(19) Deutsches Patent- und Markenamt

(10) **DE 10 2014 208 851 A1** 2015.11.12

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2014 208 851.8**
(22) Anmeldetag: **12.05.2014**
(43) Offenlegungstag: **12.11.2015**

(51) Int Cl.: ***G06F 21/12*** (2013.01)
G06F 21/60 (2013.01)

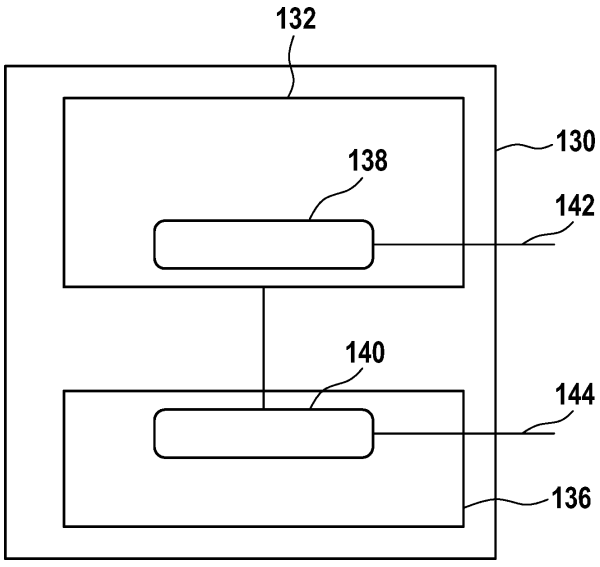
(71) Anmelder:
Robert Bosch GmbH, 70469 Stuttgart, DE

(72) Erfinder:
Egeler, Holger, 75392 Deckenpfronn, DE; Ihle, Markus, 71282 Hemmingen, DE; Opferkuch, Ingo, 71254 Ditzingen, DE; Schwepp, Thorsten, 71404 Korb, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Verfahren zum Verhindern eines unbefugten Betriebs eines Kraftfahrzeugs**

(57) Zusammenfassung: Es werden ein Verfahren zum Verhindern eines unbefugten Betriebs eines Kraftfahrzeugs und ein elektronisches Hardware-Sicherheitsmodul (132) zur Durchführung des Verfahrens vorgestellt. Hierin wird eine Wegfahrsperren-Software (138, 140) verwendet, die zumindest teilweise in dem elektronischen Hardware-Sicherheitsmodul (132) abgelegt ist.



Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zum Verhindern eines unbefugten Betriebs eines Kraftfahrzeugs, ein elektronisches Hardware-Sicherheitsmodul zur Durchführung des Verfahrens und ein Steuergerät mit einem solchen elektronischen Hardware-Sicherheitsmodul. Das elektronische Hardware-Sicherheitsmodul wird in einem Steuergerät eines Kraftfahrzeugs eingesetzt.

Stand der Technik

[0002] Steuergeräte sind elektronische Module, die bspw. in Kraftfahrzeugen eingesetzt werden, um Abläufe zu steuern und zu regeln. Hierzu sind die Steuergeräte Komponenten des Kraftfahrzeugs zugeordnet, deren Betrieb mit dem zugeordneten Steuergerät kontrolliert wird. Hierzu liest das Steuergerät von Sensoren erfasste Daten ein und wirkt durch die Ansteuerung von Aktoren auf den Betrieb ein.

[0003] Das beschriebene Verfahren kommt in Verbindung mit einem elektronischen Sicherheitsmodul zur Anwendung, das in einem Steuergerät, insbesondere im Automotive-Bereich, in sicherheitsrelevanten Bereichen eingesetzt wird. Bei den meisten Anwendungen in den sicherheitsrelevanten Bereichen ist das unmanipulierbare oder nicht einsehbare Speichern von Daten eine wesentliche Anforderung. Hierbei werden kryptographische Schlüssel eingesetzt, die in symmetrischen oder asymmetrischen Verschlüsselungsverfahren zur Anwendung kommen.

[0004] Die verwendeten Schlüssel und Verschlüsselungsverfahren stellen Geheimnisse dar, die vor Angreifern geheim gehalten werden müssen. Andere Anwendungen in sicherheitsrelevanten Bereichen betreffen bspw. den Schutz vor unerlaubten Veränderung, bspw. das Speichern von geänderten Seriennummern oder Kilometerständen, das Unterbinden von nicht genehmigten Tuning-Maßnahmen usw.

[0005] Daher ist es erforderlich, in Steuergeräten sichere Umgebungen bereitzustellen, in denen Funktionen ausgeführt werden können, die diese Geheimnisse einsehen und/oder verändern müssen. Diese Umgebungen weisen regelmäßig eine sichere Recheneinheit bzw. CPU, die auch als secure CPU bezeichnet wird, sowie ein Speichermodul auf. Eine solche Umgebung wird hierin als Hardware-Sicherheitsmodul (HSM: Hardware Security Module) bezeichnet. Dieses stellt ein leistungsfähiges Modul mit Hardware- und Software-Komponenten dar, welches den Schutz und die Vertrauenswürdigkeit von eingebetteten Systemen verbessert. Insbesondere unterstützt das HSM dabei, sicherheitskritische Anwendungen und Daten zu schützen. Mit einem HSM können ebenfalls die Sicherheitskosten reduziert werden, während zugleich ein wirksamer Schutz vor Angreifern geboten werden kann. Bezüglich des grundlegenden Aufbaus eines HSM wird auf **Fig.** 3 verwiesen.

[0006] Als Wegfahrsperren werden Einrichtungen in Kraftfahrzeugen benannt, die einen unbefugten Betrieb des Kraftfahrzeugs verhindern sollen. Dabei sind reine Hardware- und Software-Lösungen sowie kombinierte Hard-Software-Lösungen bekannt. Die Wegfahrsperren-Software ist bei bekannten Wegfahrsperren Teil der Steuergeräte-Software und besitzt damit das Sicherheitslevel der übrigen Steuergeräte-Software.

Offenbarung der Erfindung

[0007] Vor diesem Hintergrund werden ein Verfahren nach Anspruch 1, ein elektronisches Hardware-Sicherheitsmodul mit den Merkmalen des Anspruchs 5 sowie ein Steuergerät gemäß Anspruch 9 vorgestellt. Ausgestaltungen des Verfahrens und des Moduls gehen aus den abhängigen Ansprüchen und der Beschreibung hervor.

[0008] Das vorgestellte Verfahren und das beschriebene elektronische Hardware-Sicherheitsmodul ermöglichen es, den Sicherheitslevel der Wegfahrsperren-Software zu erhöhen.

[0009] Hierzu wird die Wegfahrsperren-Software oder zumindest Teile davon in das Hardware-Sicherheitsmodul (HSM: Hardware Security Modul) verlagert. Abschaltschnittstellen können zusätzlich über die HSM-exklusiven Anschlüsse bzw. Port-Pins abgesichert werden. Das bedeutet, dass die Abschaltung über die Anschlüsse des HSM gesteuert wird. Die Wegfahrsperren-Software erhält auf diese Weise den erhöhten Sicherheitslevel des HSM.

[0010] Zu beachten ist, dass die Wegfahrsperren-Software als Teil der Steuergeräte-Software ihre Gegenstelle über ein Frage-Antwort-Verfahren bzw. Challenge/Response-Verfahren authentisiert. Für die kryptographischen Berechnungen wird das Hardware Security Modul genutzt. Die Wegfahrsperren-Software im HSM prüft dabei in Ausgestaltung die Authentisierung bzw. führt die Authentisierung durch und steuert die HSM-exklusiven Abschaltschnittstellen.

[0011] In einer Ausführung bleibt ein Teil der Wegfahrsperren-Software in der Steuergeräte-Software und kann bspw. zusätzliche Abschaltschnittstellen ansteuern.

[0012] In einer weiteren Ausführung fungiert die HSM-Abschaltschnittstelle als Master. Die eventuell zusätzlich vorhandenen Abschaltschnittstellen soll-

ten gegen die Master-Abschaltschnittstelle des HSM plausibilisiert werden.

[0013] Eine mögliche Ausbaustufe besteht in der hardwaremäßigen Verknüpfung der beschriebenen Abschaltschnittstellen.

[0014] Weitere Vorteile und Ausgestaltungen der Erfindung ergeben sich aus der Beschreibung und den beiliegenden Zeichnungen.

[0015] Es versteht sich, dass die voranstehend genannten und die nachstehend noch zu erläuternden Merkmale nicht nur in der jeweils angegebenen Kombination, sondern auch in anderen Kombinationen oder in Alleinstellung verwendbar sind, ohne den Rahmen der vorliegenden Erfindung zu verlassen.

Kurze Beschreibung der Zeichnungen

[0016] **Fig.** 1 zeigt eine Vertrauenspyramide.

[0017] **Fig.** 2 zeigt in einer schematischen Darstellung Funktionen eines HSM.

[0018] **Fig.** 3 zeigt in einer schematischen Darstellung den Aufbau einer Ausführung des HSM.

[0019] **Fig.** 4 zeigt ein Steuergerät nach dem Stand der Technik.

[0020] **Fig.** 5 zeigt eine Ausführung des beschriebenen Steuergeräts.

Ausführungsformen der Erfindung

[0021] Die Erfindung ist anhand von Ausführungsformen in den Zeichnungen schematisch dargestellt und wird nachfolgend unter Bezugnahme auf die Zeichnungen ausführlich beschrieben.

[0022] Um einem IT-System dahingegen zu vertrauen, dass es immer so agiert, wie dies erwartet ist, erfordert es, aufeinanderfolgend allen Schichten zu vertrauen, die eingebunden sind, um ein vertrauenswürdiges IT-System zu erzeugen.

[0023] **Fig.** 1 zeigt eine Pyramide des Vertrauens, die als Trust Pyramid bezeichnet wird, für ein typisches IT-System. Diese ist insgesamt mit der Bezugsziffer **10** bezeichnet und umfasst eine Schicht für eine organisatorische Sicherheit **12**, eine Schicht für eine Systemsicherheit **14**, eine Schicht für eine Hardware-Sicherheit **16**, eine Schicht für eine Software-Sicherheit **18** und eine oberste Schicht für Vertrauen **20** bzw. Trust.

[0024] Um dem gesamten IT-System vertrauen zu können, ist es erforderlich, dass jede Schicht auf die wirksame Sicherheit der darunterliegenden Schicht vertrauen kann, ohne in der Lage zu sein, dies direkt zu verifizieren. Dies bedeutet bspw., dass sich eine perfekte Software- und Hardware-Sicherheitslösung durch eine schwache darunterliegende Sicherheitssystemgestaltung als nutzlos erweisen kann. Darüber hinaus kann gegeben sein, dass eine mögliche Schwäche in der Systemgestaltung nicht erfasst oder durch die oberen Hard- und Software-Schichten verhindert wird.

[0025] Im Gegensatz zu typischen Back- und IT-Systemen ist die Hardware-Schicht von eingebetteten Systemen oftmals physischen Angriffen ausgesetzt, die Hardware- oder Software-Funktionen durch physische Mittel beeinflussen, bspw. einen Flash-Speicher manipulieren oder Alarmfunktionen deaktivieren. Ein Ansatz, solche physischen Attacken zu erschweren, besteht darin, insbesondere manipuliergeschützte Hardware-Sicherheitsmodule (HSM) einzusetzen, wie diese bspw. in **Fig.** 2 gezeigt sind. Ein solches HSM schützt wichtige Informationen, bspw. Personen-Identifikationsnummern (PIN), sichere Schlüssel und kritische Operationen, bspw. eine PIN-Verifikation, eine Datenverschlüsselung, bspw. durch starke physische Abschirmung.

[0026] Wie ein HSM ausgebildet sein kann und was für Funktionen von diesem durchgeführt werden können, um die Sicherheit eines eingebetteten Systems zu verbessern, wird im Folgenden dargestellt.

[0027] **Fig.** 2 zeigt die Kernfunktionen eines typischen Hardware-Sicherheitsmoduls. Die Darstellung zeigt eine Software-Schicht **30** und eine Hardware-Schicht **32**, die vor unberechtigten Zugriffen geschützt ist.

[0028] Die Software-Schicht **30** umfasst eine Reihe von Anwendungen **34**, von denen hier drei dargestellt sind. Weiterhin ist ein Betriebssystem **36** vorgesehen. Die Hardware-Schicht **32** umfasst eingebettete Standard-Hardware **38** und ein Hardware-Sicherheitsmodul (HSM) **40**. In diesem HSM **40** ist ein erster Block **42** für Schnittstellen und Steuerung, ein zweiter Block **44** für sichere Verschlüsselungsfunktionen, ein dritter Block **46** für sichere Funktionen und ein sicherer Speicher **48** vorgesehen.

[0029] Der sichere Speicher **48** ist ein kleiner, nicht flüchtiger Datenspeicher, bspw. mit einer Kapazität von einigen kB, innerhalb des manipuliergeschützten HSM **40**, um ein nichtautorisiertes Auslesen, eine Manipulation oder ein Löschen von kritischen Informationen, wie bspw. von kryptographischen Schlüsseln, kryptographischen Zertifikaten oder Authentifizierungsdaten, bspw. PINs oder Passwörter zu verhindern. Der sichere Speicher **48** des HSM **40** enthält weiterhin alle HSM-Konfigurationsinformationen, bspw. Informationen zum Eigentümer des HSM **40**

oder Zugriffautorisierungen zu gesicherten internen Einheiten.

[0030] Im zweiten Block **44** für sichere Verschlüsselungsfunktionen sind kryptographische Algorithmen, die für eine Datenverschlüsselung und -entschlüsselung verwendet werden, bspw. AES oder 3DES, eine Datenintegritätsverstärkung, bspw. MAC oder HMAC, oder eine Datenursprungsverifikation, bspw. durch Verwenden von digitalen Signatur-Algorithmen, wie bspw. RSA oder ECC, und alle zugehörigen kryptographischen Aktivitäten, wie bspw. Schlüsselerzeugung, Schlüsselverifikation, enthalten.

[0031] Sichere Funktionen im dritten Block **46** umfassen alle geschützten Funktionen, die nicht direkt einem kryptographischen Verfahren zugeordnet sind, wobei das HSM **40** als physisch geschützter "Trust Anchor" dient. Dies kann bspw. ein physisch geschütztes Taktsignal, ein interner Zufallszahlengenerator, ein Ladeprogramm-Schutzmechanismus oder irgendeine kritische Anwendungsfunktion sein, bspw. um einen sicheren Dongle zu realisieren.

[0032] Der erste Block **42** für Schnittstellen und Steuerung umfasst die interne HSM-Logik, welche die HSM-Kommunikation mit der Außenwelt implementiert und die den Betrieb aller internen Basiskomponenten, wie diese vorstehend erwähnt sind, verwaltet.

[0033] Alle funktionalen Basiskomponenten des Hardware-Sicherheitsmoduls **40**, wie dies vorstehend beschrieben ist, sind von einer kontinuierlichen physischen Grenze umgeben, was verhindert, dass interne Daten und Prozesse abgehört, kopiert bzw. nachgebildet oder manipuliert werden können. Dies könnte dazu führen, dass ein nichtautorisierter Nutzer interne Geheimnisse verwenden oder kompromittieren kann. Die kryptographische Grenze wird üblicherweise mit algorithmischen und physischen Zeitkanal-Gegenmaßnahmen mit dedizierten Zugriffsschutzmitteln implementiert, bspw. eine spezielle Abschirmung oder Beschichtungen, um einen Seitenkanalwiderstand, einen Zugriffshinweis, einen Zugriffswiderstand oder eine Zugriffsantwort zu ermöglichen.

[0034] Wie das HSM **40** die Sicherheit einer eingebetteten Produktlösung verbessern kann, wird nachstehend dargelegt:
Das HSM **40** schützt kritische Informationen, bspw. Identitäten, Signierschlüssel oder Schlüssel, durch die physische Abschirmung, die nicht durch eine Software-Anfälligkeit umgangen werden kann.

[0035] Das HSM **40** kann dabei helfen, mächtige POI-Angreifer (POI: Point of Interest) zu erfassen, abzuschwächen oder abzuhalten, indem wirksame Seitenkanal-Widerstand- und Zugriffsschutz-Barrieren implementiert werden, die u. a. starke Zugriffsrestriktionen haben, selbst für autorisierte Nutzer. Es werden bspw. einige Informationen immer exklusiv innerhalb des HSM **40** gehalten.

[0036] Das HSM **40** kann Sicherheitsmechanismen beschleunigen, bei denen bestimmte Beschleunigungsschaltkreise angewendet werden.

[0037] Mit dem HSM **40** können Sicherheitskosten reduziert werden, indem hoch optimierte Spezialschaltkreise hinzugefügt werden, bspw. für eine standardisierte Kryptographie.

[0038] Ein möglicher Aufbau des HSM ist in **Fig.** 3 dargestellt. Diese zeigt das HSM **70**, das in eine Umgebung eingebettet ist. Die Darstellung zeigt eine Hauptrecheneinheit **72**, einen Systembus **74**, einen RAM-Baustein **76** mit einem gemeinsam zu nutzenden Bereich und ein Testprogramm **78** bzw. Debugger mit zugeordneter Hardware **80** und Schnittstelle **82**, die wiederum ein Register **84** umfasst. Die Darstellung zeigt weiterhin einen Speicherbaustein **86** für Flash-Code mit einem Datenbereich **88** und einem sicheren Bereich **90**, in dem sichere Kerndaten enthalten sind.

[0039] In dem HSM **70** sind eine Schnittstelle **100** zum Testprogram **78**, ein sicherer Rechenkern **102**, ein sicherer RAM-Baustein **104**, ein Zufallsgenerator **106**, bspw. ein TRNG oder PRNG, und Schlüssel **108**, bspw. AES, vorgesehen.

[0040] **Fig.** 4 zeigt ein Steuergerät nach dem Stand der Technik, das insgesamt mit der Bezugsziffer **110** bezeichnet ist. Dieses Steuergerät **110** umfasst ein elektronisches Hardware-Sicherheitsmodul (HSM) **112** und eine Steuergeräte-Software **114**. Teil der Steuergeräte-Software **114** ist eine Wegfahrsperren-Software **116**, die auf eine Abschaltschnittstelle **118** zugreift.

[0041] Die Steuergeräte-Software **114** ist typischerweise in einem Speicher abgelegt, der einer Hauptrecheneinheit (nicht dargestellt) des Steuergeräts **110** zugeordnet ist. Dieser Speicher ist üblicherweise als nichtflüchtiger Speicher ausgebildet.

[0042] Bei dieser Ausführung authentisiert die Wegfahrsperren-Software **116** als Teil der Steuergeräte-Software **114** ihre Gegenseite bspw. über ein Frage-Antwort-Verfahren. Eine ggf. erforderliche kryptographische Berechnung erfolgt üblicherweise mit dem HSM **112**. Im Bedarfsfall überprüft die Wegfahrsperren-Software **116** die Authentifizierung und steuert die Abschaltschnittstelle **118**.

[0043] **Fig.** 5 zeigt eine Ausführung des beschriebenen Steuergeräts, das insgesamt mit der Bezugsziffer **130** bezeichnet ist. Dieses Steuergerät **130** umfasst ein elektronisches Hardware-Sicherheitsmodul

(HSM) **132** und eine Steuergeräte-Software **136**, die in einem Speicher abgelegt ist. Dabei ist in dem HSM **132** ein erster Teil **138** einer Wegfahrsperren-Software abgelegt. Ein zweiter Teil **140** der Wegfahrsperren-Software ist in der Steuergeräte-Software **136** enthalten. Der erste Teil **138** steuert eine erste Abschaltschnittstelle **142**, die durch einen exklusiven HSM-Anschluss gegeben ist, an. Der zweite Teil **140** steuert eine zweite Abschaltschnittstelle **144** an.

[0044] Der erste Teil **138** der Wegfahrsperren-Software authentisiert seine Gegenseite über ein Frage-Antwort-Verfahren. Für die kryptographische Berechnung wird das HSM **132** verwendet. Der erste Teil **138** prüft die Authentisierung bzw. führt die Authentisierung durch und steuert die erste Abschaltschnittstelle **142** an.

[0045] Die erste Abschaltschnittstelle **144** dient als Master, die zweite Abschaltschnittstelle **144** muss gegen die erste Abschaltschnittstelle **142** des HSM **132** plausibilisiert werden. Die beiden Abschaltschnittstellen **142** und **144** können über eine Hardware miteinander verbunden werden.

Patentansprüche

1. Verfahren zum Verhindern eines unbefugten Betriebs eines Kraftfahrzeugs, bei dem eine Wegfahrsperren-Software (**138**, **140**) verwendet wird, wobei die Wegfahrsperren-Software (**138**, **140**) zumindest teilweise in einem elektronischen Hardware-Sicherheitsmodul (**40**, **70**, **132**) abgelegt ist.

2. Verfahren nach Anspruch 1, bei dem der Teil (**138**) der Wegfahrsperren-Software (**138**, **140**), der im elektronischen Hardware-Sicherheitsmodul (**40**, **70**, **132**) abgelegt ist, eine Authentisierung durchführt.

3. Verfahren nach Anspruch 1 oder 2, bei dem der Teil (**138**) der Wegfahrsperren-Software (**138**, **140**), der im elektronischen Hardware-Sicherheitsmodul (**40**, **70**, **132**) abgelegt ist, eine erste Abschaltschnittstelle ansteuert.

4. Verfahren nach einem der Ansprüche 1 bis 3, bei dem ein erster Teil (**138**) der Wegfahrsperren-Software (**138**, **140**) in dem elektronischen Hardware-Sicherheitsmodul (**40**, **70**, **132**) abgelegt ist und ein zweiter Teil (**140**) der Wegfahrsperren-Software (**138**, **140**) in einer Steuergeräte-Software (**136**) abgelegt ist, wobei der erste Teil (**138**) eine erste Abschaltschnittstelle (**142**) ansteuert und der zweite Teil (**140**) eine zweite Abschaltschnittstelle (**144**) ansteuert, wobei die zweite Abschaltschnittstelle (**144**) gegen die erste Abschaltschnittstelle (**142**) plausibilisiert wird.

5. Elektronisches Hardware-Sicherheitsmodul, insbesondere zur Durchführung eines Verfahrens nach einem der Ansprüche 1 bis 4, mit einem Speicher (**48**), in dem eine Wegfahrsperren-Software (**138**, **140**) zumindest teilweise abgelegt ist.

6. Elektronisches Hardware-Sicherheitsmodul nach Anspruch 5, bei dem die Wegfahrsperren-Software vollständig in dem Speicher (**48**) abgelegt ist.

7. Elektronisches Hardware-Sicherheitsmodul nach Anspruch 5 oder 6, bei dem der Teil der Wegfahrsperren-Software (**138**, **140**), der im Speicher (**48**) des elektronischen Hardware-Sicherheitsmoduls (**40**, **70**, **132**) abgelegt ist, dazu eingerichtet ist, eine Authentisierung durchzuführen.

8. Elektronisches Hardware-Sicherheitsmodul nach einem der Ansprüche 5 bis 7, bei dem der Teil (**138**) der Wegfahrsperren-Software (**138**, **140**), der im Speicher (**48**) des elektronischen Hardware-Sicherheitsmoduls (**40**, **70**, **132**) abgelegt ist, dazu eingerichtet ist, eine HSM-exklusive Abschaltschnittstelle (**142**) anzusteuern.

9. Steuergerät mit einem elektronischen Hardware-Sicherheitsmodul nach einem der Ansprüche 5 bis 8.

10. Steuergerät nach Anspruch 9, bei der eine erste Abschaltschnittstelle (**142**) vorgesehen ist, die dem elektronischen Hardware-Sicherheitsmodul (**40**, **70**, **132**) zugeordnet ist, und eine zweite Abschaltschnittstelle (**144**), die einer Steuergeräte-Software zugeordnet ist, wobei die beiden Abschaltschnittstellen (**142**, **144**) über eine Hardware miteinander verknüpft sind.

Es folgen 3 Seiten Zeichnungen

Anhängende Zeichnungen

FIG. 1

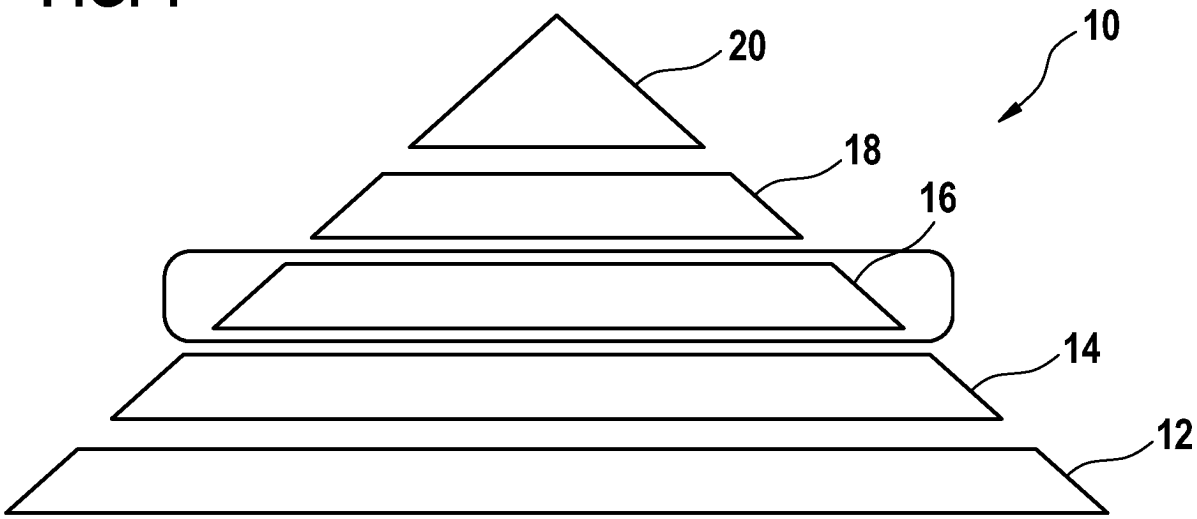


FIG. 2

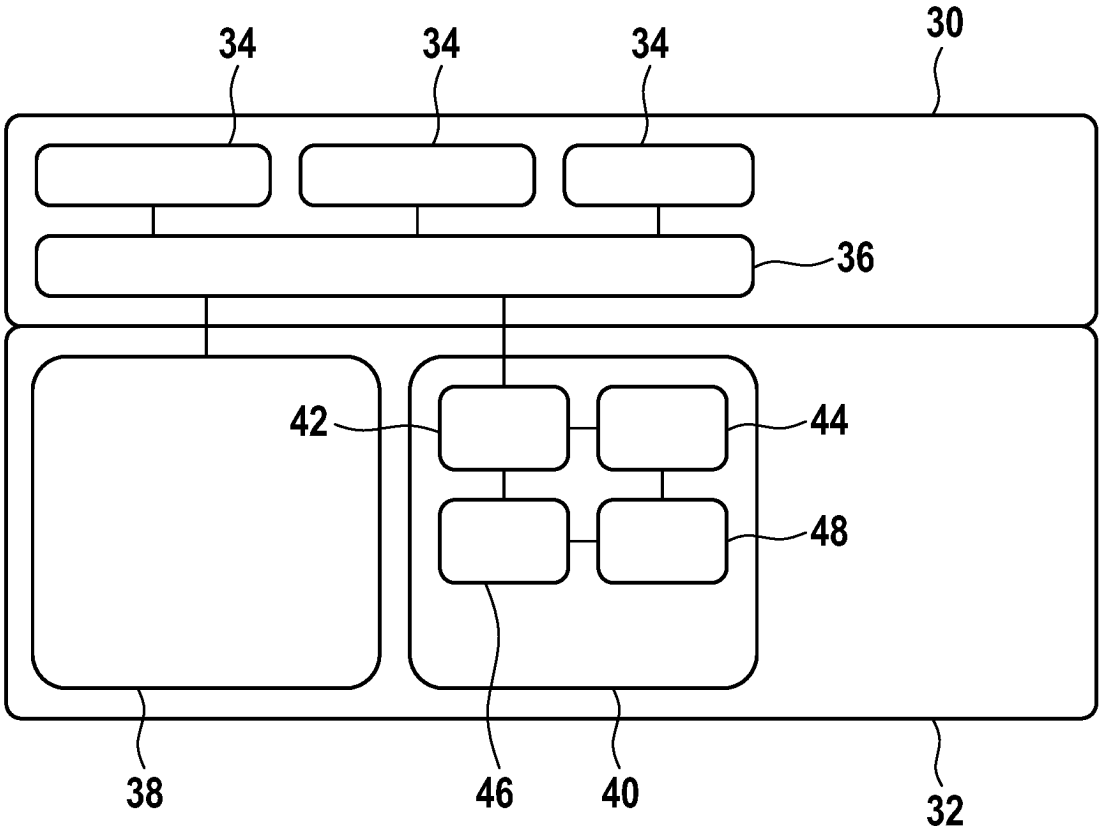


FIG. 3

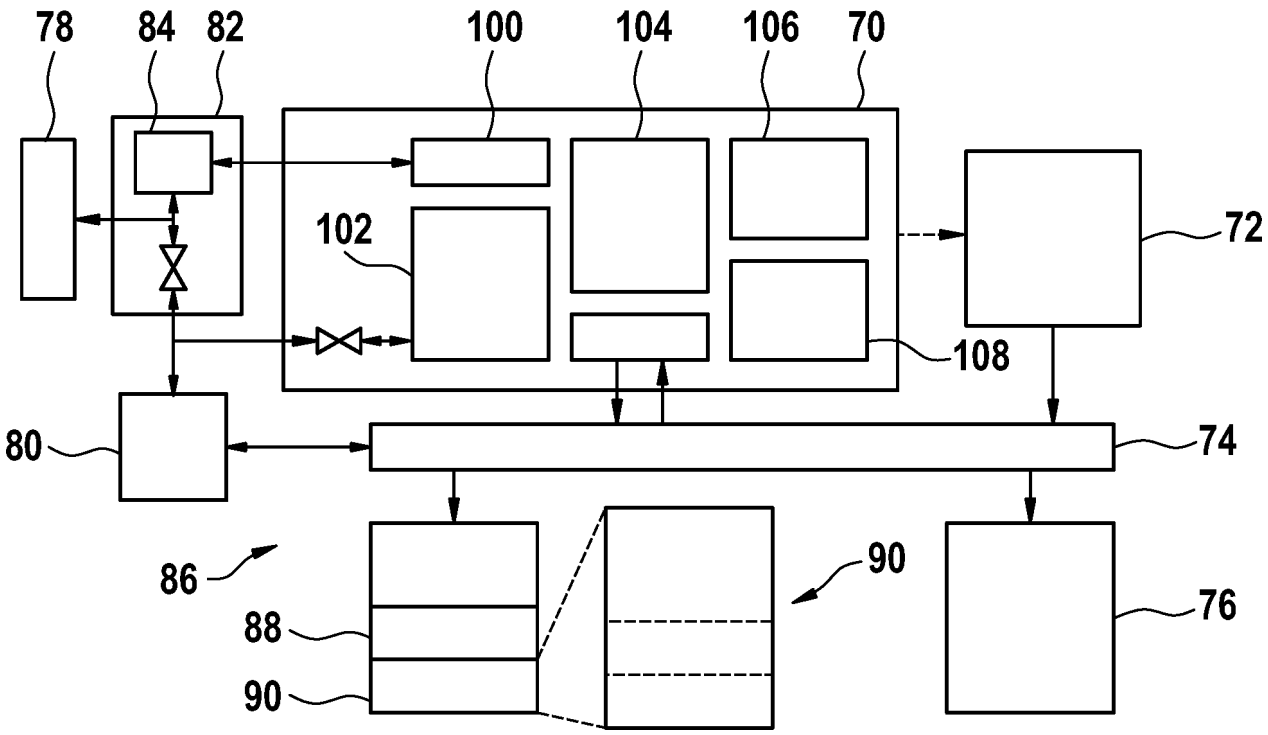


FIG. 4

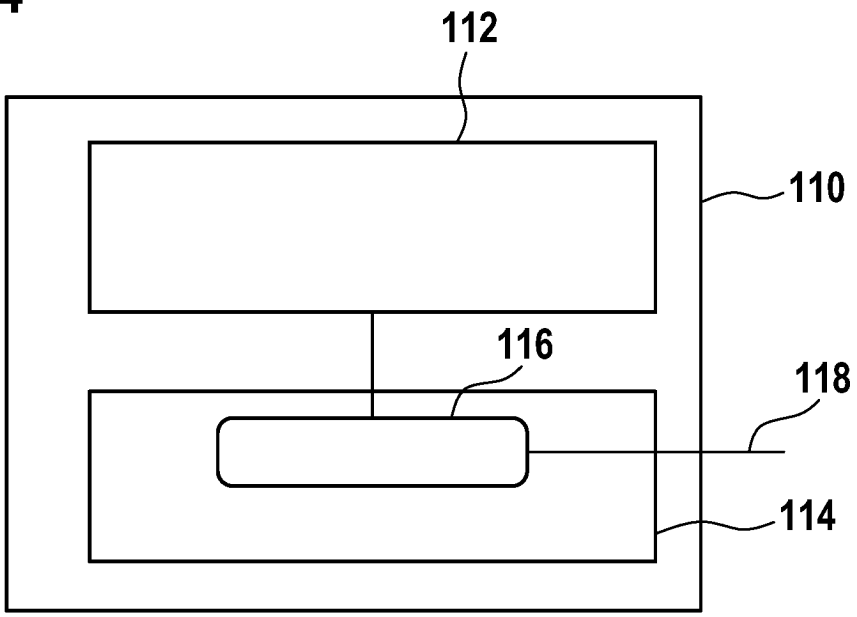


FIG. 5