(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 605 410 A2

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
14.12.2005 Patentblatt 2005/50

(51) Int Cl.[7]: **G07C 5/08**

(21) Anmeldenummer: **05104736.3**

(22) Anmeldetag: **01.06.2005**

(84) Benannte Vertragsstaaten:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU MC NL PL PT RO SE SI SK TR
Benannte Erstreckungsstaaten:
AL BA HR LV MK YU

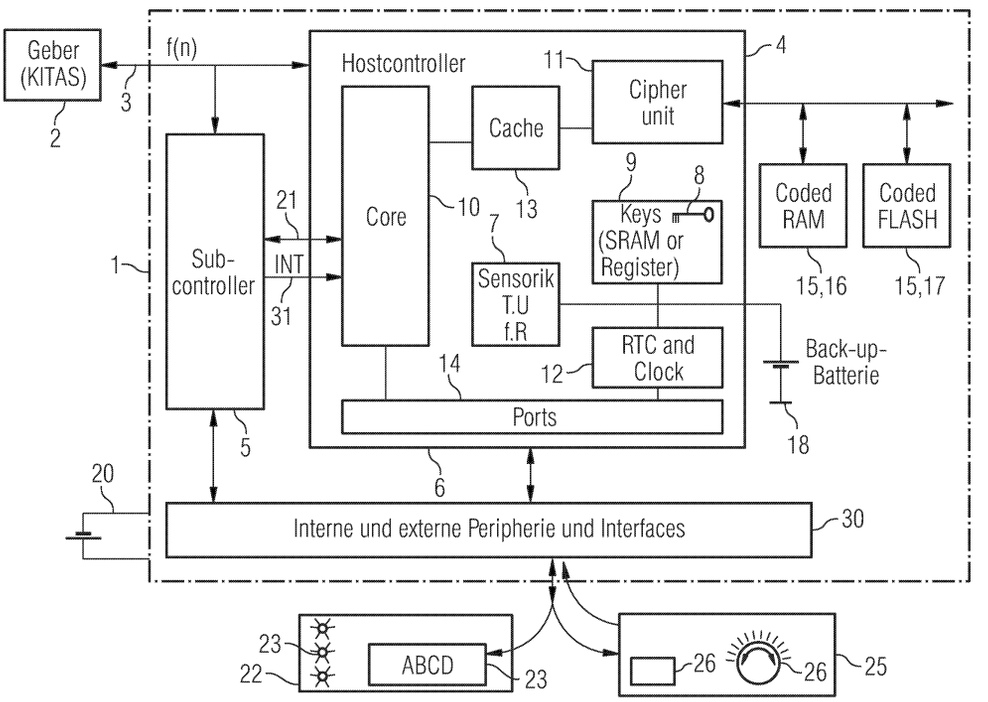
(30) Priorität: **11.06.2004 DE 102004028338**

(71) Anmelder: **SIEMENS AKTIENGESELLSCHAFT**
80333 München (DE)

(72) Erfinder:
- **Kiemes, Jochen**
  70499, Stuttgart (DE)
- **Stumpe, Reinhard Ewald**
  73765, Neuhausen (DE)
- **Rombach, Gerhard**
  78098, Triberg (DE)

(54) Tachograph

(57) Die Erfindung betrifft einen Tachographen (1) der Fahrzeugbetriebsdaten digital in einem Speicher speichert, mit einer Anzeige und Bedienelementen und mit einem ersten Mikrokontroller (4). Bisher erfordern Änderungen an derartigen Geräten ei-nen hohen behördlichen Zertifizierungsaufwand. Um dem Abhilfe zu schaffen, wird vorgeschlagen, dass der erste Mikrokontroller (4) ein Rechenwerk, eine Verschlüsselungseinheit (11), einen ersten Speicher und eine Sicherheitssensorik (7) als integrale Bauelemente aufweist, welche Sicherheitssensorik (7) mindestens einen sicherheitskritischen Umgebungsparameter über-wacht, wobei der erste Mikrokontroller (4) mit einem zweiten Mikrokontroller (5) in einer ersten Verbindung (21) steht und der zweite Mikrokontroller (5) mittels einer zweiten Verbindung mit einem Bediensystem (22) oder einem Anzeigesystem (25) verbunden ist und das Layout der Darstellung der Anzeige (26) oder die Funktion der Bedienelemente (23) steuert.



EP 1 605 410 A2

Beschreibung

[0001] Die Erfindung betrifft einen Tachographen , der Fahrzeugbetriebsdaten digital in einem Speicher speichert, mit einer Anzeige und Bedienelementen und mit einem ersten Mikrokontroller.

[0002] Die neue Generation von Fahrtschreibern bzw. Tachographen verwendet zur Aufzeichnung der Fahrzeugbetriebsdaten nicht mehr, wie herkömmlich, eine papierne Diagrammscheibe sondern speichert die Daten digital auf einem elektronischen Medium. Ein so genannter digitaler Tachograph ist bereits aus dem deutschen Gebrauchsmuster DE 298 12 216 U1 bekannt. Für den Einsatz in Nutzfahrzeugen muss ein derartiges Gerät von einschlägigen Behörden eine Sicherheitszertifiz ierung erhalten, was sehr aufwändig, zeitintensiv und kostenträchtig ist. Das Verfahren der Zertifizierung muss im Rahmen jeglicher Änderungen an den von der Zertifizierungsinstanz zu überprüfenden Bauteile durchschritten werden, so dass bereits die Berücksichtigung kleinerer Kundenwünsche mit einem sehr hohen behördlichen Aufwand einhergeht.

[0003] Die Erfindung hat es sich daher zur Aufgabe gemacht, einen Tachographen der eingangs genannten Art zu schaffen, der den hohen Anforderungen an die Manipulationssicherheit gerecht wird und gleichzeitig in seinem Aufbau derart ausgebildet ist, dass kleinere Änderungen, insbesondere hinsichtlich des Ersche inungsbildes und der Benutzerführung, mit geringerem Aufwand realisiert werden können.

[0004] Zur Lösung der Aufgabe schlägt die Erfindung vor, dass der erste Mikrokontroller des eingangs beschriebenen Tachographen ein Rechenwerk, eine Verschlüsselungseinheit, einen ersten Speicher und eine Sicherheitssensorik als integrale Bauelemente aufweist, welche Sicherheitssensorik mindestens einen sicherheitskritischen Umgebungsparameter überwacht, nämlich eine Taktfrequenz des ersten Mikrokontrollers, eine Betriebstemperatur des Mikrokontrollers, eine Versorgungsspannung des Mikrokontrollers, oder einen Widerstandswert einer den Mikrokontroller im Wesentlichen umgebenden Schutzschicht, wobei der erste Mikrokontroller mit einem zweiten Mikrokontroller in einer ersten Verbindung steht, mittels derer Daten übertrag bar sind, welcher zweite Mikrokontroller mittels einer zweiten Verbindung mit einem Bediensystem oder einem Anzeigesystem verbunden ist und das Layout der Darstellung der Anzeige oder die Funktion der Bedienelemente steuert.

[0005] Die Vorteile eines Tachographen mit einer derartigen Architektur des ersten Mikrokontrollers und das Zusammenwirken mit einem zweiten Mikrokontroller bestehen vor allem in der weitgehenden Integration der Sicherheitsfunktionen in dem ersten Mikrokontroller, was die Gerätekosten in Bez ug auf die Fläche der Leiterplatten, Bauteilevielfalt und Montagekosten erheblich reduziert. Das führt dazu, dass eine Erhöhung der Qualität der einzelnen übrigen Baugruppen gleichfalls mit reduzierten Kosten einhergeht. Der entscheidende Vorteil der Erfin dung liegt vor allem in der Trennung flexibel zu handhabender Eigenschaften und sicherheitskritischer Funktionen des Tachographen. Die flexibel handhabbaren Eigenschaften, deren Änderung keine neuerliche Sicherheitszertifizierung erfordert und die mittels des zweiten Mikrokontrollers realisiert werden, können unter Berücksichtigung von Kundenwünschen leicht angepasst werden. Beispielsweise können dem Kunden ein eigenes Anzeige -Konzept oder besondere Schnittstellenfunktionen angeboten werden, ohne sicherheitsrelevante Funktionen des Tachographen verändern zu müssen. Der zweite Mikrokontroller kann hierbei Treiberbauelemente für eine Anzeige, insbesondere für eine LCD, gegebenenfalls als integrales Bauelement, umfassen. Daneben ist es zweckmäßig, wenn Bedienelemente, beispielsweise Druckknöpfe oder Drehregler bzw. die mit diesen Bedienelementen korrespondierenden Bediensysteme mit dem zweiten Mikrokontroller in Verbindung stehen, der die mittels dieser Bedienelemente bzw. Bediensysteme getätigten Eingaben in für den ersten Mikrokontroller geeignete Anweisungen bzw. Eingaben umsetzt.

[0006] Besonders zweckmäßig ist die Speicherung kryptologischer Schlüssel in dem ersten Speicher, mittels derer die Verschlüsselungseinheit Fahrzeugsbetriebsdaten verschlüsselt. Insbesondere, wenn der erste Mikrokontroller einen aktiven Hardwareschutz aufweist, beispielsweise eine Schutzschicht, die das Halbleiterbauelement umgibt und mittels einer Sicherheitssensorik stetig auf Unversehrtheit überprüft wird, ist es sinnvoll, wenn diese sensiblen Daten in dieser Weise manipulationsgesichert und vor unbefugtem Zugriff geschützt sind.

[0007] Ein hohes Maß an Flexibilität hinsichtlich der Ausbildung des Speichermediums, auf dem die Fahrzeugbetriebsdaten digital abgelegt sind, ergibt sich, wenn die Verschlüsselungseinheit mit einem dritten Speicher, der kein integrales Bauelement des ersten Mikrokontrollers ist, in Verbindung steht und die Fahrzeugbetriebsdaten verschlüsselt in dem dritten Speicher speichert. Aufgrund des besonderen Schutzes der Ver schlüsselungseinheit, die dem Mikrokontroller zugeordnet ist und der kryptologischen Schlüssel ermöglicht die Erfindung ohne jegliche Einbuße der Schwierigkeit einer Manipulation eine Ablage der verschlüsselten Fahrzeugsbetriebsdaten in einem ansonsten nicht zwingend gegen mechanische Manipulation geschützten Speichermedium. Der dritte Speicher kann hierbei zweckmäßig als verschlüsselter Speicher wahlfreien Zugriffs (Coded RAM) oder verschlüsselter nichtflüchtiger Speicher (Coded Flash) kostengünstig ausgebildet sein.

[0008] Zur Gewährleistung der korrekten Funktion auch bei Ausfall einer externen Spannungsversorgung ist es sinnvoll, wenn der erste Mikrokontroller mit einer nicht in den Mikrokontroller integrierten Batterie in Verbindung steht, welche den Inhalt des ersten Speichers und eine in den Mikrokontroller integrierte Real-

Time-Clock mit der erforderlichen Betriebsenergie versorgt. Zweckmäßig kann die Batteriespannung von der Sicherheitssensorik überwacht werden, wobei die Real -Time-Clock zusätzlich als Manipulations-Indikator verwendbar ist, indem bestimmte Zeitmarken einer nachträglichen Auswertung unterzogen werden. Aufgrund der energetischen Pufferung der Real -Time-Clock und des Speichers, der kryptologische Schlüssel enthält, kann der erste Mikrokontroller vom Versorgungsnetz abgeschaltet werden. Auf diese Weise können verhältnismäßig niedrige Versorgungsenergien erreicht werden. Dieses Power-Down-Konzept ist im Kraftfahrzeug, wo Energiequellen begrenzte Kapazität aufweisen, besonders wertvoll. Wenn der erste Mikrokontroller von einem Betriebsenergieversorgungsnetz abschaltbar ausgebildet ist, ist es zweckmäßig, den ersten Mikrokontroller von dem zweiten Mikrokontroller mittels einer Interrupt -Leitung zwischen den beiden Mikrokontrollern einschaltbar auszubilden.

[0009] Damit der erste Mikrokontroller auch abhängig von gemessenen Fahrzeugbetriebsdaten situationsgerecht eine Anzeige ansteuern kann, ist es von Vorteil, wenn zwischen dem ersten Mikrokontroller und dem zweiten Mikrokontroller eine Dat enübertragungsverbindung vorgesehen ist, mittels derer der erste Mikrokontroller dem zweiten Mikrokontroller Fahrzeugbetriebsdaten übermittelt, die der zweite Mikrokontroller auf der Anzeige zur Darstellung bringt. Zur Aufzeichnung und Auswertung der mittels eines Messwertgebers gemessenen Drehzahl an einem Getriebebauelement erweist sich eine direkte Verbindung zwischen dem ersten Mikrokontroller und dem Messwertgeber zur Signalübertragung als zweckmäßig. Gegebenenfalls kann der zweite Mikrokontroller eine direkte Verbindung zu dem Messwertgeber aufweisen, so dass beispielsweise eine direkte Darstellung der Geschwindigkeit ohne vorherige Auswertung durch den ersten Mikrokontroller auf einer Anzeige des Tachographen möglich ist.

[0010] Eine maximale Sicherheit gegen unbefugten Zugriff wird erhalten, wenn die Sicherheitssensorik bei einem Über - oder Unterschreiten eines vorbestimmten Grenzwerts für einen Umgebungsparameter die in dem ersten Speicher gespeicherten kryptologischen Schlüssel löscht. Zusätzlich kann ein Löschen des Programmspeichers in dem ersten Mikrokontroller für diesen Fall vorgesehen sein. Damit der Löschvorgang stets gewährleistet ist, kann eine in den ersten Mikrokontroller integrierte Hilfsenergiepufferung vorgesehen sein.

[0011] Im Folgenden ist die Erfindung anhand eines Ausführungsbeispiels unter Bezugnahme auf eine Zeichnung näher beschrieben. Es zeigt:

Fig. 1: eine schematische Darstellung der Funktionsweise des erfindungsgemäßen Tachographen.

[0012] Der in Fig. 1 dargestellte Tachograph 1 steht mit einem Messwertgeber 2 in einer zur Datenübertragung geeigneten dritten Verbindung 3. Der Messwertgeber 2 übermittelt die gemessenen Daten, nämlich die Drehzahl n eines nicht dargestellten Getriebebauelements, mittels einer gleichfalls nicht dargestellten internen Verschlüsselungseinheit verschlüsselt an den Tachographen 1. In dem Tachographen 1 wird die verschlüsselte Drehzahl N mittels der dritten Verbindung 3 sowohl an einen ersten Mikrokontroller 4 als auch an einen zweiten Mikrokon troller 5 übermittelt.

[0013] Der erste Mikrokontroller 4 ist von einer aktiven Schutzschicht 6 umgeben, die aus Leiterbahnen besteht, welche mittels einer Sicherheitssensorik 7 auf ihre Unversehrtheit überwacht werden. Hierzu misst die Sicherheitssensorik 7 stetig einen Widerstandswert R dieser nicht dargestellten Leiterbahnen bzw. der Schutzschicht 6 und veranlasst bei Überschreiten oder Unterschreiten eines bestimmtes Grenzwerts das Löschen von kryptologischen Schlüsseln 8, die in einem ersten Speicher 9 des ersten Mikrokontrollers 4 gespeichert sind sowie eines Programmcodes, mit dem der erste Mikrokontroller 4 arbeitet. Neben einem Rechenwerk 10, einem ersten Speicher 9 und der Sicherheitssensorik 7 sind auch noch eine Verschlüsselungseinheit 11, eine Real-Time-Clock 12, ein zwischen dem Rechenwerk 10 und der Verschlüsselungseinheit 11 angeordneter Zwischenspeicher 13 (Cache) und ein verschiedener Schnittstellen verwaltendes Bauteil 14 wesentliche Bestandteile des ersten Mikrokontrollers 4. Die Verschlüsselungseinheit 11 steht mit nicht in den ersten Mikrokontroller 4 integrierten dritten Speichern 15 in Verbindung, nämlich einem verschlüsselten Speicher wahlfreie Zugriffs (Coded RAM) 16 und einem verschlüsselten nichtflüchtigen Speicher (Coded Flash) 17. Von dem Messwertgeber 2 an den ersten Mikrokontroller 4 übermittelte Drehzahlmesswerte werden zunächst von dem Rechenwerk 10 verarbeitet und anschließend an den Zwischenspeicher 13 übermittelt, auf den die Verschlüsselungseinheit 11 zur Verschlüsselung diese r ausgewerteten Fahrzeugsbetriebsdaten zugreift, welche anschließend in den dritten Speicher 15 abgelegt werden.

[0014] Eine Batterie 18 sorgt selbst bei Ausfall einer Energieversorgung mittels eines externen Betriebsenergieversorgungsnetzes 20 für die Aufrechterhaltung der Funktionen der Sicherheitssensorik 7, des ersten Speichers 9 und der Real -Time-Clock 12.

[0015] Mittels einer ersten Verbindung 21 steht der erste Mikrokontroller 4 mit dem zweiten Mikrokontroller 5 im Datenaustausch, so dass der zweite Mikrokontroller 5 mittels des Bauteils 14 eine Ansteuerung von Anzeigesystemen 22 und Anzeigen 23 veranlasst. Benutzerseitige Eingaben in den Tachographen 1 sind möglich mittels Bediensystemen 25 bzw. Bedienelementen 26, deren Betätigung mittels eines Interfaces 30 an den ersten Mikrokontroller 4 und/oder den zweiten Mikrokontroller 5 übermittelt werden.

[0016] Die Sicherheitssensorik 7 überwacht neben der Unversehrtheit bzw. dem Widerstandswert R der aktiven Schutzschicht 6 auch noch die Umgebungspara-

meter Taktfrequenz F , Betriebstemperatur T und Versorgungsspannung U. Für jeden der Umgebungsparameter sind zwei Grenzwerte definiert, bei deren Überschreiten bzw. Unterschreiten eine Löschung der Programmdateien und der kryptologischen Schlüssel 8 erfolgt.

[0017] Der erste Mikrokontroller 4 ist von der Spannung des Betriebsversorgungsnetzes 20 trennbar, wobei eine Interrupt -Leitung 31 zwischen dem zweiten Mikrokontroller 5 und dem ersten Mikrokontroller 4 ein Einschalten bzw. eine Aufnahme der vollen Betriebsspannung des ersten Mikrokontrollers 4, veranlasst durch den zweiten Mikrokontroller 5 ermöglicht.

Patentansprüche

1. Tachograph mit einer Anzeige und Bedienelementen, der Fahrzeugbetriebsdaten digital in einem Speicher speichert, mit einem ersten Mikrokontroller (4), **dadurch gekennzeichnet, dass** der erste Mikrokontroller (4) ein Rechenwerk, eine Verschlüsselungseinheit (11), einen ersten Speicher und eine Sicherheitssensorik (7) als integrale Bauelemente aufweist, welche Sicherheitssensorik (7) mindestens einen sicherheitskritischen Umgebungsparameter überwacht, nämlich eine Taktfrequenz des ersten Mikrokontrollers (4), eine Betriebstemperatur T des Mikrokontrollers, eine Versorgungsspannung (U) des Mikrokontrollers oder einen Widerstandswert (R) einer den Mikrokontroller im Wesentlichen umgebenden Schutzschicht (6), wobei der erste Mikrokontroller (4) mit einem zweiten Mikrokontroller (5) in einer ersten Verbindung (21) steht, mittels derer Daten übertragbar sind, welcher zweite Mikrokontro ller (5) mittels einer zweiten Verbindung mit einem Bediensystem (22) oder einem Anzeigesystem (25) verbunden ist und das Layout der Darstellung der Anzeige (26) oder die Funktion der Bedienelemente (23) steuert.

2. Tachograph nach Anspruch 1, **dadurch gekennzeichnet, dass** in dem ersten Speicher (9) kryptologische Schlüssel (8) gespeichert sind, mittels derer die Verschlüsselungseinheit (11) Fahrzeugbetriebsdaten verschlüsselt.

3. Tachograph nach Anspruch 1, **dadurch gekennzeichnet, dass** die Verschlüsselungseinheit (11) mit einem dritten Speicher (15), der kein integrales Bauelement des ersten Mikrokontrollers (4) ist, in Verbindung steht und die Fahrzeugbetriebsdaten verschlüsselt in dem dritten Speicher (15) speichert.

4. Tachograph nach Anspruch 3, **dadurch gekennzeichnet, dass** der dritte Speicher (15) als verschlüsselter Speicher wahlfreiem Zugriffs (Coded RAM) (16) oder verschlüsselter nichtflüchtiger Speicher (Coded Flash) (17) ausgebildet ist.

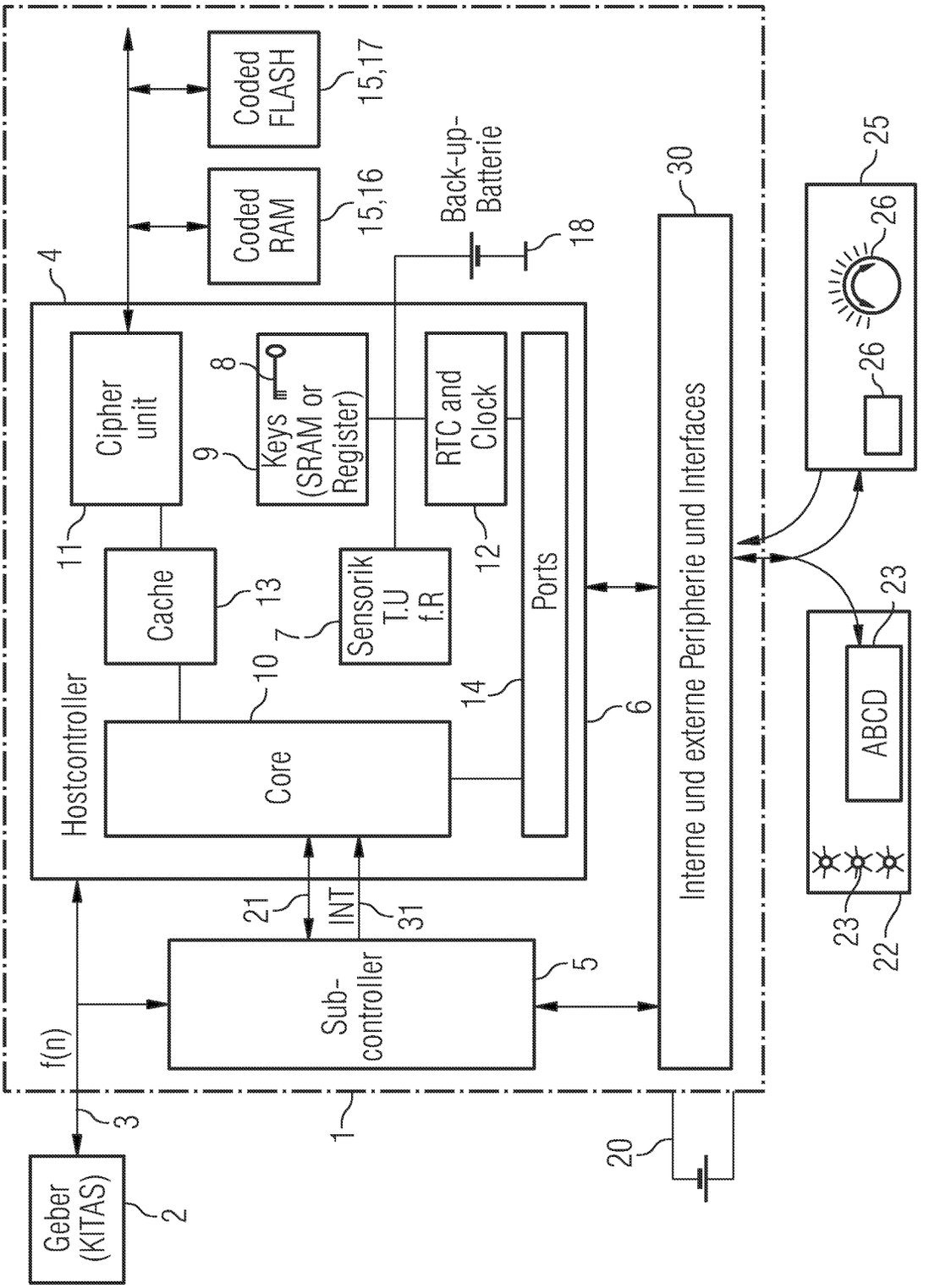
5. Tachograph nach Anspruch 1, **dadurch gekennzeichnet, dass** der erste Mikrokontroller (4) mit einer nicht in den Mikrokontroller integrierten Batterie (18) in Verbindung steht, welche den Inhalt des ersten Speichers (9) und eine in den Mikrokontroller integrierte Real -Time-Clock (12) bei Ausfällen einer externen Spannungsversorgung mit einer Betriebsenergie versorgt.

6. Tachograph nach Anspruch 5, **dadurch gekennzeichnet, dass** der erste Mikrokontroller (4) von einem Betriebsenergieversorgungsnetz abschaltbar ist und der erste Mikrokontroller (4) von dem zweiten Mikrokontroller (5) mittels einer Interrupt-Leitung (31) zwischen dem ersten Mikrokontroller (4) und dem zweiten Mikrokontroller (5) einschaltbar ausgebildet ist.

7. Tachograph nach Anspruch 1, **dadurch gekennzeichnet, dass** der erste Mikrokontroller (4) mit einem Messwertgeber (2) in einer Signale übertragenden dritten Verbindung (3) steht, der an einem Getriebebauelement eine Drehzahl n misst und dem ersten Mikrokontroller (4) übermittelt.

8. Tachograph nach Anspruch 1, **dadurch gekennzeichnet, dass** zwischen dem ersten Mikrokontroller (4) und dem zweiten Mikrokontroller (5) eine Datenübertragungsverbindung vorgesehen ist, mittels derer der erste Mikrokontroller (4) dem zweiten Mikrokontroller (5) Fahrzeugbetriebsdaten übermittelt, die der zweite Mikrokontroller (5) auf der Anzeige (26) zur Darstellung bringt.

9. Tachograph nach Anspruch 2, **dadurch gekennzeichnet, dass** der Mikrokontroller, wenn die Sicherheitssensorik (7) ein Überschreiten oder Unterschreiten eines bestimmten Grenzwertes für einen Umgebungsparameter ermittelt, in dem ersten Speicher (9) gespeicherte kryptologische Schlüssel (8) löscht.


Coded FLASH
15,17
Coded RAM
15,16
Back-up-Batterie
18
4
Cipher unit
11
8
Keys (SRAM or Register)
9
RTC and Clock
12
Cache
13
Sensorik T.U f.R
7
Ports
14
Hostcontroller
10
Core
6
Interne und externe Peripherie und Interfaces
30
25
26
26
23
ABCD
23
22
21
INT
31
Sub-controller
5
f(n)
3
1
20
Geber (KITAS)
2