



Microcontrollersicherungsverfahren

Die Erfindung betrifft ein Verfahren zum Sichern von Microcontrollerprogrammen mit externen Speichern vor Auslesbarkeit und das Sichern von Microcontrollerbaugruppen vor Dublizierbarkeit.

- 5 In vielen Anwendungsfällen wird häufig eine Vielzahl von Mikrocontrollern benötigt, wobei jeder Microcontroller möglichst einzigartig sein soll und der Inhalt des Microcontrollers nicht für Außenstehende zugänglich sein darf. Ein Anwendungsbereich ist beispielsweise im Identifikations- und Verschlüsselungsbereich zu sehen, wo spezielle interne Schlüssel benötigt werden, aber eine
- 10 Serienproduktion von geschlossenen Schaltkreisen in EEPROM-Technologie aus Kostengründen nicht möglich ist. Oft muß die Know-how tragende Firma ihre Produktion außer Haus geben, in einem solchen Fall kommt es zu einer notwendigen Informationsübergabe an den Produktionsbetrieb, so daß dieser in der Lage ist, mehr oder sehr ähnliche Bauelemente auf eigene Kosten herzustellen und
- 15 selbst zu vermarkten, ohne daß der Auftraggeber davon etwas weiß.

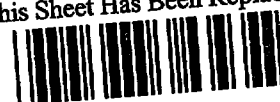
- Im bisherigen Stand der Technik ist ein Verfahren und eine Schaltungsanordnung zur Lösung einer ähnlichen Aufgabe nach der Druckschrift EP 0 114 522 bekannt. Das Ziel dieses Verfahrens besteht lediglich darin, daß nach der Fertigstellung des
- 20 ROM-Bausteins, die Kopie dieses Bausteins erschwert wird, indem nicht nur ein einfacher ROM an die Microcontrollerbaugruppe angeschlossen wird, sondern ein Modul, bestehend aus einem ROM, einer Ver- und Entschlüsselungseinheit und einem Schlüsselspeicher. Die vom Microcontroller benötigten Informationen gelangen so verschlüsselt zum Microcontroller, der wiederum eine Ver- und Entschlüsselungseinheit und ein Schlüsselfeld benötigt, um dann die so
- 25 gewonnenen Informationen in umsetzbaren Code oder Klartext zu verarbeiten. Dabei wird in der Initialisierungsphase von der Microcontrollereinheit ein Schlüssel an den ROM gesandt, mit dem dann die Informationen im weiteren verschlüsselt übertragen werden. Damit soll sichergestellt werden, daß kein Nutzer die Information im Klartext lesen kann.

Der Nachteil dieses Verfahrens besteht darin, daß lediglich vor der Kopie des Inhaltes des ROM's durch nichtprofessionelle Anwender geschützt wird. Die Kosten für eine solche Lösung sind auch erheblich größer gegenüber der Benutzung eines standardmäßigen ROM's, es muß die Ver- und Entschlüsselungseinheit sowohl im ROM-Modul als auch im Microcontrollermodul implementiert werden. Einen Angriffspunkt stellt auch das Abhören des zugesandten Schlüssels dar. In Kenntnis der Ver- und Entschlüsselungstechnik, die aus Kostengründen nicht sehr aufwendig sein darf, ist eine Dublizierung des ROM's auch für nichtprofessionelle Anwender möglich. Die Art des Verschlüsselungsalgorithmus kann ebenfalls nur durch die Änderung des gesamten Microcontrollersystems erreicht werden. Es können immer nur Module verwandt werden, die diesem im Microcontrollermodul befindlichen Verschlüsselungssystem entsprechen, so daß die zugesandten Paßwörter auch diesen einen bestimmten verschlüsselten Text erzeugen.

Für professionelle Anwender, die einen solchen ROM als Raubkopie herstellen möchten, das kann auch der Produzent des Moduls sein, ist eine Kopie der Einheit problemlos möglich. Es wird einfach der gesamte ROM und die Schaltungstruktur kopiert.

Weiterhin ist ein Verfahren nach der Druckschrift EP 0449256A2 bekannt, in welchem Programme 5 und Daten verschlüsselt in einem Speicher abgelegt werden und bei Bedarf durch einen im zweiten Speicher 7 abgelegten Schlüssel mit Hilfe einer Ver- und Entschlüsselungseinrichtung wieder decodiert werden. Die Entschlüsselungseinheit befindet sich zwischen der CPU und dem Datenbus und der CPU. Die Entschlüsselungseinheit besteht aus AND und OR Gattern, die bei einem Zugriff auf den Daten- und Programmspeicher mit Hilfe des Schlüssels aus dem Schlüsselspeicher die notwendigen Daten in Echtzeit entschlüsseln und der CPU zuführen. Der Entschlüsselungsalgorithmus ist durch die Hardwarestruktur der Entschlüsselungseinheit vorgegeben. Der benötigte Schlüssel für die Programme befindet sich ebenfalls im Speicher 5 und wird beim Start des Systems in den Speicher 7 übertragen.

This Sheet Has Been Replaced





Der Nachteil des Verfahrens besteht darin, daß ein solcher Microcontroller mit externen Speichern jederzeit beliebig dubliziert werden kann und kein Schutz gegenüber dem Produzenten von solchen Microcontrollerbaugruppen existiert. Zusätzlich zu einem Standardmicrocontroller wird eine Codier- und Decodiereinheit benötigt. Gegenüber dieser Decodiereinheit besteht die Anforderung, die benötigten Befehle mit Hilfe des Schlüssels, der im Speicher 7 abgelegt ist, in Echtzeit zu entschlüsseln. Dies bedeutet, daß der Entschlüsselungsalgorithmus nicht zu kompliziert sein darf, weil sonst die benötigte Zeit zum Entschlüsseln der Befehle zu hoch wird und so die Leistung des Microcontrollers ausgebremst werden könnte. Desweiteren wächst mit der Komplexität des benötigten Entschlüsselungsaufwandes auch die benötigte Chipfläche an. Ein wesentlicher Nachteil besteht ebenfalls darin, daß der Schlüssel für den Programmspeicher 5 innerhalb des Programmspeichers abgelegt wird. Ein Hersteller der Microcontrollerbaugruppe ist somit in die Lage versetzt, das verschlüsselte Programmmodul zu entschlüsseln und Zugriff auf das mögliche Know-how des Auftraggebers zu erhalten.

Weitere Schriften beziehen sich lediglich auf die verschiedenen Methoden zum Schutz von internen ROM-Inhalten vor unberechtigttem Auslesen, wie in der Druckschrift nach EP 468535A2 dargestellt. Hier wird ein Verfahren vorgestellt, indem ein interner ROM 4 und ein Ein- und Ausgabeports 5 und 6 mit einer CPU über einen Bus verbunden ist und der Inhalt des ROM's erst dann über den Ausgabeport ausgegeben wird, nachdem über den Eingabeport Teile oder der ganze Inhalt des internen ROM's eingegeben wurde. Diese Verfahren sind nur im weitesten Sinne der erfinderischen Lösung zuzuordnen.

Durch die Lösung nach der Druckschrift EP 536 943 A2 ist eine Datensicherungsanordnung bekannt, bei welcher in einem im Bezug auf eine programmierbare logische Einheit (11), extern angeordneten ROM (24), die Daten nicht nur verschlüsselt- und damit gesichert gegen ein Raubkopieren- sind, sondern auch der externe ROM Speicher der logischen Einheit unvertauschbar fest zugeordnet ist.



Der Nachteil dieser Lösung besteht darin, daß bei der Produktion der Datensicherungsanordnung keine Sicherheit gegenüber dem Produzenten der Einheit gewährt wird. Damit kann der Produzent der Datensicherungseinheit beliebig viele Kopien mit einer beliebigen Serialisierung des Systems erstellen, ohne
5 daß der Auftraggeber darüber Kenntnis erlangen kann. Die Sicherheit des Systems kann damit auch schon durch Mitarbeiter des Produzenten oder der eigenen Firma untergraben werden.

Desweiteren können keine beliebig großen Programme in variabler Größe aus dem externen Speicher nachgeladen werden. Der externe Speicher kann nur so groß
10 gewählt werden, wie der intern zur Verfügung stehende SRAM abbilden kann. Damit ist eine Einschränkung der Nutzung, besonders im hochvariablen Microcontrollerbereich von vornherein gegeben.

Mit der Weiterentwicklung der Rechentechnik und der Kryptologie müssen besonders bei sicherheitsrelevanten Systemen, die zum Zahlungsverkehr oder zur
15 Identifikation von Personen genutzt werden sollen, hochwertige Verschlüsselungsalgorithmen eingesetzt werden. Ein Einsatz eines komplexen Verschlüsselungssystems würde in diese Lösung den Kostenrahmen und die Komplexität des Systems sprengen.

Desweiteren bedarf die Austauschbarkeit des Entschlüsselungsalgorithmus in dieser Lösung einer kostenintensiven Hardwareänderung. Mit der fortschreitenden
20 Entwicklung der Rechentechnik und der Mathematik können besonders Verschlüsselungsalgorithmen, die heute noch als sicher galten, morgen schon durch einfache PC-Programme entschlüsselt werden. Damit muß auch der Algorithmus der Entwicklung der Mathematik (Kryptologie) und der Rechentechnik Schritt
25 halten. Eine Variabilisierung der Algorithmen muß damit eine Voraussetzung für einen längeren Einsatz eines preiswerten Moduls sein.

Die Serialisierung der einzelnen Datensicherheitseinrichtungen nach dieser Druckschrift ist nicht unfälschbar möglich. Da die Seriennummern nur im Klartext

oder über das Keyword an die Datensicherheitseinrichtung nach übertragen werden können. Damit kann der Produzent der Einrichtung beliebig viele Datensicherungseinrichtungen mit weiteren Seriennummern produzieren, ohne daß der entsprechende Know-How-Träger davon Kenntnis erhält. Die Sicherheit der
5 Produktion von elektronischen Bauelementen dieser Art ist besonders bedeutungsvoll, da solche Elemente, meist aus Kostengründen, in Billiglohnländern außerhalb der Know-How tragenden Firmen produziert werden, aber gleichzeitig solche Systeme im Zahlungsverkehr- und Identifikationsystem eingesetzt werden sollen. Damit ist die Versuchung, weitere Module oder Kopien und Plagiate
10 herzustellen sehr groß. Viele der Videoverschlüsselungsverfahren z. B. wurden unter anderem geknackt oder kopiert, weil es in der Produktion der einzelnen Einheiten „Informationslücken“ in den produzierenden Unternehmen gab, die als Quelle für Fälscher und Plagiathersteller dienten.

Um die oben genannten Nachteile des Standes der Technik, zur Verhinderung des
15 unberechtigten Kopierens und Vervielfältigens von Microcontrollermodulen mit externen Speichern und zur Verhinderung der Auslesung und Duplizierung von externen Microcontrollerspeichern und zur Befehls- und Informationsergänzung für Microcontroller, insbesondere durch einen beauftragten Hersteller solcher Module, abzustellen, ist es Aufgabe der Erfindung, ein Verfahren zu schaffen, das
20 in Kombination mit einer einfachen Schaltungsanordnung, unter herkömmlichen Bestückungsbedingungen beliebig viele selektiv identifizierbare Microcontrollergruppen entstehen, die für nicht autorisierte Personen nicht nachbaubar oder deren Inhalt nicht auslesbar oder duplizierbar sind; und daß der Produzent von solchen Microcontrollereinheiten ebenfalls keine Microcontroller selbst
25 produzieren oder nachbauen kann.

Erfindungsgemäß wird die Aufgabe durch die im Patentanspruch 1 angegebenen Merkmale gelöst. Bevorzugte Weiterbildungen der Erfindung ergeben sich aus den Unteransprüchen.

This Sheet Has Been Replaced



Die Vorteile der Erfindung bestehen darin, daß eine einheitliche Microcontrollerbaugruppe (Modul) standardmäßig hergestellt werden kann und daß beliebige Programme in variabler Größe aus dem externen Speicher nachgeladen werden können, wobei das externe Programm weder für den
5 Produzenten der Baugruppe noch für Dritte auslesbar oder analysierbar ist. Dieses Verfahren benötigt keine spezielle hardwaremäßige Entschlüsselungseinheit und damit kann der Entschlüsselungsalgorithmus mit geringem Aufwand getauscht werden. Dadurch, daß die Entschlüsselung des externen ROM's nicht in Echtzeit vorgenommen werden muß, können auch sehr anspruchsvolle
10 Verschlüsselungsverfahren in das System implementiert werden. Die Produktion solch eines Microcontrollermoduls ist ohne besondere Sicherheitsmaßnahmen möglich. Desweiteren erlaubt das Verfahren eine Nachladbarkeit von fehlenden Befehlen in den eigentlichen Microcontroller und es ist ausschließbar, daß der Produzent mehr Microcontroller herstellen oder nachmachen kann, als ihm in Auftrag gegeben wurden.
15

Die Erfindung wird nachstehend an Figur 1 - Figur 3 erläutert.

Die Erfindung soll anhand eines Anwendungsbeispiels für einen Verschlüsselungs-Microcontroller erläutert werden. Prinzipiell kann dieses Verfahren jedoch für jede beliebige andere Anwendung , z. B. bei Kreditkarten oder Telefonkarten
20 angewandt werden.

Das in Figur 1 dargestellte Microcontrollermodul 1, besteht aus einem Microcontroller 2, in dem eine -interne CPU- 3 über einen -internen Bus- 4 mit einem -internen ROM- 5, einem -internen RAM- 6, einem Selektionsmodul 7, einem -ROM Schnittstellenmodul- 8 und einem Interface 9 verbunden ist und aus
25 einem -internen Programmiersignal- 10, einem -externen Programmiersignal- 11 und einem -externen Speicher (PROM)- 12, der mit einem -externem Bus- 13 über das -ROM Schnittstellenmodul- 8 mit dem Microcontroller 2 verbunden ist.



Beim Start des Microcontrollermoduls 1, lädt der Microcontroller 2 den Inhalt des -externen Speichers (PROM)- 12 in den -internen RAM- 6. In diesem -internen RAM- 6, auf den nur durch die -interne CPU- 3 zugegriffen werden kann, wird der Inhalt des -internen RAM- 6 mit Hilfe des Selektionsmoduls 7, dessen Inhalt als Schlüssel dienen kann und mit Hilfe der eingelesenen Daten aus dem -externen Speicher (PROM)- 12, die auch als Schlüssel dienen können, unter Verwendung eines Entschlüsselungsalgorithmus, der im -internen ROM- 5 steht, zu Programmcode und Daten entschlüsselt. Dabei kann das Programm im -internen ROM- 5 auch weitere Programmteile, wie Selbsttestroutinen oder Routinen zum blockweisen Einlesen des -externen Speichers (PROM)- 12, beinhalten. Nachdem das Programm oder die gerade benötigten Programmteile aus dem -externem Speicher (PROM)- 12 von der spezifisch verschlüsselten Form, in eine einheitliche abarbeitbare Form gebracht wurden, führt die -interne CPU- 3 die Befehle, die im -internen RAM- 6 stehen, aus. Das Interface 9 kann beliebige Kommunikationsteile eines standardmäßigen Microcontrollers beinhalten, beispielsweise PIO, SIO oder sogar externe Bus-ähnliche Architekturen aufweisen. Über dieses Interface 9 kann der Microcontroller 2 mit anderen Einheiten, die zur Erledigung der gestellten Aufgabe erforderlich sind, kommunizieren. Das Selektionsmodul 7 dient lediglich zur Ablage eines microcontrollerpezifischen internen Schlüssels, mit dessen Hilfe der -externe Speicher (PROM)- 12 entschlüsselt werden kann. Dadurch, daß jedes Selektionsmodul 7 einen anderen zufälligen Schlüssel beinhalten kann, können die -externen Speicher (PROM)- 12 auch nicht ausgetauscht werden, trotz daß der unverschlüsselte Originalinhalt des -externen Speichers (PROM)- 12 gleich sein kann. Damit kann kein Microcontrollermodul 1 unberechtigt durch einen unbefugten Hersteller kopiert werden, indem er einen ihm bekannten -externen Speicher (PROM)- 12 nimmt und den Mikrocontroller 2 kauft, um damit gleiche Microcontrollermodule 1 herzustellen. Er kann nicht wissen, welchen Wert das Selektionsmodul 7 hat. Das Selektionsmodul 7, kann als eine lange PROM-Zelle -ausgeführt werden, deren Wert von der -internen CPU- 3 einmal programmiert werden kann, und danach nur gelesen werden kann, oder es kann auch ein unscharfer Rauschgenerator sein, der beim Anschalten immer den gleichen Wert liefert, aber wegen der geringen Toleranzgrenze pro Schaltkreis statistisch immer



einen anderen Wert hat. Dabei kann es sich auch um einen Bereich handeln, der bestrahlt wurde und so durch Strukturveränderungen verschiedene Speicherzustände entstanden sind, oder um einen Bereich handeln, in dem verschiedene Bondinseln vorhanden sind, die beim Bonden des Schaltkreises verschieden gebondet wurden. Das Feld der Erzeugung von internen Nummern ist hier sehr
5 weit, so daß nur einige Beispiele aufgezeigt werden konnten.

Das interne und externe Programmiersignal 10, 11 dient zur einmaligen Programmierung des -externen Speichers (PROM)- 12, mit Hilfe des -ROM Schnittstellenmoduls- 8 über den -externen BUS- 13, durch den Microcontroller 2.
10 Dieser Vorgang wird nachfolgend durch Figur 2 und Figur 3 erläutert.

Der in Figur 2 dargestellte Ablaufplan, bestehend aus einer -primären ROM Inhaltsdatei- 14, zusammengesetzt aus einem -externen ROM Programmcode- 15, aus einem -externen Variabelteil- 16 und einem -externen Seriennummerenteil- 17, sowie aus einem dem Know-how Träger bekannten, Verschlüsselungsalgorithmus-
15 18, einem -anwenderspezifisch bekannten Produktionsschlüssel- 19 und einer erzeugten Produktionsdatei 20.

Die Funktion ist dadurch charakterisiert, daß der Know-How Träger den Inhalt der -primären ROM Inhaltsdatei- 14 erstellt. Diese Datei soll dann in den -externen ROM Programmcode- 15 übertragen werden. Der Inhalt der Datei kann beliebig
20 gestaltet werden. In diesem Ausführungsbeispiel, welches keinen allgemeinen Charakter haben soll, sondern nur diesem speziellen Anwendungsfall gerecht wird, besteht die -primäre ROM Inhaltsdatei- 14, aus dem -externen ROM Programmcode- 15, der es auch erlaubt, ganze Programmteile des Microcontrollers 2 nach der Produktion dieses Microcontrollers zu ergänzen oder zu modifizieren und
25 aus dem -externen Variabelteil- 16, dieser dient zur teilweisen Serialisierung der Microcontroller 2, so daß am Microcontroller 2 die Nummer des Systems abgefragt werden kann, und so sicher gestellt werden kann, das kein Microcontroller 2 zweimal hergestellt wurde, also die Einzigartigkeit jedes Microcontrollermoduls 1 gewährleistet werden kann, ohne daß der Produzent

selbst Microcontroller herstellen kann. In den -externen Variblen- 16 können z. B. spezifische personengebundene Daten oder spezifische Schlüsselerzeugungsalgorithmen für den Verschlüsselungsmicrocontroller abgelegt werden. Dieser Bereich kann auch zur Ablage einer wachsenden Seriennummer benutzt werden, die durch einen Microcontrollerbefehl extern abfragbar ist, darüber können auch Vertriebs- oder Produktionskontrollsysteme eingeführt werden. Eine Zuordnung der Microcontrollermodule 1 zu Personen wird durch diese Selektion möglich.

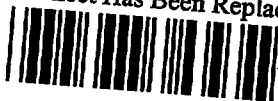
Nachdem der Know-how-Träger den Inhalt der -primären ROM Inhaltsdatei- 15 festgelegt hat, verschlüsselt er, mit dem ihm bekannten Verschlüsselungsalgorithmus 18 die -primäre ROM Inhaltsdatei- 15 mit dem ihm bekannten Schlüssel 19. So entsteht die Produktionsdatei 20. Der -Know-how Träger bekannte Verschlüsselungsalgorithmus- 18 kann dem Know-how Träger in Form eines Programmes beispielsweise auf einem PC zur Verfügung gestellt werden. Auch wenn der gleiche Umschlüsselungsalgorithmus 21 im Microcontroller 2 vorhanden ist, können dennoch mehrere Anwender (Know-how Träger) für den selben Microcontroller 2 -primäre ROM Inhaltsdateien- 14 erstellen, ohne daß es zu einem Know-how Verlust kommen kann, da der -anwenderspezifisch bekannter Produktionsschlüssel- 19 für jeden Anwender anders gewählt werden kann.

Die so erhaltene Produktionsdatei 20 wird nun bei der Herstellung der Microcontrollerbaugruppe, nach dem normalen Bestückungsprozeß, nach dem Anlegen der Speicherprogramierspannung über das Interface 9 an den Microcontroller 2 übertragen.

Der in Figur 3 dargestellte interne Ablaufplan, besteht aus dem Microcontrollermodul 1, dem Microcontroller 2, dem Selektionsmodul 7, dem Interface 9, dem -externen Programmiersignal- 11, dem -externen Speicher- 12, dem -anwenderspezifisch bekannten Produktionsschlüssel- 19, der -erzeugten Produktionsdatei- 20 und dem Umschlüsselungsalgorithmus 21.

Wenn der Produktionsprozeß der reinen physischen Produktion (Bestückung, Lötung usw.) beendet ist, wird die Microcontrollerbaugruppe über das Interface 9 kontaktiert und das -externe Programmiersignal- 11 wird an den -externen Speicher (PROM)- 12 angelegt. Wenn es notwendig ist, wird auch das -interne Programmiersignal- 10 angelegt. Nach diesem Kontaktieren wird nun der -anwenderspezifische bekannte Produktionsschlüssel- 19 dem Microcontroller 2 über das Interface 9 übertragen. Nach dieser Übertragung wird die Produktionsdatei 20 an den Microcontroller 2 übertragen. In dem Microcontroller 2 wird nun mit Hilfe des -anwenderspezifisch bekannten Produktionsschlüssels- 19 und der Produktionsdatei 20 unter Zuhilfenahme des Umschlüsselungsalgorithmus 21 die -primäre ROM Inhaltsdatei- 14 entschlüsselt. Nach dieser Entschlüsselung, kann je nach Anwendungsfall der Inhalt des Selektionsmoduls 7 mit einem Wert aus der entschlüsselten Produktionsdatei 20 aufgefüllt werden, welcher später als interner Schlüssel dient. Es kann aber auch nur ein Wert aus der entschlüsselten Produktionsdatei 20 zum Umschlüsseln durch den Umschlüsselungsalgorithmus 21 benutzt werden. Der Umschlüsselungsalgorithmus verschlüsselt die entschlüsselte im -internen RAM- 6 vorliegende Produktionsdatei 20 mit dem ausgewählten internen Schlüssel aus der Produktionsdatei 20 oder aus dem Selektionsmodul 7 oder aus der Kombination von beiden. Diese so erneut verschlüsselten Daten werden nun mit Hilfe des -ROM Schnittstellenmoduls- 8 in den -externen Speicher (PROM)- 12 eingebrannt. Damit ist ein spezifisch verschlüsselter -externer Speicher (PROM)- 12 erzeugt worden, dessen Verschlüsselung nicht einmal dem Know-how Träger oder seinen Mitarbeitern bekannt sein muß. Es ist auch nicht unbedingt notwendig, daß der Schlüssel (Bpw. der Inhalt des Selektionsmoduls 7) bekannt sein muß. Damit ist eine sehr hohe Sicherheit erreicht worden und der Hersteller der Microcontrollermoduls 1 kann keine eignen Microcontroller 2 illegal herstellen.

This Sheet Has Been Replaced



Verwendete Bezugszeichen

	1	Microcontrollermodul
	2	Microcontroller
	3	- interne CPU -
5	4	- interner Bus -
	5	- interner ROM -
	6	- interner RAM -
	7	Selektionsmodul
	8	- ROM Schnittstellenmodul -
10	9	Interface
	10	-internes Programmiersignal-
	11	- externes Programmiersignal -
	12	- externer Speicher (PROM) -
	13	- externer Bus -
15	14	- primäre ROM Inhaltsdatei -
	15	- externer ROM Programmcode -
	16	- externer Variabelteil -
	17	- externer Seriennummernteil -
	18	- Know-how Träger bekannter Verschlüsselungsalgorithmus -
20	19	- anwenderspezifisch bekannter Produktionsschlüssel -
	20	Produktionsdatei
	21	Umschlüsselungsalgorithmus

This Sheet Has Been Replaced





Patentansprüche

1. Microcontrollersicherungsverfahren, nach dem ein Auslesen des externen Microcontrollerprogramms und das Duplizieren der Microcontrollerbaugruppen ausgeschlossen ist, dadurch gekennzeichnet, daß serialisierte Microcontroller (2)
- 5 hergestellt werden, die von Dritten nicht kopierbar sind und die Vergabe von weiteren Seriennummern, auch besonders vom Hersteller eines Microcontrollermoduls (1) verhindert und das sehr anspruchsvolle Verschlüsselungsverfahren in das System implementiert, wobei beliebige Programme in variabler Größe aus einem externen Speicher PROM (12)
- 10 nachgeladen werden können und daß mit geringem Aufwand Entschlüsselungsalgorithmen ausgetauscht werden können, indem eine -primäre ROM Inhaltsdatei- (14), bestehend aus einem -externen Variabelteil- (16) und einem -externen Seriennummernteil- (17) und eine Produktionsdatei (20) für die Produktion der Microcontrollerbaugruppe nacheinander von einem Know-how
- 15 Träger erstellt wird, wobei die Produktionsdatei (20) an einen Microcontroller (2), der aus einer -internen CPU- (3), einem -internen Bus- (4), einem -internen ROM- (5), einem -internen RAM- (6), einem Selektionsmodul- (7), einem -ROM Schnittstellenmodul (8), einem Interface (9) und einem -internen Programmiersignal (10) besteht, übertragen wird, gleichzeitig wird an den
- 20 Microcontroller (2) über das Interface (9) ein -anwenderspezifisch bekannter Produktionsschlüssel- (19) gesendet und aus der Produktionsdatei (20) wird mit Hilfe eines Umschlüsselungsalgorithmus 21 unter Benutzung des -anwenderspezifisch bekannten Produktionsschlüssels- (19) eine -primäre ROM Inhaltsdatei- (14) erzeugt und aus Teilen der -primären ROM Inhaltsdatei- (14) oder aus dem
- 25 Inhalt des Selektionsmoduls (7) oder aus den Kombinationen des Selektionsmodules (7) und der -primären ROM Inhaltsdatei- (14) wird ein verschlüsselter Datenstrom, der über das -ROM Schnittstellenmodul- (8) einmalig oder wahlweise mehrfach, je nach Ausführung des -externen Speichers (PROM)- (12) mit Hilfe eines -externen Programmiersignals- (11) und des -internen
- 30 Programmiersignals- (10) zum -externen Speicher (PROM)- (12) übertragen, dadurch ist gewährleistet, daß der -externe Speicher (PROM)- (12) nach jedem

Prozeß für jedes Microcontrollermodul (1) einzigartig ausgeführt ist, somit ist ein Duplizieren des Microcontrollermoduls (1) ausgeschlossen und externe Programme sind weder für Produzenten der Baugruppe noch für Dritte auslesbar oder analysierbar.

- 5 2. Microcontrollersicherungsverfahren nach Anspruch 1., dadurch gekennzeichnet, daß das Selektionsmodul (7) als EPROM-Zelle ausgeführt werden kann, oder es kann auch ein unscharfer Rauschgenerator sein, der beim Anschalten immer den gleichen Wert liefert und bei anderen Schaltkreisen durch die engen Toleranzbedingungen Streuwerte liefert, wobei es sich um einen Bereich handelt,
10 der bestrahlt wurde und so durch Strukturveränderungen verschiedene Speicherzustände entstanden sind, oder um einen Bereich, in dem verschiedene Bondinseln vorhanden sind, die beim Bonden des Schaltkreises verschieden gebondet sind.
3. Microcontrollersicherungsverfahren nach Anspruch 1 und Anspruch 2., dadurch gekennzeichnet, daß der Umschlüsselungsalgorithmus (21) aus
15 unterschiedlichen Teilalgorithmen bestehen kann.
4. Microcontrollersicherungsverfahren nach Anspruch 1 bis Anspruch 3., dadurch gekennzeichnet, daß der Inhalt des Selektionsmoduls (7) weder dem Hersteller noch dem Know-how Träger bekannt ist.



This Sheet Has Been Replaced

