dass
diesen Schnittstellen eine dynamische Schnittstellen-Freigabe
vorgesaltet ist.

20

Kurzbeschreibung der Figuren

Zur weiteren Erläuterung der Erfindung wird im nachfolgenden
25 Teil der Beschreibung auf die Figuren Bezug genommen, aus der
weitere vorteilhafte Ausgestaltungen, Einzelheiten und
Weiterbildungen der Erfindung zu entnehmen sind. Die Figuren
sind beispielhaft zu verstehen und sollen den
Erfindungscharakter zwar darlegen, ihn aber keinesfalls
30 einengen oder gar abschließend wiedergeben. Es zeigen:

- Fig. 1 eine schematische Darstellung einer integrierten
Schaltung nach dem Stand der Technik
- 35 Fig. 2 eine schematische Darstellung einer
erfindungsgemäßen integrierten Schaltung

Ausführung der Erfindung

Für die integrierte Schaltung IC sind in den Figuren nur die für die Erfindung wesentlichen Einheiten dargestellt. Sie
5 kann und wird in der Regel darüber hinaus weitere Einheiten, wie Ein-/Ausgabeeinheiten, Controller, zusätzliche Schnittstellen, weitere Prozessoren, Speicher, enthalten.

In Fig. 1 ist eine integrierte Schaltung IC gemäß dem Stand
10 der Technik dargestellt, mit einem Prozessor CPU und einem Arbeitsspeicher RAM, wobei CPU und RAM über eine Verbindungseinheit (Interconnect) I, z.B. ein Bussystem, miteinander verbunden sind. An das Verbindungssystem sind
15 auch ein interner Boot-Speicher (Boot ROM) B-ROM, eine Schnittstelle für den Start-Speicher (Serial Flash Interface) SFI sowie eine Schnittstelle für einen Massenspeicher (Mass Storage Interface) MSI angeschlossen. Alle genannten Einheiten sind Bestandteil der integrierten Schaltung IC.

20 Auf derselben Baugruppe wie die integrierte Schaltung IC, aber nicht als Bestandteil der integrierten Schaltung IC, ist ein Start-Speicher SF vorgesehen und etwa als serieller Flash-Speicher (Serial Flash) ausgeführt. Der Start-Speicher SF ist fix mit der Schnittstelle SFI verbunden.

25 Ebenso kann am selben Board wie die integrierte Schaltung IC, aber nicht als Bestandteil der integrierten Schaltung IC, ein Massenspeicher (Mass Storage) MS vorgesehen sein, der mit der entsprechenden Schnittstelle MSI fest verbunden ist. Oder der
30 Massenspeicher MS könnte lösbar mit der Schnittstelle MSI verbunden sein, etwa als SD-Karte. Die Schnittstelle MSI ist hier bereits während des Startvorgangs freigegeben.

Nach einem Power-on Reset oder bei einem Neustart muss die
35 integrierte Schaltung initialisiert werden. Das heißt, nach dem Anlegen einer Betriebsspannung wird die integrierte Schaltung gezielt in einen definierten Anfangszustand übergeführt. Dies ist deshalb erforderlich, da integrierte

Schaltkreise sowohl kombinatorische Funktionen (logische Gatter) als auch Speicherelemente wie zum Beispiel Flip-Flops oder RAM-Zellen umfassen. Diese können sich aus Gründen der gegenseitigen Beeinflussung und der physikalisch bedingten leicht unterschiedlichen Beaufschlagung mit Strom während des Einschaltzeitpunkts unvorhersehbar verhalten und somit auch nach dem Einschalten ebenfalls unvorhersehbare Zustände annehmen. Damit befindet sich die gesamte integrierte Schaltung in einem undefinierten Zustand und arbeitet fehlerhaft oder gar nicht.

Bei der Initialisierung greift der Prozessor CPU auf den Boot-Speicher B-ROM zu, was durch einen Pfeil dargestellt ist. Während dieses Startvorgangs werden aber auch übergelagerte Programmteile in den Arbeitsspeicher RAM geladen, sogenannter „Second Level Boot Code“, der auf dem Start-Speicher SF gespeichert ist, siehe entsprechender Pfeil. Während des Betriebs werden andere Programme und/oder Daten in den Arbeitsspeicher RAM geladen, die auf dem Massenspeicher MS abgespeichert sind, und die ebenfalls für den anschließenden Normalbetrieb der integrierten Schaltung notwendig sind.

Während des Startvorgangs (=Boot, = Initialisierens) könnte nun von außerhalb der integrierten Schaltung IC unbefugt eine Manipulation des Start-Speichers SF und/oder des Massenspeichers MS erfolgen, sodass der Startvorgang nicht korrekt abgeschlossen wird und die integrierte Schaltung IC den Normalbetrieb gar nicht oder nicht ordnungsgemäß aufnehmen kann. Oder es könnte während des Startvorgangs unbefugt ein CPU-Debugger über eine der Schnittstellen SFI oder MSI die integrierte Schaltung IC ausspionieren.

Dies wird durch eine erfindungsgemäße Schaltung gemäß Fig. 2 verhindert: Diese integrierte Schaltung IC ist grundsätzlich gleich wie jene in Fig. 1 ausgeführt, jedoch weist sie eine erfindungsgemäße Hardware-Einheit auf, die in der integrierten Schaltung IC integriert ist. Die Hardware-

Einheit besteht im Wesentlichen aus den folgenden Einheiten, die untereinander verbunden sind: ein Zeitschalter (Boot Timer) BT, zumindest eine elektronische programmierbare Sicherung (eFUSE) EF und eine dynamische Schnittstellen-Freigabe DIF.

Die dynamische Schnittstellen-Freigabe DIF ist vor der Schnittstelle SFI für den Start-Speicher und der Schnittstelle für den Massenspeicher MSI angeordnet und kann diese Schnittstellen freigegeben oder sperren. Diese dynamische Schnittstellen-Freigabe DIF befindet sich somit zwischen Start-Speicher SF und Massenspeicher MS einerseits und den Schnittstellen SFI und MSI andererseits.

Den elektronischen programmierbaren Sicherungen (eFUSES) EF wird bei der Herstellung der integrierten Schaltung IC jene Zeitdauer einprogrammiert, die für den Startvorgang benötigt wird. Beim Startvorgang beginnt der Zeitschalter BT der integrierten Schaltung zu zählen und wird von den eFUSES zum vorprogrammierten Zeitpunkt gestoppt. Dann sperrt die dynamische Schnittstellen-Freigabe DIF den Zugang zur Schnittstelle SFI für den Start-Speicher, sodass über diese Schnittstelle von außen keine Verbindung zur integrierten Schaltung IC mehr hergestellt werden kann.

Die dynamische Schnittstellen-Freigabe DIF sorgt weiters dafür, dass die Schnittstelle MSI für den Massenspeicher MS während des Startvorgangs gesperrt ist und erst nach Abschluss des Startvorgangs freigegeben wird. Auf diese Weise wird sichergestellt, dass über die Schnittstelle MSI während des Startvorgangs keine Manipulationen vorgenommen werden können.

Wenn der Startvorgang ordnungsgemäß verlaufen ist, wurden die Daten des Startspeichers SF vollständig in den Arbeitsspeicher RAM geladen, und gegebenenfalls ebenso die Daten vom Massenspeicher MS, und die integrierte Schaltung IC kann ordnungsgemäß ihren Normalbetrieb beginnen.

Ist während des Startvorgangs eine Manipulation am Start-Speicher SF oder ein unerlaubter Zugriff über die Schnittstelle SFI erfolgt, werden diese nach der
5 vorprogrammierten Zeitdauer jedenfalls durch die Sperre der Schnittstelle SFI beendet. Die Sperre der Schnittstelle SFI kann nur durch einen Power-on Reset wieder aufgehoben werden, weil nur auf diese Weise der Zeitschalter BT wieder neu gestartet werden kann.

10 Grundsätzlich besteht die Möglichkeit, mehrere Zeitschalter BT mit zugeordneten programmierbaren eFUSES EF vorzusehen, sodass ein Zeitschalter BT die Zeitdauer bis zur Sperre der Schnittstelle für den Start-Speicher SFI zählt, während ein
15 zweiter Zeitschalter eine andere (kürzere) Zeitdauer vorgibt, nach deren Verstreichen die Schnittstelle MSI für den Massenspeicher freigegeben wird.

20 Bezugszeichenliste:

	B-ROM	interner Boot-Speicher (Boot ROM)
	BT	Zeitschalter (Boot Timer)
	CPU	Prozessor
25	DIF	dynamische Schnittstellen-Freigabe
	EF	elektronische programmierbare Sicherung (eFUSE)
	I	Verbindungseinheit
	IC	integrierte Schaltung
	MS	Massenspeicher (Mass Storage)
30	MSI	Schnittstelle für den Massenspeicher (Mass Storage Interface)
	RAM	Arbeitsspeicher
	SF	Start-Speicher (Serial Flash, serieller Flash-Speicher)
35	SFI	Schnittstelle für den Start-Speicher (Serial Flash Interface)

Patentansprüche

1. Verfahren zur Überwachung des Startvorgangs einer integrierten Schaltung (IC), wobei der Startvorgang unter Verwendung eines außerhalb der integrierten Schaltung befindlichen Start-Speichers (SF) erfolgt, der mittels einer in der integrierten Schaltung angeordneten Start-Schnittstelle (SFI) mit der integrierten Schaltung verbunden ist, **dadurch gekennzeichnet**,
dass durch die Hardware der integrierten Schaltung (IC) eine nicht veränderbare Zeitdauer für den Startvorgang vorgegeben wird und bei Überschreiten der vorgegebenen Zeitdauer die Start-Schnittstelle (SFI) gesperrt wird.
2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet**, dass die Zeitdauer durch einen als Teilschaltung ausgeführten Zeitschalter (BT) der integrierten Schaltung gemessen wird.
3. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet**, dass die Zeitdauer im Zeitpunkt der Fertigung der integrierten Schaltung (IC) mit zumindest einer elektronischen programmierbaren Sicherung (EF), die in der integrierten Schaltung enthalten ist, eingestellt wird.
4. Verfahren nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet**, dass das Entsperren der Start-

Schnittstelle (SFI) ausschließlich durch ein Einschalt zurücksetzsignal erfolgt.

5. Verfahren nach einem der Ansprüche 1 bis 4, **dadurch gekennzeichnet**, dass zumindest eine weitere
5 Schnittstelle (MSI) der integrierten Schaltung (IC) in Abhängigkeit vom Fortschritt des Startvorgangs freigegeben wird.
6. Verfahren nach Anspruch 5, **dadurch gekennzeichnet**, dass
10 die weitere Schnittstelle (MSI) der integrierten Schaltung (IC) erst nach Abschluss des Startvorgangs freigegeben wird.
7. Verfahren nach einem der Ansprüche 1 bis 6, **dadurch gekennzeichnet**, dass der Start-Speicher (SF) als serieller Flash-Speicher ausgeführt ist.
- 15 8. Verfahren nach einem der Ansprüche 1 bis 7, **dadurch gekennzeichnet**, dass durch die Hardware der integrierten Schaltung (IC) eine nicht veränderbare Zeitdauer bis zur Freigabe eines Massenspeichers (MS) vorgegeben wird.
9. Integrierte Schaltung (IC) zur Durchführung eines
20 Verfahrens nach einem der Ansprüche 1 bis 8, umfassend zumindest eine Start-Schnittstelle (SFI), mittels welcher ein Start-Speicher (SF) mit der integrierten Schaltung verbunden werden kann, **dadurch gekennzeichnet**,

dass in der integrierten Schaltung eine Hardware-Einheit (EF, BT, DIF) vorgesehen ist, die so ausgebildet ist, dass nach Ablauf einer für den Startvorgang vorgegeben, nicht veränderbaren Zeitdauer die Start-Schnittstelle (SFI) gesperrt wird.

10. Integrierte Schaltung (IC) nach Anspruch 9, **dadurch gekennzeichnet**, dass die Hardware-Einheit (EF, BT, DIF) einen als Teilschaltung ausgeführten Zeitschalter (BT) aufweist.
- 10 11. Integrierte Schaltung (IC) nach Anspruch 9 oder 10, **dadurch gekennzeichnet**, dass die Hardware-Einheit (EF, BT, DIF) zumindest eine elektronisch programmierbare Sicherung (EF) aufweist.
12. Integrierte Schaltung (IC) nach einem der Ansprüche 9 bis 11, **dadurch gekennzeichnet**, dass die Hardware-Einheit (EF, BT, DIF) so ausgebildet ist, dass zumindest eine weitere Schnittstelle (MSI) der integrierten Schaltung in Abhängigkeit vom Fortschritt des Startvorgangs freigegeben wird.
- 15 12. Integrierte Schaltung (IC) nach einem der Ansprüche 9 bis 11, **dadurch gekennzeichnet**, dass die Hardware-Einheit (EF, BT, DIF) so ausgebildet ist, dass zumindest eine weitere Schnittstelle (MSI) der integrierten Schaltung in Abhängigkeit vom Fortschritt des Startvorgangs freigegeben wird.
- 20 13. Integrierte Schaltung (IC) nach Anspruch 12, **dadurch gekennzeichnet**, dass die weitere Schnittstelle (MSI) nach Ablauf der für den Startvorgang vorgegeben, nicht veränderbaren Zeitdauer freigegeben wird.

14. Integrierte Schaltung (IC) nach einem der Ansprüche 9 bis 13, **dadurch gekennzeichnet**, dass ein Start-Speicher (SF) als serieller Flash-Speicher ausgeführt und mit der integrierten Schaltung (IC) verbunden ist.
- 5 15. Integrierte Schaltung (IC) nach einem der Ansprüche 9 bis 14, **dadurch gekennzeichnet**, dass die Hardware-Einheit (EF, BT, DIF) so ausgebildet ist, dass der Start-Schnittstelle (SFI) und gegebenenfalls der weiteren Schnittstelle (MSI) eine dynamische
- 10 Schnittstellen-Freigabe (DIF) vorgeschaltet ist.
16. Integrierte Schaltung (IC) nach einem der Ansprüche 9 bis 15, **dadurch gekennzeichnet**, dass die Hardware-Einheit (EF, BT, DIF) so ausgebildet ist, dass eine nicht veränderbare Zeitdauer bis zur Freigabe eines
- 15 Massenspeichers (MS) vorgegeben wird.

FIG 1

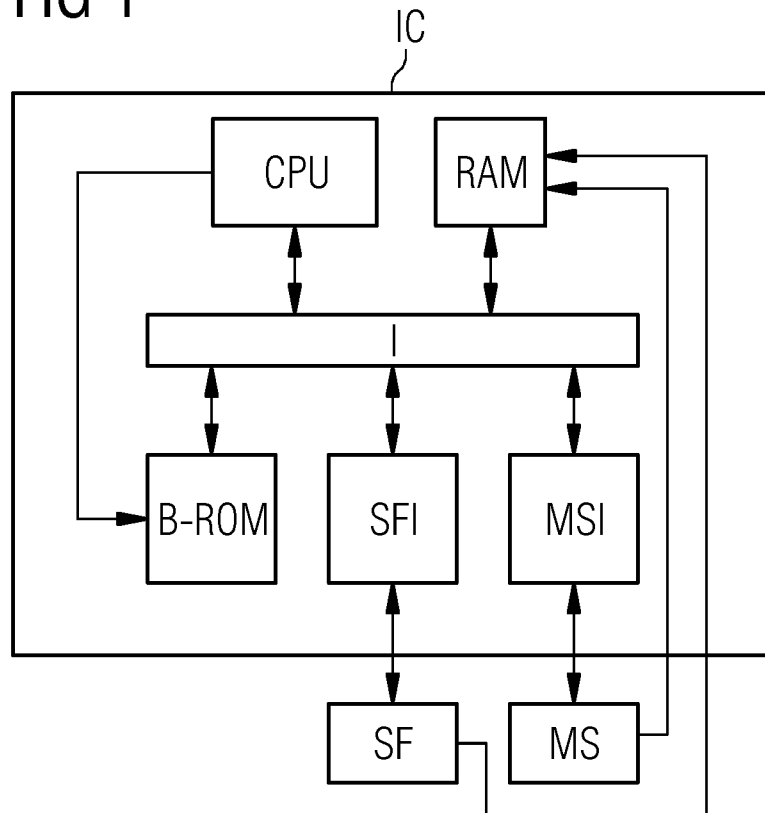
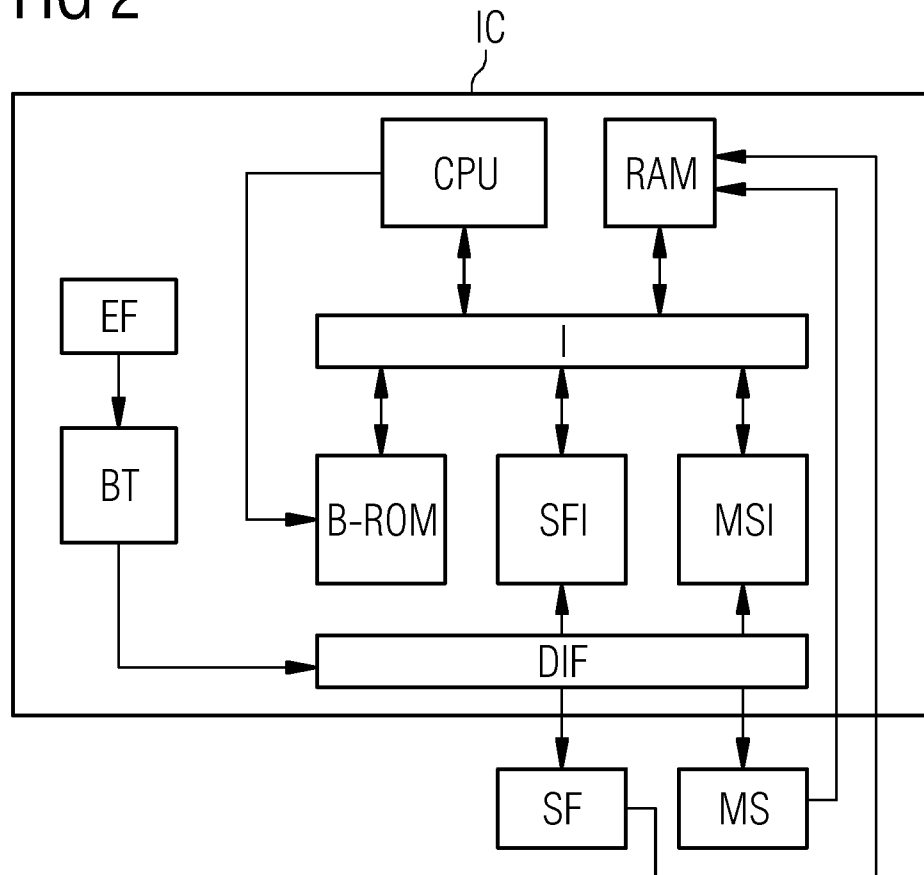


FIG 2



INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2016/053816A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/57
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 2014/142659 A1 (UKSI B V [NL]) 18 September 2014 (2014-09-18) page 1, line 30 - page 2 page 5, line 30 - page 6, line 7 -----	1-16



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

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

"E" earlier 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

15 April 2016

Date of mailing of the international search report

03/05/2016

Name and mailing address of the ISA/

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

Authorized officer

Ebert, Werner

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2016/053816

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2014142659 A1	18-09-2014	NL 2010437 C WO 2014142659 A1	15-09-2014 18-09-2014

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. G06F21/57
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 2014/142659 A1 (UKSI B V [NL]) 18. September 2014 (2014-09-18) Seite 1, Zeile 30 - Seite 2 Seite 5, Zeile 30 - Seite 6, Zeile 7 -----	1-16



Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen



Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" 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

15. April 2016

Absendedatum des internationalen Recherchenberichts

03/05/2016

Name und Postanschrift der Internationalen Recherchenbehörde

Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Ebert, Werner

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

PCT/EP2016/053816

Formblatt PCT/ISA/210 (Anhang Patentfamilie) (April 2005)