(19) Deutsches Patent- und Markenamt

(10) **DE 11 2011 103 745 T5** 2013.08.14

(12) # Veröffentlichung

der internationalen Anmeldung mit der
(87) Veröffentlichungs-Nr.: **WO 2012/063724**
in deutscher Übersetzung (Art. III § 8 Abs. 2 IntPatÜG)
(21) Deutsches Aktenzeichen: **11 2011 103 745.7**
(86) PCT-Aktenzeichen: **PCT/JP2011/075393**
(86) PCT-Anmeldetag: **04.11.2011**
(87) PCT-Veröffentlichungstag: **18.05.2012**
(43) Veröffentlichungstag der PCT Anmeldung
in deutscher Übersetzung: **14.08.2013**

(51) Int Cl.: ***G06F 21/00*** (2013.01)
B60R 16/023 (2013.01)
G06F 11/00 (2013.01)
G06F 21/20 (2013.01)
H04L 12/28 (2013.01)

(30) Unionspriorität:
2010-254123 **12.11.2010** **JP**

(71) Anmelder:
Hitachi Automotive Systems, Ltd., Hitachinaka-shi, Ibaraki, JP

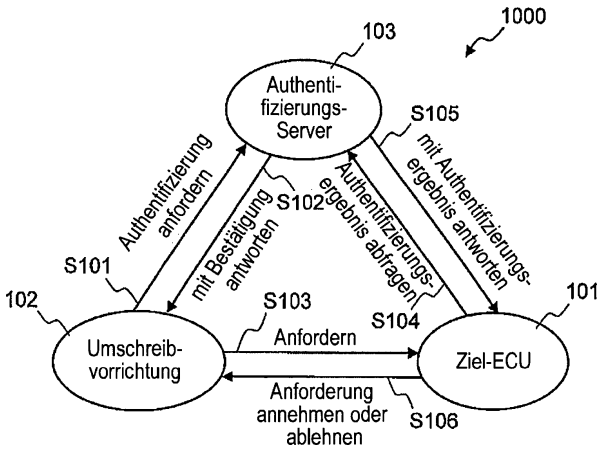
(74) Vertreter:
MERH-IP Matias Erny Reichl Hoffmann, 80336, München, DE

(72) Erfinder:
Miyake, Junji, Hitachinaka-shi, Ibaraki, JP

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Fahrzeugmontiertes Netzwerksystem**

(57) Zusammenfassung: Es wird ein Verfahren geschaffen, das die Sicherheit eines fahrzeugmontierten Netzwerkes steigern und dabei die Verarbeitungslasten in jeder fahrzeugmontierten Steuervorrichtung verringern kann.
In einem fahrzeugmontierten Netzwerksystem gemäß der vorliegende Erfindung wird eine Kommunikationsvorrichtung, die eine Leseanforderung oder eine Schreibanforderung an Daten, die in der fahrzeugmontierten Steuervorrichtung gehalten werden, ausgibt, im Voraus durch eine Authentifizierungsvorrichtung authentifiziert.



Beschreibung

Technisches Gebiet

[0001] Die vorliegende Erfindung bezieht sich auf ein fahrzeugmontiertes Netzwerksystem.

Stand der Technik

[0002] In den letzten Jahren sind fahrzeugmontierte ECUs (elektronische Steuereinheiten) zum Steuern jeder Funktionseinheit in Personenkraftwagen, Lastkraftwagen und Bussen montiert worden. Die jeweiligen ECUs sind miteinander über ein fahrzeugmontiertes Netzwerk verbunden, um zusammenzuwirken.

[0003] Jede ECU führt in ihrer Entwicklungsphase eine Kalibrierung, Adaption oder Anpassung genannten Schritt aus. In dem Schritt werden Steuerparameter von außerhalb der ECU überwacht, wobei Steuerkonstanten, auf die durch ein internes Programm Bezug genommen wird, geändert werden und in jede ECU zurückgeschrieben werden, um eingestellt zu werden.

[0004] Außerhalb der Entwicklungsphase muss Software bei einer Rückruf- oder Kundendienstkampagne nach der Auslieferung der Fahrzeuge umgeschrieben werden. Das bedeutet, dass dann, wenn ein Fehler des Steuerprogramms festgestellt wird, nachdem Produkte an den Markt ausgeliefert worden sind, das Programm der fahrzeugmontierten ECUS umgeschrieben wird, nachdem Händler die Fahrzeuge zurückgerufen haben.

[0005] Die Steuerparameter werden von außerhalb der fahrzeugmontierten ECU über ein fahrzeugmontiertes Netzwerk wie etwa ein CAN (Controller-Bereichsnetzwerk) oder FlexRay neu eingestellt oder das Programm wird von außerhalb der fahrzeugmontierten ECU über ein solches Netzwerk umgeschrieben. Zu diesem Zeitpunkt wird ein dediziertes Umschreib-Endgerät mit dem fahrzeugmontierten Netzwerk verbunden oder ein Fahrzeugkommunikationsnetzwerk außerhalb des Fahrzeugs wie etwa des Internet und das fahrzeugmontierte Netzwerk werden elektrisch miteinander verbunden, um die Umschreibarbeit auszuführen. Um hierbei ein nicht autorisiertes Umschreiben auszuschließen, ist es notwendig, zu authentifizieren, ob das Umschreib-Endgerät oder eine Vorrichtung, das bzw. die mit dem fahrzeugmontierten Netzwerk verbunden ist, um einen Umschreibbefehl auszugeben, genehmigt ist.

[0006] Typischerweise ist das Steuerprogramm der fahrzeugmontierten ECU in einer Speichervorrichtung wie etwa einem Flash-ROM (Festwertspeicher) in einem eingebauten Mikrocomputer gespeichert. Um das Programm umzuschreiben, werden sämtliche gespeicherten Daten in dem Bereich, der das alte Programm enthält, physikalisch temporär gelöscht, woraufhin ein neues Programm in diesen initialisierten Bereich geschrieben werden muss.

[0007] Wenn das Umschreib-Endgerät oder dergleichen bösartig ist, wird das alte Programm in der ECU gelöscht, es wird jedoch kein neues Programm übertragen, wodurch die Funktion der ECU einfach angehalten wird. Die Funktion wird angehalten, außerdem kann das Programm in ein neues, bösartiges Programm umgeschrieben werden. Dadurch kann ein Programm, das absichtlich ein unsicheres Verhalten für die Steuerung hervorruft, installiert werden. Ferner kann das Problem hervorgerufen werden, das von jenem, dass die ECU umgeschrieben wird, verschieden ist. Beispielsweise kann ein Programm, das absichtlich den Kommunikationsverkehr des fahrzeugmontierten Netzwerkes sättigt, installiert werden. Außerdem werden die Informationen, dass eine spezifische ECU ausgefallen ist, an das fahrzeugmontierte Netzwerk geliefert, wodurch andere normale ECUs in einem absichtlichten Ausfallsicherungsbetrieb arbeiten.

[0008] Oben ist das Programmumschreiben beschrieben worden, außerdem kann jedoch eine Funktion zum Bestätigen von Variablen in der ECU in der Entwicklungsphase missbräuchlich verwendet werden und Daten in der ECU könnten illegal erfasst werden. Beispielsweise könnten die Steuerparameter einer spezifischen ECU über das fahrzeugmontierte Netzwerk illegal überwacht werden und ein Reverse-Engineering könnte anhand des überwachten Ergebnisses ausgeführt werden, um technische Informationen über die ECU zu sammeln, oder persönliche Informationen könnten aus Informationssystem-ECUs wie etwa der Fahrzeugnavigation, der ETC (elektronische Gebührensammlung) oder dem Zellentelephon erfasst werden.

[0009] PTL1, die später beschrieben wird, offenbart als eine Technik zum Schützen eines fahrzeugmontierten Netzwerkes und von ECUs, die das Netzwerk konfigurieren, vor dem bösartigen Endgerät, das oben beschrieben wurde, und ein Verfahren, in dem eine mit einem externen Endgerät kommunizierende ECU ein Teilneh-

merendgerät individuell authentifiziert, um dadurch ein nicht berechtigtes Eindringen über das fahrzeugmontierte Netzwerk zu beseitigen.

Entgegenhaltungsliste

Patentliteratur: PTL1: JP 2010-23556 A

Zusammenfassung der Erfindung

Technisches Problem

[0010] In einem Fall wie etwa bei einem Verkehrssättigungsangriff in einem fahrzeugmontierten Netzwerk hängt die Sicherheit des gesamten fahrzeugmontierten Netzwerkes von einer ECU mit am stärksten gefährdeter Sicherheit ab. Selbst wenn daher eine einzelne ECU ihre Sicherheit erhöht, kann die Sicherheit des gesamten fahrzeugmontierten Netzwerkes aufgrund anderer gefährdeter ECUS nicht erhöht werden.

[0011] Was jedoch die fahrzeugmontierte ECU betrifft, sind die Rechenfähigkeit des montierten Mikrocomputers oder ein Betriebsmittel wie etwa ein ROM/RAM (Schreib-Lese-Speicher) verhältnismäßig niedrige Funktionen, weshalb es schwierig ist, einen fortschrittlichen Authentifizierungsalgorithmus zu verwenden.

[0012] Die vorliegende Erfindung ist gemacht worden, um die obigen Probleme zu lösen, wobei es eine Aufgabe der vorliegenden Erfindung ist, ein Verfahren zu schaffen, das die Sicherheit eines fahrzeugmontierten Netzwerkes verbessern kann, während Verarbeitungslasten jeder fahrzeugmontierten Steuervorrichtung verringert werden.

Lösung für das Problem

[0013] In einem fahrzeugmontierten Netzwerksystem gemäß der vorliegenden Erfindung wird eine Kommunikationsvorrichtung für die Ausgabe einer Leseanforderung oder einer Schreibanforderung für Daten, die in einer fahrzeugmontierten Steuervorrichtung gehalten werden, im Voraus durch eine Authentifizierungsvorrichtung authentifiziert.

Vorteilhafte Wirkungen der Erfindung

[0014] In dem fahrzeugmontierten Netzwerksystem gemäß der vorliegenden Erfindung führt die Authentifizierungsvorrichtung die Authentifizierungsverarbeitung insgesamt aus, so dass ein fortschrittliches Authentifizierungsverfahren ausgeführt werden kann, ohne Verarbeitungslasten in jeder fahrzeugmontierten Steuervorrichtung zu erhöhen. Daher kann die Sicherheit des fahrzeugmontierten Netzwerkes erhöht werden, während die Verarbeitungslasten in jeder fahrzeugmontierten Steuervorrichtung verringert werden.

Kurzbeschreibung der Zeichnungen

[0015] Fig. 1 ist ein Diagramm, das eine Konfiguration eines fahrzeugmontierten Netzwerksystems **1000** gemäß einer ersten Ausführungsform veranschaulicht.

[0016] Fig. 2 ist ein Diagramm, das eine beispielhafte Konfiguration des fahrzeugmontierten Netzwerksystems **1000** gemäß einer zweiten Ausführungsform veranschaulicht.

[0017] Fig. 3 ist ein Diagramm, das eine weitere beispielhafte Konfiguration des fahrzeugmontierten Netzwerksystems **1000** veranschaulicht.

[0018] Fig. 4 ist ein Ablaufdiagramm, das eine Kommunikationsprozedur zwischen einer Ziel-ECU **101**, einer Umschreibvorrichtung **102** und einem Authentifizierungs-Server **103** veranschaulicht.

[0019] Fig. 5 ist ein Ablaufdiagramm, das eine weitere Kommunikationsprozedur zwischen der Ziel-ECU **101**, der Umschreibvorrichtung **102** und dem Authentifizierungs-Server **103** veranschaulicht.

[0020] Fig. 6 ist ein Diagramm, das eine Verarbeitungsfolge zum Bestätigen, ob eine Kommunikation zwischen dem Authentifizierungs-Server **103** und der Ziel-ECU **101** besteht, veranschaulicht.

[0021] Fig. 7 ist ein Diagramm, das eine weitere Verarbeitungsfolge zum Bestätigen, ob eine Verbindung zwischen dem Authentifizierungs-Server **103** und der Ziel-ECU **103** besteht, veranschaulicht.

[0022] Fig. 8 ist ein Diagramm zur Erläuterung der Operationen, wenn der Authentifizierungs-Server **103** eine Vorrichtung zum Manipulieren des Authentifizierungs-Servers **103** in dem fahrzeugmontierten Netzwerk detektiert.

[0023] Fig. 9 ist ein Diagramm, das einen beispielhaften Verarbeitungsablauf veranschaulicht, der ausgeführt wird, wenn die Ziel-ECU **101** eine Sitzungsbeginn-Anforderung von der Umschreibvorrichtung **102** gemäß der ersten bis vierten Ausführungsform empfängt.

[0024] Fig. 10 ist ein Diagramm, das eine beispielhafte Netzwerktopologie eines fahrzeugmontierten Netzwerkes, das in einem neuesten typischen hochentwickelten Fahrzeug vorgesehen ist, veranschaulicht.

Beschreibung von Ausführungsformen

<Erste Ausführungsform>

[0025] Fig. 1 ist ein Diagramm, das eine Konfiguration eines fahrzeugmontierten Netzwerksystems **1000** gemäß einer ersten Ausführungsform der vorliegenden Erfindung veranschaulicht. Das fahrzeugmontierte Netzwerksystem **1000** ist ein fahrzeuginternes Netzwerk, das ECUs für die Steuerung des Betriebs des Fahrzeugs verbindet. Hier ist beispielhaft nur eine Ziel-ECU **101**, deren Steuerprogramm umgeschrieben werden soll, veranschaulicht, die Anzahl von ECUs, die mit dem fahrzeugmontierten Netzwerksystem **1000** verbunden sind, ist jedoch nicht darauf eingeschränkt.

[0026] Das fahrzeugmontierte Netzwerksystem **1000** ist mit der Ziel-ECU **101** und mit einem Authentifizierungs-Server **103** über ein Kommunikationsnetzwerk verbunden. Mit dem fahrzeugmontierten Netzwerksystem **1000** wird nach Bedarf eine Umschreibvorrichtung **102** verbunden, um ein in einem Speicher wie etwa einem Flash-ROM gespeichertes Steuerprogramm durch die Ziel-ECU **101** umzuschreiben oder um interne Daten der Ziel-ECU **101** zu erfassen.

[0027] Der Authentifizierungs-Server **103** kann mit der Ziel-ECU **101** und mit der Umschreibvorrichtung **102** über das fahrzeugmontierte Netzwerk kommunizieren. Der Authentifizierungs-Server **103** kann als eine ECU konfiguriert sein oder kann als irgendeine andere Kommunikationsvorrichtung konfiguriert sein.

[0028] Die Umschreibvorrichtung **102** muss durch den Authentifizierungs-Server **103** im Voraus authentifiziert werden, um die oben beschriebene Verarbeitung an der Ziel-ECU **101** auszuführen. Die hier beschriebene Authentifizierung ist eine Verarbeitung zum Verifizieren, ob die Umschreibvorrichtung **102** eine Berechtigung hat, die Verarbeitung an der Ziel-ECU **101** auszuführen. Eine Prozedur, in der die Umschreibvorrichtung **102** die Verarbeitung an der Ziel-ECU **101** ausführt, wird im Folgenden mit Bezug auf Fig. 1 beschrieben.

(Fig. 1: Schritt S101: Authentifizierung anfordern)

[0029] Vor der Ausgabe einer Programmumschreibanforderung oder einer Datenerfassungsanforderung an die Ziel-ECU **101** fordert die Umschreibvorrichtung **102** den Authentifizierungs-Server **103** über das fahrzeugmontierte Netzwerk auf, die Umschreibvorrichtung zu authentifizieren. Zu diesem Zeitpunkt werden Informationen, die für die Umschreibvorrichtung **102** spezifisch sind, etwa eine Kennung der Umschreibvorrichtung **102**, gemeinsam übertragen.

(Fig. 1: Schritt S102: mit Bestätigung antworten)

[0030] Wenn der Authentifizierungs-Server **103** die Authentifizierungsanforderung von der Umschreibvorrichtung **102** empfängt, verwendet er einen vorgegebenen Authentifizierungsalgorithmus, um die Umschreibvorrichtung **102** zu authentifizieren. Der Authentifizierungs-Server **103** ordnet der Kennung der Umschreibvorrichtung **102** das Authentifizierungsergebnis zu und hält es in einer Speichervorrichtung wie etwa einem Speicher. Wenn die Authentifizierungsverarbeitung abgeschlossen ist, überträgt der Authentifizierungs-Server **103** eine Bestätigungsantwort an die Umschreibvorrichtung **102**.

(Fig. 1: Schritt S102: mit Bestätigung antworten: Ergänzung)

[0031] Wenn die Bestätigungsantwort im vorliegenden Schritt zu der Umschreibvorrichtung **102** übertragen wird, überträgt der Authentifizierungs-Server **103** die Bestätigungsantwort, ohne dass darin Informationen darüber enthalten sind, ob die Bestätigungsantwort authentifiziert werden muss. Dies zielt auf den Schutz des Authentifizierungsalgorithmus vor der Umschreibvorrichtung **102**, die eine oftmalige Authentifizierung versucht, um die Authentifizierungsverarbeitung zu unterbrechen.

(Fig. 1: Schritt S103: Anforderung)

[0032] Die Umschreibvorrichtung **102** überträgt eine Anforderung zum Umschreiben des in dem Speicher in der Ziel-ECU **101** gespeicherten Steuerprogramms oder eine Anforderung zum Erfassen der internen Daten der Ziel-ECU **101** an die Ziel-ECU **101**.

(Fig. 1: Schritt S104: Abfragen des Authentifizierungsergebnisses)

[0033] Die Ziel-ECU **101** fragt den Authentifizierungs-Server **103** ab, ob die Anforderungsübertragungsquelle im Schritt S103 ein autorisiertes Endgerät ist.

(Fig. 1: Schritt S105: Beantworten des Authentifizierungsergebnisses)

[0034] Der Authentifizierungs-Server **103** sucht das Authentifizierungsergebnis der Umschreibvorrichtung **102**, die im Schritt S102 gehalten wird, und überträgt das Ergebnis an die Ziel-ECU **101**.

(Fig. 1: Schritt S106: Annehmen oder Ablehnen der Anforderung)

[0035] Wenn die Antwort einer zulässigen Authentifizierung von dem Authentifizierungs-Server **103** im Schritt S105 erfasst wird, nimmt die Ziel-ECU **101** die von der Umschreibvorrichtung **102** im Schritt S103 empfangene Anforderung an. Wenn die Antwort einer unzulässigen Authentifizierung erfasst wird, wird die von der Umschreibvorrichtung **102** empfangene Anforderung abgelehnt. Die Ziel-ECU **101** antwortet der Umschreibvorrichtung **102**, ob die Anforderung angenommen wird.

<Erste Ausführungsform: Fazit>

[0036] Wie oben beschrieben, authentifiziert der Authentifizierungs-Server **103** in dem fahrzeugmontierten Netzwerksystem **1000** gemäß der ersten Ausführungsform gemeinsam die Umschreibvorrichtung **102**, die eine Leseanforderung oder eine Schreibanforderung an internen Daten der ECU **101** ausgegeben hat. Dadurch muss keine ECU die Authentifizierungsverarbeitung ausführen, sondern lediglich den Authentifizierungs-Server **103** bezüglich des Authentifizierungsergebnisses abfragen. Daher kann die Authentifizierung ohne Erhöhung von Verarbeitungslasten in jeder ECU **101** ausgeführt werden.

[0037] In dem fahrzeugmontierten Netzwerksystem **1000** gemäß der ersten Ausführungsform kann die Authentifizierungsverarbeitung in dem Authentifizierungs-Server **103** gemeinsam ausgeführt werden, weshalb eine fortschrittliche Authentifizierungstechnik wie etwa eine Verschlüsselung mit öffentlichem Schlüssel in dem Authentifizierungs-Server **103** verwendet werden kann. Daher kann die Sicherheit des fahrzeugmontierten Netzwerksystems **1000** ohne jegliche Einschränkung des Betriebsmittels jeder ECU **101** verbessert werden. Die Hardware-Leistung jeder ECU **101** muss im Gegensatz zu früher nicht gesteigert werden, um die Sicherheit zu verbessern, weshalb eine Kostensteigerung für eine erhöhte Sicherheit begrenzt werden kann.

[0038] Lediglich der Authentifizierungs-Server **103** führt eine Authentifizierungsverarbeitung in dem fahrzeugmontierten Netzwerksystem **1000** gemäß der ersten Ausführungsform aus. Somit müssen die technischen Informationen über die Authentifizierungsverarbeitung nicht für externe Hersteller offenbart werden, wodurch Sicherheitsinformationslecks aufgrund der Verbreitung der technischen Informationen verhindert werden. Das heißt, dass typische fahrzeugmontierte ECUs, obwohl sie dieselbe Spezifikation haben, bei mehreren ECU-Herstellern in Abhängigkeit vom Fahrzeugtyp oder vom Lieferziel parallel bestellt werden können, um Teilebeschaffungsrisiken zu verhindern oder um die Fahrzeuggesamtkosten zu optimieren. Bei einer solchen Teilungsform müssen im herkömmlichen System, in dem jede ECU **101** die Umschreibvorrichtung **102** wie früher authentifiziert, die technischen Informationen über die Authentifizierungsverarbeitung für externe ECU-Hersteller offenbart werden. Die vorliegende Erfindung hat den Vorteil, diesen Bedarf zu beseitigen.

[0039] Bei dem fahrzeugmontierten Netzwerksystem **1000** gemäß der ersten Ausführungsform hängt die Sicherheitsstufe des gesamten fahrzeugmontierten Netzwerkes von der Sicherheitsstärke des Authentifizierungs-Servers **103** ab. Daher besteht keine Gefahr, dass eine missbräuchliche ECU die Sicherheitsstufe des gesamten fahrzeugmontierten Netzwerkes im Vergleich zu dem Fall senkt, in dem wie früher jede ECU **101** die Authentifizierungsverarbeitung ausführt.

[0040] Wenn bei dem fahrzeugmontierten Netzwerksystem **1000** gemäß der ersten Ausführungsform die Authentifizierungsfunktion aktualisiert wird, falls ein neuer Missbrauch festgestellt worden ist, muss nur der Authentifizierungsalgorithmus des Authentifizierungs-Servers **103** umgeschrieben werden. Wenn jede ECU **101** die Authentifizierungsverarbeitung wie früher ausführt, muss der Authentifizierungsalgorithmus jeder ECU **101** umgeschrieben werden. Daher muss der Fahrzeugbetrieb angehalten werden, was für den Nutzer unangenehm ist. Gemäß der vorliegenden Erfindung steht die Operation des Authentifizierungs-Servers **103** nicht mit der typischen Fahrzeugsteuerung in Beziehung, weshalb der Authentifizierungsalgorithmus aktualisiert werden kann, ohne den Fahrzeugbetrieb anzuhalten. Selbst wenn beispielsweise das Fahrzeug fährt, wird ein Sicherheits-Patch über ein Telephonnetzwerk oder eine Internetverteilung verteilt und kann der Authentifizierungsalgorithmus umgeschrieben werden. Dadurch ist die Prozedur des Zurückrufens der Fahrzeuge für die Aktualisierung des Authentifizierungsalgorithmus nicht erforderlich, weshalb die Fahrzeuge nicht in einer Rückruf- oder Kundendienst-Kampagne zurückgeholt werden müssen, wodurch die Aktualisierungsarbeit bei geringen Aktualisierungskosten schnell ausgeführt wird.

<Zweite Ausführungsform>

[0041] In einer zweiten Ausführungsform wird eine beispielhafte spezifische Konfiguration des fahrzeugmontierten Netzwerksystems **1000**, das in der ersten Ausführungsform beschrieben worden ist, beschrieben.

[0042] Fig. 2 ist ein Diagramm zur Veranschaulichung der beispielhaften Konfiguration des fahrzeugmontierten Netzwerksystems **1000** gemäß der zweiten Ausführungsform. In Fig. 2 sind die Ziel-ECU **101** und der Authentifizierungs-Server **103** mit einem fahrzeugmontierten Netzwerk **105** wie etwa einem CAN verbunden und in dem Fahrzeug montiert.

[0043] Die Umschreibvorrichtung **102** ist mit dem fahrzeugmontierten Netzwerk **105** über einen Verbindungs-Fahrzeugverbinder **104**, der an der äußeren Oberfläche des Fahrzeugs vorgesehen ist, verbunden. Dadurch ist die Umschreibvorrichtung **102** mit der Ziel-ECU **101** verbunden, ohne dass die Ziel-ECU **101** aus dem Fahrzeug entnommen werden muss, und führt die Verarbeitung des Umschreibens des in der Ziel-ECU **101** gehaltenen Programms aus oder erfasst die internen Daten.

[0044] Fig. 3 ist ein Diagramm, das eine weitere beispielhafte Konfiguration des fahrzeugmontierten Netzwerksystems **1000** veranschaulicht. Bei der in Fig. 3 veranschaulichten Konfiguration ist zusätzlich zu dem fahrzeugmontierten Netzwerk **105** ein fahrzeugmontiertes Netzwerk **202** neu vorgesehen, wobei das fahrzeugmontierte Netzwerk **105** und das fahrzeugmontierte Netzwerk **202** über ein Kommunikations-Gateway **201** miteinander verbunden sind.

[0045] Die Ziel-ECU **101** ist unter der Steuerung des fahrzeugmontierten Netzwerkes **105** angeordnet und die Umschreibvorrichtung **102** sowie der Authentifizierungs-Server **103** sind unter der Steuerung des fahrzeugmontierten Netzwerkes **202** angeordnet. Die Erstere und die Letztere gehören zu unterschiedlichen Netzwerken. Das fahrzeugmontierte Netzwerk **105** und das fahrzeugmontierte Netzwerk **202** sind über das Kommunikations-Gateway **201** elektrisch miteinander verbunden, weshalb die Vorrichtungen miteinander kommunizieren können.

[0046] Fig. 4 ist ein Ablaufdiagramm, das eine Kommunikationsprozedur zwischen der Ziel-ECU **101** der Umschreibvorrichtung **102** und dem Authentifizierungs-Server **103** veranschaulicht. Es wird hier angenommen, dass die Umschreibvorrichtung **102** das in dem Flash-ROM in der Ziel-ECU **101** gespeicherte Programm umschreibt, um einen Rückruf aufgrund eines Fehlers in dem Programm anzusprechen. Jeder Schritt in Fig. 4 wird im Folgenden beschrieben.

(Fig. 4: Schritt S410)

[0047] Die Umschreibvorrichtung **102** und der Authentifizierungs-Server **103** führen einen Authentifizierungsablauf S410 aus, der in den Schritten S411 bis S415, die später beschrieben werden, erfolgt. Die Authentifizierungsfolge S410 entspricht den Schritten S101 bis S102 in Fig. 1. Dort ist ein Verfahren zum Authentifizieren

der Umschreibvorrichtung **102** durch die Verwendung einer digitalen Signatur auf der Grundlage beispielsweise eines Verschlüsselungssystems mit öffentlichem Schlüssel beschrieben, es könnte jedoch auch ein anderes Authentifizierungssystem verwendet werden. Übrigens wird angenommen, dass ein Paar aus einem öffentlichen Schlüssel und einem privaten Schlüssel im Voraus für die Umschreibvorrichtung **102** erzeugt worden ist und dass der öffentliche Schlüssel im Voraus an die Authentifizierungsvorrichtung **103** verteilt wird.

(Fig. 4: Schritt S411)

[0048] Die Umschreibvorrichtung **102** fordert den Authentifizierungs-Server **103** auf, die Umschreibvorrichtung als ein autorisiertes Endgerät zu authentifizieren, bevor sie eine Leseanforderung oder eine Schreibanforderung an die Ziel-ECU **101** ausgibt, etwa dann, wenn sie erstmals mit dem fahrzeugmontierten Netzwerk verbunden wird. Zu diesem Zeitpunkt wird ein Identifizierungscode der Umschreibvorrichtung **102** (oder ähnliche Informationen je nach Fall) gemeinsam übertragen, um dem Authentifizierungs-Server **103** die für die Umschreibvorrichtung **102** spezifischen Informationen zu demonstrieren.

(Fig. 4: Schritt S411: Ergänzung)

[0049] Das hier autorisierte Endgerät wird dadurch sichergestellt, dass die Umschreibvorrichtung **102** durch den Fahrzeughersteller autorisiert wird und nicht als falsch erklärt wird und dass die Umschreibvorrichtung **102** nicht durch eine andere Vorrichtung manipuliert wird.

(Fig. 4: Schritt S412)

[0050] Der Authentifizierungs-Server **103** führt eine Authentifizierungsbeginn-Verarbeitung aus. Spezifisch erzeugt er einen Typcode durch eine Pseudozufallszahl und leitet ihn zu der Umschreibvorrichtung **102** zurück. Ferner verwendet er den von der Umschreibvorrichtung **102** im Schritt S411 empfangenen Identifizierungscode, um den der Umschreibvorrichtung **102** entsprechenden öffentlichen Schlüsseln zu spezifizieren.

(Fig. 4: Schritt S413)

[0051] Die Umschreibvorrichtung **102** signiert durch ihren privaten Schlüssel den Typcode, der von dem Authentifizierungs-Server im Schritt S412 empfangen wird, und leitet ihn als einen signierten Code zu dem Authentifizierungs-Server **103** zurück.

(Fig. 4: Schritt S414)

[0052] Der Authentifizierungs-Server **103** liest den im Schritt S411 spezifizierten öffentlichen Schlüssel und verwendet ihn, um den von der Umschreibvorrichtung **102** im Schritt **413** empfangenen signierten Code zu decodieren. Der Authentifizierungs-Server **103** vergleicht das Decodierungsergebnis mit dem Typcode, der im Schritt S412 zu der Umschreibvorrichtung **102** übertragen wurde, und bestimmt dann, wenn beide übereinstimmen, dass die Umschreibvorrichtung **102** ein autorisiertes Endgerät ist. Der Authentifizierungs-Server **103** speichert Informationen, dass die Umschreibvorrichtung **102** autorisiert ist, in einer internen Liste authentifizierter Vorrichtungen. Wenn beide nicht übereinstimmen, wird die Umschreibvorrichtung **102** nicht authentifiziert.

(Fig. 4: Schritt S415)

[0053] Der Authentifizierungs-Server **103** überträgt als Bestätigungsantwort die Tatsache, dass die Authentifizierungsfolge S410 endet, an die Umschreibvorrichtung **102**. Zu dieser Zeit sind Informationen darüber, ob die Umschreibvorrichtung **102** authentifiziert ist, in der Bestätigungsantwort nicht enthalten. Der Grund ist der gleiche wie jener, der in Schritt S102 in der ersten Ausführungsform beschrieben worden ist.

(Fig. 4: Schritt S420)

[0054] Die Umschreibvorrichtung **102** überträgt eine Sitzungsbeginn-Anforderung zu der Ziel-ECU **101**. Der Schritt antwortet auf den Schritt S103 in **Fig. 1**. Es wird angenommen, dass die Sitzungsbeginn-Anforderung den Identifizierungscode der Umschreibvorrichtung **102** enthält.

(Fig. 4: Schritt S430)

[0055] Die Umschreibvorrichtung **102** und die Ziel-ECU **101** führen eine Authentifizierungsabfragefolge S430, die in den später beschriebenen Schritten S431 bis S432 erfolgt, aus. Die Authentifizierungsabfragefolge S430 entspricht den Schritten S104 bis S105 in Fig. 1.

(Fig. 4: Schritt S431)

[0056] Wenn die Ziel-ECU **101** die Sitzungsbeginn-Anforderung von der Umschreibvorrichtung **102** empfängt, beginnt sie mit der Verarbeitung der Bestätigung des Authentifizierungsergebnisses der Umschreibvorrichtung **102**. Die Ziel-ECU **101** verwendet den Identifizierungscode der Umschreibvorrichtung **102**, der im Schritt S420 empfangen wurde, um bei dem Authentifizierungs-Server **103** anzufragen, ob die Umschreibvorrichtung **102** authentifiziert ist.

(Fig. 4: Schritt S432)

[0057] Der Authentifizierungs-Server **103** gleicht ab, ob der im Schritt S431 empfangene Identifizierungscode der Umschreibvorrichtung **102** in der Liste authentifizierter Vorrichtungen eingetragen ist. Wenn der relevante Identifizierungscode gefunden wird, wird die Antwort, das die Umschreibvorrichtung **102** authentifiziert ist, an die Ziel-ECU **101** übertragen, wenn er hingegen nicht gefunden wird, wird die Antwort, dass die Umschreibvorrichtung **102** nicht authentifiziert ist, an die Ziel-ECU **101** übertragen.

(Fig. 4: Schritt S440)

[0058] Die Ziel-ECU **101** beginnt eine normale Sitzung mit der Umschreibvorrichtung **102**. Wenn die Ziel-ECU **101** die Antwort, dass die Umschreibvorrichtung **102** authentifiziert ist, im Schritt S432 empfängt, nimmt sie die Sitzungsbeginn-Anforderung von der Umschreibvorrichtung **102** an und gibt eine Sitzungsannahmemeldung zu der Umschreibvorrichtung **102** aus. Wenn sie im Schritt S432 die Antwort empfängt, dass die Umschreibvorrichtung **102** nicht authentifiziert ist, wird die Sitzungsbeginn-Anforderung von der Umschreibvorrichtung **102** abgelehnt. Beispielsweise wird die Sitzungsbeginn-Anforderung ignoriert und wird keine Antwort an die Umschreibvorrichtung **102** ausgegeben.

(Fig. 4: Schritt S450)

[0059] Als Ergebnis des Schrittes S440 wird eine Sitzung zwischen der Umschreibvorrichtung **102** und der Ziel-ECU **101** aufgebaut. Die Umschreibvorrichtung **102** führt die Verarbeitungen des Umschreibens des in der Ziel-ECU **101** gehaltenen Programms oder des Erfassens der internen Daten aus.

(Fig. 4: Schritt S460)

[0060] Nach einem normalen Beenden der Authentifizierungsfolge S410 und dem Eintragen der Umschreibvorrichtung **102** in die Liste authentifizierter Vorrichtungen hält der Authentifizierungs-Server **103** die Inhalte der Liste der authentifizierten Vorrichtungen unverändert als Vorbereitung für eine Abfrage von der Ziel-ECU **101**. Der Authentifizierungs-Server **103** verwirft die alte Liste authentifizierter Vorrichtungen anhand einer Referenz, dass die Liste authentifizierter Vorrichtungen während eines Fahrzyklus gehalten wird oder dass die Liste authentifizierter Vorrichtungen bis zum Verstreichen einer vorgegebene Zeit gehalten wird oder dass die Liste authentifizierter Vorrichtungen gehalten wird, bis der Zündschlüssel des Fahrzeugs in die Aus-Stellung gedreht wird.

(Fig. 4: Schritt S460: Ergänzung)

[0061] Der Fahrzyklus ist ein Konzept, das in der Fahrzeug-Selbstdiagnosetechnik wie etwa OBD-II (On-Board-Diagnostics, Second Generation, ISO-9141-2) präsentiert wird. Bei dieser Technik gibt der Fahrzyklus eine Periode an, die jeweils einen Motorstart (mit Ausnahme eines Starts nach einem automatischen Stopp des Motors in einem Fahrzeug mit automatischem Start/Stopp-System), einen Fahrzustand und einen Motorstoppzustand (mit Ausnahme eines automatischen Motorstopps in einem Fahrzeug mit automatischem Start/Stopp-System) umfasst.

[0062] Fig. 5 ist ein Ablaufdiagramm, das eine weitere Kommunikationsprozedur zwischen der Ziel-ECU **101**, der Umschreibvorrichtung **102** und dem Authentifizierungs-Server **103** veranschaulicht. Im Gegensatz zu Fig. 4

wird statt der Authentifizierungsfolge S410 eine Authentifizierungsfolge S510 verwendet, die ein einmaliges Passwort in einem Anforderungs- und Antwortsystem verwendet. Jeder Schritten Fig. 5 wird im Folgenden hauptsächlich anhand der Unterschiede zu Fig. 4 beschrieben.

(Fig. 5: Schritt S510)

[0063] Die Umschreibvorrichtung **102** und der Authentifizierungs-Server **103** führen die Authentifizierungsfolge S510, die aus den Schritten S511 bis S517, die später beschrieben werden, gebildet ist, aus. Es wird angenommen, dass eine im Voraus definierte Funktion, die in den später beschriebenen Schritten S513 bis S515 verwendet wird, im Voraus zwischen der Umschreibvorrichtung **102** und der Authentifizierungsvorrichtung **103** gemeinsam genutzt wird.

(Fig. 5: Schritt S511)

[0064] Dieser Schritt ist der gleiche wie der Schritt S411 in Fig. 4.

(Fig. 5: Schritt S512)

[0065] Der Authentifizierungs-Server **103** führt die Authentifizierungsbeginn-Verarbeitung aus. Insbesondere erzeugt er einen Typcode durch eine Zufallszahl und leitet ihn zu der Umschreibvorrichtung **102** zurück. Ferner verwendet er den von der Umschreibvorrichtung **102** im Schritt S511 empfangenen Identifizierungscode, um im Voraus die im Voraus definierte Funktion, die der Umschreibvorrichtung **102** entspricht, zu spezifizieren.

(Fig. 5: Schritte S513 bis S514)

[0066] Die Umschreibvorrichtung **102** wendet den im Schritt S512 empfangenen Typcode auf die im Voraus definierte Funktion an, um dadurch ein Rechenergebnis zu berechnen (S513). Die Umschreibvorrichtung **102** überträgt das Rechenergebnis an den Authentifizierungs-Server **103** (S514).

(Fig. 5: Schritt S515)

[0067] Der Authentifizierungs-Server **103** liest die im Schritt S512 spezifizierte im Voraus definierte Funktion und wendet denselben Code wie jenen, der an die Umschreibvorrichtung **102**. übertragen wird, im Schritt S515 auf die im Voraus definierte Funktion an, um dadurch ein Rechenergebnis zu berechnen.

(Fig. 5: Schritt S516)

[0068] Der Authentifizierungs-Server **103** vergleicht das von der Umschreibvorrichtung **102** im Schritt S514 empfangene Rechenergebnis mit dem im Schritt S515 berechneten Rechenergebnis. Wenn beide übereinstimmen, wird die Umschreibvorrichtung **102** als ein autorisiertes Endgerät bestimmt. Der Authentifizierungs-Server **103** speichert Informationen, dass die Umschreibvorrichtung **102** authentifiziert ist, in der internen Liste authentifizierter Vorrichtungen. Wenn beide nicht übereinstimmen, wird festgestellt, dass die Umschreibvorrichtung **102** nicht authentifiziert ist.

(Fig. 5: Schritt S517)

[0069] Der Authentifizierungs-Server **103** überträgt als eine Bestätigungsantwort die Tatsache, dass die Authentifizierungsfolge S510 endet, an die Umschreibvorrichtung **102**. Zu dieser Zeit sind Informationen darüber, ob die Umschreibvorrichtung **102** authentifiziert ist, in der Bestätigungsantwort nicht enthalten. Der Grund ist der gleiche wie im Schritt S102 in der ersten Ausführungsform beschrieben.

(Fig. 5: Schritte S520 bis S560)

[0070] Die Schritte sind die gleichen wie die Schritte S420 bis S460 in Fig. 4.

<Zweite Ausführungsform: Fazit>

[0071] Wie oben beschrieben, kann in dem fahrzeugmontierten Netzwerksystem **1000** gemäß der zweiten Ausführungsform der Authentifizierungs-Server **103** die Umschreibvorrichtung **102** durch die Verwendung einer digitalen Signatur anhand eines Verschlüsselungssystems mit öffentlichem Schlüssel authentifizieren. Das

Verschlüsselungssystem mit öffentlichem Schlüssel erfordert nicht, dass der private Schlüssel der Umschreibvorrichtung **102** über das Netzwerk offenbart wird, außerdem erfordert es nicht, dass der private Schlüssel der Umschreibvorrichtung **102** für den Authentifizierungs-Server **103** offenbart wird. Daher kann der private Schlüssel der autorisierten Umschreibvorrichtung **102** für Dritte vertraulich gehalten werden, wodurch die Sicherheit des fahrzeugmontierten Netzwerksystems **1000** gesteigert ist.

[0072] In dem fahrzeugmontierten Netzwerksystem **1000** gemäß der zweiten Ausführungsform kann der Authentifizierungs-Server **103** die Umschreibvorrichtung **102** durch die Verwendung des einmaligen Passworts in dem Anforderungs- und Antwortsystem authentifizieren. Bei dem einmaligen Passwort in dem Anforderungs- und Antwortsystem ändert sich der Typcode, der durch den Authentifizierungs-Server **103** erzeugt wird, jedes Mal, weshalb die im Voraus definierte Funktion, die von der Umschreibvorrichtung **102** und von dem Authentifizierungs-Server **103** gemeinsam genutzt wird, schwer vorherzusagen ist. Daher können die Inhalte der Authentifizierungsverarbeitung für Dritte vertraulich gehalten werden, wodurch die Sicherheit des fahrzeugmontierten Netzwerksystems **1000** gesteigert wird.

[0073] In dem fahrzeugmontierten Netzwerksystem **1000** gemäß der zweiten Ausführungsform kann das Kommunikations-Gateway **201**, das mit Bezug auf Fig. 3 beschrieben wurde, als der Authentifizierungs-Server **103** dienen. Wenn bei einer solchen Konfiguration jede der Authentifizierungsfolgen S410 und S510 in den Fig. 4 bzw. Fig. 5 scheitert, kann eine Kommunikation von der Umschreibvorrichtung **102** von dem fahrzeugmontierten Netzwerk **105**, zu dem die Ziel-ECU **101** gehört, elektrisch getrennt werden. Bei einer solchen Konfiguration ist für das Kommunikations-Gateway **201** eine so genannte Firewall-Funktion (Feuerschutzwand-Funktion) gegeben, weshalb die Gefahr eines Eindringens von außen in das fahrzeugmontierte Netzwerk verringert ist und dadurch die Sicherheit weiter gesteigert wird.

<Dritte Ausführungsform>

[0074] Nun wird eine Struktur gemäß einer dritten Ausführungsform der vorliegenden Erfindung beschrieben, in der der Authentifizierungs-Server **103** von dem fahrzeugmontierten Netzwerksystem **1000** getrennt ist, um zu verhindern, dass die Authentifizierungsverarbeitung gestört wird oder dass der Authentifizierungs-Server durch eine andere Vorrichtung manipuliert wird, um eine illegale Authentifizierungsverarbeitung auszuführen.

[0075] Gemäß den oben beschriebenen ersten und zweiten Ausführungsformen wird die Authentifizierungsverarbeitung in dem Authentifizierungs-Server **103** gemeinsam ausgeführt, um dadurch die Sicherheitsstufe zu erhöhen. Wenn jedoch die Sicherheitsfunktion des Authentifizierungs-Servers **103** gestört wird, kann die Sicherheit des gesamten fahrzeugmontierten Netzwerksystems **1000** gefährdet sein.

[0076] Beispielsweise wird angenommen, dass die Untrennbarkeit zwischen der Ziel-ECU **101** und dem Authentifizierungs-Server **103** unterbrochen wird und der Authentifizierungs-Server **103** manipuliert wird. Das heißt, der Authentifizierungs-Server **103** wird aus dem fahrzeugmontierten Netzwerk entnommen oder seine Verbindung mit dem fahrzeugmontierten Netzwerk wird gestört und die Ziel-ECU **101** wird durch die bösartige Umschreibvorrichtung **102** und eine dritte Vorrichtung, die als der Authentifizierungs-Server **103** manipuliert, betrogen.

[0077] Um die obige Situation zu vermeiden, sollte verhindert werden, dass die Verbindung zwischen der Ziel-ECU **101** und dem Authentifizierungs-Server **103** getrennt wird, außerdem sollte verhindert werden, dass die Kommunikation zwischen ihnen gestört wird. Die folgenden drei Mittel können verwendet werden, um diese Verwundbarkeit anzusprechen.

(Gegenmaßnahme 1: Gegenmaßnahme auf Seiten der Ziel-ECU **101**)

[0078] Die Ziel-ECU **11** überwacht ständig, ob die Verbindung mit dem Authentifizierungs-Server **103** sicher ist, wobei die Ziel-ECU **101** dann, wenn sie detektiert, dass sie von dem Authentifizierungs-Server **103** getrennt ist, eine Leseanforderung oder eine Schreibanforderung an Daten in dem Speicher von der Umschreibvorrichtung **102** ablehnt, selbst wenn sie die Anforderung empfängt.

(Gegenmaßnahme 2: Gegenmaßnahme auf Seiten des Authentifizierungs-Servers)

[0079] Der Authentifizierungs-Server **103** überwacht ständig, ob die Verbindung mit der Ziel-ECU **101** sicher ist, wobei der Authentifizierungs-Server **103** dann, wenn er detektiert, dass er von der Ziel-ECU **101** getrennt ist, bestimmt, dass die Netzwerkkonfiguration illegal geändert worden ist oder dass der Authentifizierungs-Server

103 aus dem fahrzeugmontierten Netzwerk entfernt worden ist. Zu diesem Zeitpunkt hält der Authentifizierungs-Server **103** die Authentifizierungsverarbeitung an und lehnt die Authentifizierung für irgendeine Anforderung von außen ab.

(Gegenmaßnahme 2: Gegenmaßnahme auf Seiten des Authentifizierungs-Servers **103**: Ergänzung)

[0080] Da der Authentifizierungs-Server **103** typischerweise die Verbindung mit mehreren ECUs überwacht, kann der Authentifizierungs-Server **103** nicht nur die Entfernung einer spezifischen ECU, sondern auch eine Änderung in der gesamten Netzwerkkonfiguration detektieren. Wenn eine illegale Änderung in der Netzwerkkonfiguration mit einer solchen Funktion detektiert wird, kann diese Tatsache anderen ECUs gemeldet werden oder kann eine Funktionsausfall-Situation, die durch die illegale Änderung verursacht wird, gemeldet werden.

(Gegenmaßnahme 3: Alarmauslösung)

[0081] Wenn detektiert wird, dass eine Vorrichtung als der Authentifizierungs-Server **103** in dem fahrzeugmontierten Netzwerk manipuliert, löst der Authentifizierungs-Server **103** endgültig eine Alarmnachricht wie etwa eine Meldung einer erzwungenen Unterbrechung zu der Ziel-ECU aus, um die Ziel-ECU vor einem illegalen Zugriff zu schützen.

[0082] Fig. 6 ist ein Diagramm, das eine Verarbeitungsfolge zur Bestätigung, ob die Verbindung zwischen dem Authentifizierungs-Server **103** und der Ziel-ECU **101** besteht, veranschaulicht. Hier ist ein Beispiel veranschaulicht, in dem der Authentifizierungs-Server **103** die Verbindung bestätigt. In der in Fig. 6 veranschaulichten Verarbeitungsfolge wird ein einmaliges Passwort auf der Grundlage des Anforderungs- und Antwortsystems verwendet, um die Verbindung zu bestätigen. Jeder in Fig. 6 veranschaulichte Schritt wird im Folgenden beschrieben:

(Fig. 6: Schritt S610)

[0083] Der Authentifizierungs-Server **103** und die Ziel-ECU **101** führen eine Verbindungsbestätigungsfolge S610, die aus den später beschriebenen Schritten S611 bis S619 gebildet ist, aus. Übrigens wird angenommen, dass die Ziel-ECU **101** und der Authentifizierungs-Server **103** im Voraus eine im Voraus definierte Funktion, die in den Schritten S612 bis S614, die später beschrieben werden, gemeinsam nutzen.

(Fig. 6: Schritte S611 bis S614)

[0084] Der Authentifizierungs-Server **103** beginnt die Verbindungsbestätigungsverarbeitung. Die Schritte werden in vorgegebenen Zeitintervallen periodisch begonnen, so dass die Verbindung periodisch bestätigt werden kann. Die spezifische Verarbeitungsprozedur ist die gleiche wie in den Schritten S512 bis S516, ein Unterschied besteht jedoch darin, dass die Verarbeitung zwischen dem Authentifizierungs-Server **103** und der Ziel-ECU **101** ausgeführt wird.

(Fig. 6: Schritt S615)

[0085] Der Authentifizierungs-Server **103** vergleicht das Rechenergebnis in der Ziel-ECU **101** mit dem Rechenergebnis in dem Authentifizierungs-Server **103**. Wenn beide übereinstimmen, wird bestätigt, dass die Verbindung zwischen dem Authentifizierungs-Server **103** und der Ziel-ECU **101** besteht, wobei ein Zeitgeber zum Messen eines Zeitablaufs zurückgesetzt wird. Wenn beide nicht übereinstimmen, wird bestimmt, dass die Verbindung nicht bestätigt werden kann.

(Fig. 6: Schritt S615: Ergänzung 1)

[0086] Da die Verbindungsbestätigungsverarbeitung periodisch aktiviert wird, sollte dann, wenn die Verbindung zwischen der Ziel-ECU **101** und dem Authentifizierungs-Server **103** besteht, die Verbindung zwischen ihnen in derselben Periode bestätigt werden. Wenn eine Periode, in der die Verbindung zwischen ihnen nicht bestätigt werden kann, eine vorgegebene Zeitablaufperiode überschreitet, bestimmt der Authentifizierungs-Server **103**, dass beide voneinander getrennt sind. Wenn die Verbindung zwischen ihnen in dem momentanen Schritt bestätigt wird, wird der Zeitgeber zum Messen einer Zeitablaufperiode zurückgesetzt.

(Fig. 6: Schritt S615: Ergänzung 2)

[0087] Wenn bestimmt wird, dass die Verbindung zwischen der Ziel-ECU **101** und dem Authentifizierungs-Server **103** getrennt ist, hält der Authentifizierungs-Server **103** die Authentifizierungsverarbeitung an und führt eine Schutzmaßnahme wie etwa die Ausgabe eines Alarms, dass die Netzwerkkonfiguration illegal geändert worden ist, aus.

(Fig. 6: Schritte S616 bis S618)

[0088] Um zu veranlassen, dass die Ziel-ECU **101** bestätigt, dass die Verbindung zwischen der Ziel-ECU **101** und dem Authentifizierungs-Server **103** besteht, verwendet der Authentifizierungs-Server **103** das Rechenergebnis, das durch Anwenden der im Voraus definierten Funktion erhalten wird, erneut auf das im Schritt S614 erhaltene Rechenergebnis an, um dieselbe Verarbeitung wie in den Schritten S612 bis S614 umgekehrt auszuführen.

(Fig. 6: Schritt S619)

[0089] Die Ziel-ECU **101** vergleicht das Rechenergebnis in der Ziel-ECU **101** mit dem Rechenergebnis in dem Authentifizierungs-Server **103**. Wenn beide übereinstimmen, wird bestätigt, dass die Verbindung zwischen dem Authentifizierungs-Server **103** und der Ziel-ECU **101** besteht, wobei der Zeitgeber zum Messen des Zeitablaufs zurückgesetzt wird. Wenn beide nicht übereinstimmen, wird angenommen, dass die Verbindung nicht bestätigt ist.

(Fig. 6: Schritt S619: Ergänzung)

[0090] Wenn bestimmt wird, dass die Verbindung zwischen der Ziel-ECU **101** und dem Authentifizierungs-Server **103** getrennt ist, lehnt die Ziel-ECU **101** eine Leseanforderung oder eine Schreibanforderung an den Daten in dem Speicher von der Umschreibvorrichtung **102** selbst dann ab, wenn sie eine solche empfangen hat.

[0091] Fig. 7 ist ein Diagramm, das eine weitere Verarbeitungsfolge zum Bestätigen, ob die Verbindung zwischen dem Authentifizierungs-Server **103** und der Ziel-ECU **101** besteht, veranschaulicht. Hier wird ein Beispiel veranschaulicht, in dem der Authentifizierungs-Server **103** die Verbindung wie in Fig. 6 bestätigt. In der in Fig. 7 veranschaulichten Verarbeitungsfolge wird die Verbindung unter Verwendung eines Nachrichten-ID-Sprungsystems bestätigt.

[0092] Das Nachrichten-ID-Springen ist ein System, in dem eine Nachricht, die einen vorgegebenen ID-Wert hat, an ein Ziel übertragen wird, wobei ein Ergebnis, das durch Verschieben des ID-Werts um denselben Wert auf der Sendeseite und auf der Empfangsseite erhalten wird, sowohl auf der Sendeseite als auch auf der Empfangsseite für eine gegenseitige Authentifizierung gegenseitig bestätigt wird. Jeder in Fig. 7 veranschaulichte Schritt wird im Folgenden beschrieben.

(Fig. 7: Schritt S710)

[0093] Der Authentifizierungs-Server **103** und die Ziel-ECU **101** führen eine Verbindungsbestätigungsfolge S710, die aus den später beschriebenen Schritten S717 bis S718 gebildet ist, aus. Es wird angenommen, dass ein in den später beschriebenen Schritten S712 bis S713 verwendeter Verschiebungswert im Voraus zwischen der Ziel-ECU **101** und der Authentifizierungsvorrichtung **103** gemeinsam genutzt wird.

(Fig. 7: Schritt S711)

[0094] Der Authentifizierungs-Server **103** überträgt eine Nachricht, die einen vorgegebenen ID-Wert hat, zu der Ziel-ECU **101**, um dadurch eine Anfrage bei der Ziel-ECU **101** auszulösen.

(Fig. 7: Schritt S712)

[0095] Die Ziel-ECU **101** verschiebt den ID-Wert, der von dem Authentifizierungs-Server **103** empfangen wird, unter Verwendung des vorher mit dem Authentifizierungs-Server **103** gemeinsam genutzten Verschiebungswerts und leitet ihn als eine ECU-seitige ID zu dem Authentifizierungs-Server **103** zurück.

(Fig. 7: Schritt S713)

[0096] Der Authentifizierungs-Server **103** verschiebt den an die Ziel-ECU **101** im Schritt S711 übertragenen ID-Wert unter Verwendung des mit der Ziel-ECU **101** gemeinsam genutzten Verschiebungswerts und sagt eine ECU-seitige ID voraus, die von der Ziel-ECU **101** zurückgeleitet werden soll.

(Fig. 7: Schritt S714)

[0097] Der Authentifizierungs-Server **103** vergleicht die ID auf ECU-Seite, die von der Ziel-ECU **101** im Schritt S712 übertragen wird, mit der im Schritt S713 vorhergesagten ID. Wenn beide übereinstimmen, wird bestätigt, dass die Verbindung zwischen dem Authentifizierungs-Server **103** und der Ziel-ECU **101** besteht, wobei der Zeitgeber zum Messen des Zeitablaufs zurückgesetzt wird. Wenn beide nicht übereinstimmen, wird angenommen, dass die Verbindung nicht bestätigt wird. Der Zeitablauf ist der gleiche wie in **Fig. 6**.

(Fig. 7: Schritt S714: Ergänzung)

[0098] Wenn bestimmt wird, dass die Verbindung zwischen der Ziel-ECU **101** und dem Authentifizierungs-Server **103** unterbrochen ist, hält der Authentifizierungs-Server **103** die Authentifizierungsverarbeitung an und führt eine Schutzmaßnahme wie etwa die Ausgabe eines Alarms, dass die Netzwerkkonfiguration illegal geändert worden ist, aus.

(Fig. 7: Schritte S715 bis S717)

[0099] Die Ziel-ECU **101** verwendet ihren gehaltenen vorgegebenen ID-Wert, um die gleiche Verarbeitung wie in den Schritten S711 bis S713 umgekehrt auszuführen, um zu bewirken, dass die Ziel-ECU **101** bestätigt, dass die Verbindung zwischen der Ziel-ECU **101** und dem Authentifizierungs-Server **103** besteht.

(Fig. 7: Schritt S718)

[0100] Die Ziel-ECU **101** vergleicht die ID auf Seiten des Servers, die von dem Authentifizierungs-Server **103** im Schritt S716 zurückgeleitet wird, mit der im Schritt S717 vorhergesagten ID. Wenn beide übereinstimmen, wird bestätigt, dass die Verbindung zwischen dem Authentifizierungs-Server **103** und der Ziel-ECU **101** besteht, wobei der Zeitgeber zum Messen des Zeitablaufs zurückgesetzt wird. Wenn beide nicht übereinstimmen, wird angenommen, dass die Verbindung nicht bestätigt wird.

(Fig. 7: Schritt S718: Ergänzung)

[0101] Wenn bestimmt wird, dass die Verbindung zwischen der Ziel-ECU **101** und dem Authentifizierungs-Server **103** getrennt ist, lehnt die Ziel-ECU **101** eine Leseanforderung oder eine Schreibanforderung an den Daten in dem Speicher von der Umschreibvorrichtung **102** selbst dann ab, wenn sie die Anforderung empfängt.

[0102] **Fig. 8** ist ein Diagramm zur Erläuterung der Operationen, wenn der Authentifizierungs-Server **103** eine Vorrichtung (nicht autorisiertes Endgerät **801**), das als der Authentifizierungs-Server **103** in dem fahrzeugmontierten Netzwerk manipuliert, detektiert. Jeder Schritt in **Fig. 8** wird im Folgenden beschrieben.

(Fig. 8: Schritt S801)

[0103] Das nicht autorisierte Endgerät **801** versucht, auf die Ziel-ECU **101** direkt zuzugreifen, ohne eine Authentifizierungsanforderung bei dem Authentifizierungs-Server **103** vorzunehmen. Das nicht autorisierte Endgerät **801** überträgt eine Sitzungsbeginn-Anforderung an die Ziel-ECU **101**.

(Fig. 8: Schritt S802)

[0104] Wenn die Ziel-ECU **101** die Sitzungsbeginn-Anforderung von dem nicht autorisierten Endgerät **801** empfängt, fragt sie bei dem Authentifizierungs-Server **103** an, ob das nicht autorisierte Endgerät **801** authentifiziert ist. Da zu diesem Zeitpunkt das fahrzeugmontierte Netzwerk typischerweise eine Buskonfiguration verwendet, erreicht die Abfrage jede Vorrichtung, die mit dem fahrzeugmontierten Netzwerk verbunden ist. Somit können der Authentifizierungs-Server **103** und das nicht autorisierte Endgerät **801** die Abfrage von der Ziel-ECU **101** auffangen.

(Fig. 8: Schritt S803)

[0105] Der Authentifizierungs-Server **103** meldet der Ziel-ECU **101**, dass das nicht autorisierte Endgerät **801** nicht authentifiziert ist.

(Fig. 8: Schritt S804)

[0106] Das nicht autorisierte Endgerät **801** beginnt mit der Vorbereitung einer Übertragung einer falschen Authentifizierungsmeldung zu der Ziel-ECU **101**. Das nicht autorisierte Endgerät **801** verhindert, dass die Nichtauthentifizierungsmeldung die Ziel-ECU **101** erreicht, indem sie ein Blockierungssignal sendet oder die Netzwerkverbindung zwischen der Ziel-ECU **101** und dem Authentifizierungs-Server **103** sofort anhält (nicht gezeigt), um zu verhindern, dass die von dem Authentifizierungs-Server **103** übertragene Nichtauthentifizierungsmeldung die Ziel-ECU **101** erreicht.

(Fig. 8: Schritt S805)

[0107] Das nicht autorisierte Endgerät überträgt die falsche Authentifizierungsmeldung zu der Ziel-ECU **101**, als ob sie der Authentifizierungs-Server **103** gesendet hätte. Zu diesem Zeitpunkt erreicht die falsche Authentifizierungsmeldung wie im Schritt S802 ebenfalls den Authentifizierungs-Server **103**. Daher kann der Authentifizierungs-Server **103** das Vorhandensein des nicht autorisierten Endgeräts **801** detektieren.

(Fig. 8: Schritt S806)

[0108] Die Ziel-ECU **101** empfängt die falsche Authentifizierungsmeldung und beginnt eine normale Sitzung mit dem nicht autorisierten Endgerät **801**. Zu diesem Zeitpunkt setzt sie eine Sitzungsannahmemeldung ab, die einen Identifizierungscode des nicht autorisierten Endgeräts **801** enthält.

(Fig. 8: Schritt S807)

[0109] Wenn der Authentifizierungs-Server **103** die falsche Authentifizierungsmeldung detektiert, meldet er der Ziel-ECU **101** eine erzwungene Unterbrechung. Somit beabsichtigt er, zu verhindern, dass das nicht autorisierte Endgerät **801** illegal die Daten in der Ziel-ECU **101** abfragt oder das Programm illegal neu schreibt.

(Fig. 8: Schritt S808)

[0110] Da selbst dann, wenn der Authentifizierungs-Server **103** die falsche Authentifizierungsmeldung im Schritt S807 nicht detektieren kann, die Ziel-ECU **101** die Sitzungsannahmemeldung absetzt, wenn sie mit dem nicht autorisierten Endgerät **801** die normale Sitzung beginnt, kann das Vorhandensein des nicht autorisierten Endgeräts **801** anhand einer solchen Tatsache detektiert werden. Da insbesondere die Sitzungsannahmemeldung den Identifizierungscode des nicht autorisierten Endgeräts **801** enthält, kann der Authentifizierungs-Server **103** ein Endgerät, das direkt und nicht über die Authentifizierungsverarbeitung auf die Ziel-ECU **101** zugreift, detektieren. Wenn der Authentifizierungs-Server **103** das nicht autorisierte Endgerät **801** detektiert, führt er dieselbe Verarbeitung wie im Schritt S807 aus.

(Fig. 8: Schritt S809)

[0111] Wenn die Ziel-ECU **101** die Meldung über die erzwungene Unterbrechung empfängt, beendet sie zwangsläufig die Kommunikationssitzung mit dem nicht autorisierten Endgerät **801**.

<Dritte Ausführungsform: Fazit>

[0112] Wie oben beschrieben, bestätigt in dem fahrzeugmontierten Netzwerksystem **1000** gemäß der dritten Ausführungsform der Authentifizierungs-Server **103** periodisch, ob die Kommunikation mit der Ziel-ECU **101** aufgebaut wird, wobei der Authentifizierungs-Server **103** dann, wenn er detektiert, dass die Verbindung unterbrochen ist, die Authentifizierungsverarbeitung anhält. Wenn daher der Authentifizierungs-Server **103** von dem fahrzeugmontierten Netzwerk illegal getrennt wird, kann die Authentifizierungsverarbeitung nicht ausgeführt werden, wodurch ein nicht autorisierter Zugriff verhindert wird.

[0113] Bei dem fahrzeugmontierten Netzwerksystem **1000** gemäß der dritten Ausführungsform bestätigt die Ziel-ECU **101** periodisch, ob die Kommunikation mit dem Authentifizierungs-Server **103** besteht, wobei die

Ziel-ECU **101** dann, wenn sie detektiert, dass die Verbindung unterbrochen ist, eine Leseanforderung und eine Schreibanforderung von der Umschreibvorrichtung **102** ablehnt. Somit können die gleichen Vorteile wie oben erhalten werden.

[0114] In dem fahrzeugmontierten Netzwerksystem **1000** gemäß der dritten Ausführungsform wird die Verbindung zwischen dem Authentifizierungs-Server **103** und der Ziel-ECU **101** in dem Anforderungs- und Antwortsystem oder in dem Nachrichten-ID-Verschiebungssystem bestätigt. Daher kann das Verbindungsbestätigungssystem dazwischen vor einem Dritten verborgen werden, so dass ein nicht autorisiertes Endgerät, das versucht, die Verbindungsbestätigungsprozedur zu kopieren, beseitigt werden kann. Der Nachrichten-ID-Verschiebungsbetrag kann im Voraus zwischen beiden Knoten, dessen Verbindung bestätigt werden soll, gemeinsam genutzt werden oder er kann geheim durch vorheriges Einfügen von Daten für den Verschiebungsbetrag in die erste Abfragenachricht gemeinsam genutzt werden.

[0115] Bei dem fahrzeugmontierten Netzwerksystem **1000** gemäß der dritten Ausführungsform überträgt der Authentifizierungs-Server **103** dann, wenn er eine Vorrichtung detektiert, die als der Authentifizierungs-Server **103** in dem fahrzeugmontierten Netzwerk manipuliert, eine Meldung für erzwungene Unterbrechung zu der Ziel-ECU **101**. Somit kann das nicht autorisierte Endgerät **801**, das einen nicht autorisierten Zugriff versucht, beseitigt werden, ohne die Verbindung zwischen dem Authentifizierungs-Server **103** und der Ziel-ECU **101** zu unterbrechen.

[0116] In der dritten Ausführungsform ist beschrieben worden, dass der Authentifizierungs-Server **103** die Verbindung bestätigt, es kann jedoch auch die Ziel-ECU **101** bestätigen. In jedem Fall bestätigen sowohl der Authentifizierungs-Server **103** als auch die Ziel-ECU **101** gegenseitig die Verbindung, wodurch die Verbindung genauer bestätigt wird.

<Vierte Ausführungsform>

[0117] Wenn gemäß den ersten bis dritten Ausführungsformen die Authentifizierung der Umschreibvorrichtung **102** erfolgt, kann der Authentifizierungs-Server **103** ein Sitzungsticket ausgeben, das die Berechtigung angibt, Daten aus der Ziel-ECU **101** zu lesen oder in diese zu schreiben. Die Ziel-ECU **101** kann eine Leseanforderung oder eine Schreibanforderung an die Umschreibvorrichtung **102**, die das Sitzungsticket mit der Berechtigung nicht hält, selbst dann ablehnen, wenn der Authentifizierungs-Server **103** die Umschreibvorrichtung **102** authentifiziert hat.

[0118] Das Sitzungsticket ist eine Kommunikationskennung, die nur zwischen dem Authentifizierungs-Server **103** und der Ziel-ECU **101** gemeinsam genutzt wird und angibt, dass die Umschreibvorrichtung **102** authentifiziert ist und die Berechtigung hat, in die Ziel-ECU **101** zu schreiben oder aus ihr zu lesen. Nur wenn die Umschreibvorrichtung **102** durch den Authentifizierungs-Server **103** authentifiziert ist, kann sie das Sitzungsticket erhalten.

[0119] Das Sitzungsticket gemäß der vierten Ausführungsform wird zusammen mit dem Verfahren gemäß den ersten bis dritten Ausführungsformen verwendet, wodurch die Sicherheit des fahrzeugmontierten Netzwerksystems **1000** weiter gesteigert wird.

<Fünfte Ausführungsform>

[0120] Fig. 9 ist ein Diagramm, das einen beispielhaften Verarbeitungsablauf veranschaulicht, der ausgeführt wird, wenn die Ziel-ECU **101** eine Sitzungsbeginn-Anforderung von der Umschreibvorrichtung **102** gemäß den ersten bis vierten Ausführungsformen empfängt. Da die Authentifizierungsverarbeitung gemeinsam in dem Authentifizierungs-Server **103** gemäß der vorliegenden Erfindung ausgeführt wird, sind die Verarbeitungen, die von der Ziel-ECU **101** auszuführen sind, vereinfacht. Hier ist ein Fall veranschaulicht, in dem die Umschreibvorrichtung **102** beispielsweise anfordert, das in dem Flash-ROM in der Ziel-ECU **101** gespeicherte Programm umzuschreiben. Im Folgenden wird jeder Schritt in Fig. 9 beschrieben.

(Fig. 9: Schritte S901 bis S902)

[0121] Die Ziel-ECU **101** führt die Verbindungsbestätigungsverarbeitung, die in Fig. 6 oder in Fig. 7 veranschaulicht ist, aus und bestimmt, ob die Verbindung mit dem Authentifizierungs-Server **103** besteht. Wenn die Ziel-ECU **101** detektiert, dass die Verbindung mit dem Authentifizierungs-Server **103** unterbrochen ist, geht

sie weiter zum Schritt S908, während dann, wenn bestätigt wird, dass die Verbindung besteht, die Ziel-ECU **101** zum Schritt S903 weitergeht.

(Fig. 9: Schritt S903)

[0122] Die Ziel-ECU **101** führt wiederholt die Schritte S901 bis S903 aus, bis von der Umschreibvorrichtung **102** die Sitzungsbeginn-Anforderung empfangen wird, wobei die Ziel-ECU **101** dann, wenn sie die Sitzungsbeginn-Anforderung empfängt, zum Schritt S904 weitergeht.

(Fig. 9: Schritte S904 bis S906)

[0123] Die Ziel-ECU **101** fragt bei dem Authentifizierungs-Server **103** das Authentifizierungsergebnis der Umschreibvorrichtung **102** ab. Wenn die Umschreibvorrichtung authentifiziert ist, geht die Verarbeitung weiter zum Schritt S906, um eine normale Sitzung mit der Umschreibvorrichtung zu beginnen und um eine Sitzungsannahmemeldung abzusetzen. Wenn die Umschreibvorrichtung nicht authentifiziert ist, geht die Verarbeitung weiter zum Schritt S908.

(Fig. 9: Schritt S907)

[0124] Die Ziel-ECU **101** beginnt eine Prozedur zum Verarbeiten der Schreibanforderung von der Umschreibvorrichtung **102**. Wenn der Authentifizierungs-Server **103** die Sitzungsannahmemeldung im Schritt S906 empfängt, kann er erkennen, dass die Ziel-ECU **101** begonnen hat, die Schreibanforderung zu verarbeiten. Da eine andere ECU keine Antwort geben kann, selbst wenn sie versucht, mit der Ziel-ECU **101** zu kommunizieren, während die Ziel-ECU **101** die Verarbeitung ausführt, kann der Authentifizierungs-Server **103** an andere ECUs im Rundsendeverfahren melden, dass die Ziel-ECU **101** momentan beschäftigt ist.

(Fig. 9: Schritt S908)

[0125] Die Ziel-ECU **101** bestimmt, dass eine Sicherheitsanomalie in dem fahrzeugmontierten Netzwerksystem **1000** auftritt und beendet erzwungen die Schreibanforderung von der Umschreibvorrichtung **102**. Wenn sie die Schreibanforderung nicht empfangen hat, verhindert sie einen späteren Empfang.

(Fig. 9: Schritt S909)

[0126] Auch nach dem Beginn des Schrittes S907 prüft die Ziel-ECU **101** periodisch eine Meldung über erzwungene Unterbrechung (Abbruchmeldung) von dem Authentifizierungs-Server **103**. Falls eine Abbruchmeldung erfolgt, wird die Verarbeitung zum Schritt S908 übersprungen, um die Schreibanforderung erzwungen zu beenden. Dies entspricht dem Schritt S809 in **Fig. 8**. Falls eine Abbruchmeldung nicht erfolgt, geht die Verarbeitung weiter zum Schritt S910.

(Fig. 9: Schritte S910 bis S911)

[0127] Die Ziel-ECU **101** verarbeitet die Schreibanforderung von der Umschreibvorrichtung **102** mittels einer vorgegebenen Verarbeitung.

[0128] Wenn die Schreibanforderung vollständig verarbeitet ist, endet der Verarbeitungsablauf, wenn sie jedoch bestehen bleibt, kehrt die Verarbeitung zum Schritt S909 zurück, um dieselbe Verarbeitung zu wiederholen.

<Fünfte Ausführungsform: Fazit>

[0129] Im Schritt S907 wird angenommen, dass die Ziel-ECU **101** die Daten in dem Flash-ROM umgeschrieben hat. Da das Steuerprogramm, das verwendet wird, um die Daten in dem Flash-ROM umzuschreiben, nicht in dem Flash-ROM gelassen werden kann, muss das Programm temporär in einen nichtflüchtigen Speicher wie etwa einen RAM entwickelt werden. In einem typischen Mikrocomputer ist die Kapazität des RAM viel kleiner als jene des Flash-ROM, so dass ein fortschrittliches Authentifizierungsprogramm oder Sicherheitsüberwachungsprogramm nicht zusammen mit dem Umschreibprogramm geladen werden kann.

[0130] Wenn Daten in den Flash-ROM geschrieben werden, muss eine vorgegebene Menge elektrischer Ladungen in die Speicherzellen im Flash-ROM eingegeben werden, was durch ein Steuerprogramm zeitlich mo-

dulierend ausgeführt wird. Somit muss die Verarbeitung im Schritt S907 aufgrund einer strikten Zeitbeschränkung innerhalb einer geplanten Zeit strikt abgeschlossen sein.

[0131] Um daher Verarbeitungslasten der Ziel-ECU **101** im Schritt S907 nur für die Schreibverarbeitung zu verringern, ist es nützlich, wenn die Authentifizierungsprozedur und die Sicherheitsüberwachungsprozedur nach den Sitzungsstarts in den Authentifizierungs-Server **103** übernommen werden.

<Sechste Ausführungsform>

[0132] Das Verfahren zum Umschreiben des Programms, das in der Ziel-ECU **101** vorgesehen ist, ist in den ersten bis fünften Ausführungsformen beschrieben worden, das Programm, das in dem Authentifizierungs-Server **103** gehalten wird, kann jedoch unter Verwendung desselben Verfahrens umgeschrieben werden. Dadurch wird der Authentifizierungsalgorithmus aktualisiert, damit er fortschrittlicher ist, um die Sicherheitsstufe zu erhöhen. Die Authentifizierungsverarbeitung kann ohne Umschreiben des Programms jeder ECU aktualisiert werden, was hinsichtlich der Kosten vorteilhaft ist.

[0133] Die Funktion des Authentifizierungs-Servers **103** hat keine Beziehung zu einer normalen Steueroperation jeder ECU, weshalb es vorteilhaft ist, wenn nur der Authentifizierungsalgorithmus umgeschrieben werden kann, ohne das fahrzeugmontierte Netzwerk anzuhalten oder den Fahrzeugbetrieb anzuhalten.

[0134] Die Verarbeitung des Umschreibens des Programms des Authentifizierungs-Servers **103** kann durch die Umschreibvorrichtung **102** wie in den ersten bis fünften Ausführungsformen ausgeführt werden. Die Authentifizierungsverarbeitung hat in diesem Fall keine Beziehung zu der Ziel-ECU **101** und erfolgt nur zwischen dem Authentifizierungs-Server **103** und der Umschreibvorrichtung **102**.

<Siebte Ausführungsform>

[0135] Fig. 10 ist ein Diagramm, das eine beispielhafte Netzwerktopologie des fahrzeugmontierten Netzwerkes, das in einem neuesten repräsentativen hochentwickelten Fahrzeug vorgesehen ist, veranschaulicht. Die Konfigurationen und Operationen des Authentifizierungs-Servers **103**, der Gateway-Vorrichtung **201** und jeder ECU sind die gleichen wie jene in den ersten bis sechsten Ausführungsformen.

[0136] In Fig. 10 sind vier Netzwerkgruppen vorgesehen, wobei jedes Netzwerk durch ein Kommunikations-Gateway (Gateway-ECU) **201**, das in Fig. 3 beschrieben ist, organisiert ist. In Fig. 10 wird eine sternartige Netzwerkanordnung um die Gateway-ECU **201** verwendet, es können jedoch mehrere Gateway-ECUs **201** vorgesehen sein, um eine Kaskadenverbindungsform zu verwenden.

[0137] Das fahrzeugmontierte Netzwerk, das in Fig. 10 veranschaulicht ist, ist mit einem Antriebsstrang-Netzwerk **301**, einem Systemnetzwerk **305** für Chassis/Sicherheit, einem Systemnetzwerk **309** für Karosserie/elektrische Komponenten und mit einem Systemnetzwerk **313** für AV/Informationen versehen.

[0138] Unter der Steuerung des Antriebsstrang-Netzwerkes **301** sind eine Motorsteuerungs-ECU **302**, eine AT-Steuerungs-ECU (Automatikgetriebesteuerungs-ECU) **303** und eine HEV-Steuerungs-ECU (Hybridelektrofahrzeugsteuerungs-ECU) **304** verbunden. Unter der Steuerung des Systemnetzwerkes **305** für Chassis/Sicherheit sind eine Bremssteuerungs-ECU **306**, eine Chassissteuerungs-ECU **307** und eine Lenksteuerungs-ECU **308** verbunden. Unter der Steuerung eines Systemnetzwerkes **309** für Karosserie/elektrische Komponenten sind eine Messgerätanzeige-ECU **310**, eine Klimaanlagensteuerungs-ECU **311** und eine Diebstahlverhinderungssteuerungs-ECU **312** verbunden. Unter der Steuerung des Systemnetzwerkes **313** für AV/Informationen sind eine Navigations-ECU **314**, eine Audio-ECU **315** und eine ETC/Telephon-ECU **316** verbunden.

[0139] Eine Kommunikationseinheit **317** außerhalb des Fahrzeugs ist mit der Gateway-ECU **201** über ein Informationsnetzwerk **322** außerhalb des Fahrzeugs verbunden, um Informationen zwischen dem Fahrzeug und der äußeren Umgebung auszutauschen. Die Kommunikationseinheit **317** außerhalb des Fahrzeugs ist mit einem ETC-Funk **318**, einem VICS-Funk (Fahrzeuginformations- und -kommunikationssystem-Funk) **319**, einem TV/FM-Funk **320** und einem Telephonfunk **321** verbunden.

[0140] Die Umschreibvorrichtung **102** ist konfiguriert, um als ein Knoten des fahrzeugexternen Informationsnetzwerkes **322** über den im Fahrzeug vorgesehen Verbindungsfahrzeug-Verbinder **104** verbunden zu werden. Sie kann jedoch lediglich mit anderen Netzwerken (dem Antriebsstrang-Netzwerk **301**, dem Systemnetzwerk **305** für Chassis/Sicherheit, dem Systemnetzwerk **309** für Karosserie/elektrische Komponenten und dem

Systemnetzwerk **313** für AV/Informationen) oder mit der Gateway-ECU **201** verbunden sein. Das heißt, ein elektrisches Signal muss nur die Ziel-ECU entweder direkt oder über die Gateway-ECU **201** unabhängig von der mechanischen Anordnung erreichen.

[0141] Die Daten oder das Programm in einer spezifischen fahrzeugmontierten ECU können von außerhalb über den Telephonfunk **321** umgeschrieben werden. In diesem Fall kann dasselbe Verfahren wie in den ersten bis sechsten Ausführungsformen verwendet werden, um die Vorrichtung, die die Schreibanforderung zu der fahrzeugmontierten ECU über ein Telephon ausgibt, zu authentifizieren.

[0142] Das Verfahren zum Umschreiben der Software der ECU über ein Telephonnetzwerk oder das Internet ist wichtig bei der Senkung der Kosten, um einen Fehler wie etwa einen Rückruf zu verringern, wobei erwartet wird, dass dies künftig üblich ist. Auch in diesem Fall kann die in der vorliegenden Erfindung offenbarte Technik ein nicht berechtigtes Eindringen in das fahrzeugmontierte Netzwerk verhindern und kann die Verteilung und das Umschreiben autorisierter (vor Falsifikation geschützter) Software sicherstellen.

[0143] Der Authentifizierungs-Server **103** ist direkt mit der Kommunikations-Gateway-ECU **201** in Fig. 10 verbunden, der Authentifizierungs-Server **103** kann jedoch über dem Netzwerk beliebig positioniert sein. Das heißt, er kann direkt mit einem anderen Netzwerk wie die Umschreibvorrichtung **102** verbunden sein, solange die Verbindung für elektrische Signale sichergestellt werden kann.

[0144] Ein Unterschied zu der Umschreibvorrichtung **102** besteht darin, dass die elektrische Trennung von der Ziel-ECU **101** (jeder ECU in Fig. 10) verhindert werden muss. Deswegen wird bevorzugt, dass die Kommunikations-Gateway-ECU **201** auch als Authentifizierungs-Server **103** dient. Der Grund hierfür besteht darin, dass dann, wenn der Authentifizierungs-Server **103** entfernt wird, eine gegenseitige Kommunikation über mehrere fahrzeugmontierte Netzwerke nicht erfolgen kann.

[0145] Die Erfindung, die von den Erfindern gemacht worden ist, ist oben anhand von Ausführungsformen beschrieben worden, die vorliegende Erfindung ist jedoch nicht auf die Ausführungsformen eingeschränkt und kann auf verschiedene Weise modifiziert werden, ohne vom Erfindungsgedanken abzuweichen.

[0146] Sämtliche Konfigurationen, Funktionen und Verarbeitungseinheiten oder Teile hiervon können in Hardware wie etwa in einer integrierten Schaltung verwirklicht sein oder sie können in Software wie etwa den Programmen für die Ausführung der jeweiligen Funktionen, die von dem Prozessor ausgeführt werden, verwirklicht sein. Die Informationen wie etwa Programme oder Tabellen für die Verwirklichung der jeweiligen Funktionen können in einer Speichervorrichtung wie etwa einem Speicher oder einer Festplatte oder in einem Speichermedium wie etwa einer IC-Karte oder einer DVD gespeichert sein.

Bezugszeichenliste

101	Ziel-ECU
102	Umschreibvorrichtung
103	Authentifizierungs-Server
104	Verbindungs-Fahrzeugverbinder
105	fahrzeugmontiertes Netzwerk
201	Kommunikations-Gateway
202	fahrzeugmontiertes Netzwerk
301	Antriebsstrang-Netzwerk
302	Motorsteuerungs-ECU
303	AT-Steuerungs-ECU
304	HEV-Steuerungs-ECU
305	Systemnetzwerkwerk für Chassis/Sicherheit
306	Bremssteuerungs-ECU
307	Chassis-Steuerungs-ECU
308	Lenksteuerungs-ECU

309	Systemnetzwerk für Karosserie/elektrische Komponenten
310	Messgerätanzeige-ECU
311	Klimaanlagensteuerungs-ECU
312	Diebstahlverhinderungssteuerungs-ECU
313	Systemnetzwerk für AV/Informationen
314	Navigations-ECU
315	Audio-ECU
316	ETC/Telephon-ECU
317	fahrzeugexterne Kommunikationseinheit
318	ETC-Funk
319	VICS-Funk
320	TV/FM-Funk
321	Telephonfunk
1000	fahrzeugmontiertes Netzwerksystem

ZITATE ENTHALTEN IN DER BESCHREIBUNG

Diese Liste der vom Anmelder aufgeführten Dokumente wurde automatisiert erzeugt und ist ausschließlich zur besseren Information des Lesers aufgenommen. Die Liste ist nicht Bestandteil der deutschen Patent- bzw. Gebrauchsmusteranmeldung. Das DPMA übernimmt keinerlei Haftung für etwaige Fehler oder Auslassungen.

Zitierte Patentliteratur

- JP 2010-23556 A [**0009**]

Zitierte Nicht-Patentliteratur

- ISO-9141-2 [**0061**]

Patentansprüche

1. Fahrzeugmontiertes Netzwerksystem, das umfasst:
eine fahrzeugmontierte Steuervorrichtung, die mit einem Speicher zum Speichern von Daten versehen ist; und
eine Authentifizierungsvorrichtung, die eine Kommunikationsvorrichtung authentifiziert, die eine Leseanforderung oder eine Schreibanforderung an Daten, die in dem in der fahrzeugmontierten Steuervorrichtung vorgesehen Speicher gespeichert sind, ausgibt,
wobei die Authentifizierungsvorrichtung eine Authentifizierungsverarbeitung an der Kommunikationsvorrichtung vornimmt und ein Ergebnis hält, bevor die Kommunikationsvorrichtung die Leseanforderung oder die Schreibanforderung ausgibt,
wobei die fahrzeugmontierte Steuervorrichtung bei der Authentifizierungsvorrichtung das Ergebnis der Authentifizierungsverarbeitung an der Kommunikationsvorrichtung abfragt, wenn die Leseanforderung oder die Schreibanforderung von der Kommunikationsvorrichtung empfangen wird, und
die Leseanforderung oder die Schreibanforderung annimmt, wenn die Authentifizierungsvorrichtung die Kommunikationsvorrichtung authentifiziert, oder
die Leseanforderung oder die Schreibanforderung ablehnt, wenn die Authentifizierungsvorrichtung die Kommunikationsvorrichtung nicht authentifiziert.

2. Fahrzeugmontiertes Netzwerksystem nach Anspruch 1, wobei die Authentifizierungsvorrichtung dann, wenn sie den Abschluss der Authentifizierungsverarbeitung an der Kommunikationsvorrichtung meldet, die Antwort überträgt, ohne in die Antwort Informationen darüber aufzunehmen, dass die Authentifizierung erfolgt ist.

3. Fahrzeugmontiertes Netzwerksystem nach Anspruch 1, wobei die Authentifizierungsvorrichtung als ein Kommunikations-Gateway arbeitet, um eine Kommunikation zwischen Vorrichtungen, die mit dem fahrzeugmontierten Netzwerksystem verbunden sind, weiterzuleiten.

4. Fahrzeugmontiertes Netzwerksystem nach Anspruch 3, wobei die Authentifizierungsvorrichtung die Kommunikation zwischen der fahrzeugmontierten Steuervorrichtung und der Kommunikationsvorrichtung weiterleitet und die Authentifizierungsvorrichtung dann, wenn die Kommunikationsvorrichtung in der Authentifizierungsverarbeitung an der Kommunikationsvorrichtung nicht authentifiziert wird, die Kommunikation von der Kommunikationsvorrichtung nicht zu der fahrzeugmontierten Steuervorrichtung weiterleitet.

5. Fahrzeugmontiertes Netzwerksystem nach Anspruch 1, wobei die fahrzeugmontierte Steuervorrichtung periodisch bestätigt, ob die Kommunikation mit der Authentifizierungsvorrichtung besteht, und die fahrzeugmontierte Steuervorrichtung dann, wenn die Verbindung mit der Authentifizierungsvorrichtung nicht bestätigt wird, die Leseanforderung oder die Schreibanforderung von der Kommunikationsvorrichtung ablehnt.

6. Fahrzeugmontiertes Netzwerksystem nach Anspruch 1, wobei die Authentifizierungsvorrichtung periodisch bestätigt, ob die Verbindung mit der fahrzeugmontierten Steuervorrichtung besteht, und die Authentifizierungsvorrichtung dann, wenn die Verbindung mit der fahrzeugmontierten Steuervorrichtung nicht bestätigt wird, die Kommunikationsvorrichtung in der Authentifizierungsverarbeitung an der Kommunikationsvorrichtung nicht authentifiziert.

7. Fahrzeugmontiertes Netzwerksystem nach Anspruch 1, wobei die Authentifizierungsvorrichtung periodisch bestätigt, ob die Verbindung mit der fahrzeugmontierten Steuervorrichtung besteht, und die Authentifizierungsvorrichtung dann, wenn die Verbindung mit der fahrzeugmontierten Steuervorrichtung nicht bestätigt wird, einen Alarm absetzt, der diese Tatsache angibt.

8. Fahrzeugmontiertes Netzwerksystem nach Anspruch 1, wobei die Authentifizierungsvorrichtung die Kommunikation zwischen der fahrzeugmontierten Steuervorrichtung und der Authentifizierungsvorrichtung überwacht und die Authentifizierungsvorrichtung dann, wenn sie eine Störung oder eine Blockade der Kommunikation zwischen der fahrzeugmontierten Steuervorrichtung und der Authentifizierungsvorrichtung durch eine weitere Vorrichtung detektiert oder wenn sie detektiert, dass eine weitere Vorrichtung als die Authentifizierungsvorrichtung manipuliert, einen Alarm absetzt, der diese Tatsache angibt.

9. Fahrzeugmontiertes Netzwerksystem nach Anspruch 1, wobei die Authentifizierungsvorrichtung dann, wenn die fahrzeugmontierte Steuervorrichtung und die Kommunikationsvorrichtung in Kommunikation stehen, nachdem die Kommunikationsvorrichtung in der Authentifizierungsverarbeitung authentifiziert worden ist, diese Tatsache an andere Vorrichtungen, die mit dem fahrzeugmontierten Netzwerksystem verbunden sind, meldet.

10. Fahrzeugmontiertes Netzwerksystem nach Anspruch 1, wobei die Authentifizierungsvorrichtung dann, wenn sie die Kommunikationsvorrichtung in der Authentifizierungsverarbeitung authentifiziert, eine Kommunikationskennung, die die Authentifizierung angibt, an die Kommunikationsvorrichtung verteilt,
die fahrzeugmontierte Steuervorrichtung dann, wenn sie die Leseanforderung oder die Schreibanforderung von der Kommunikationsvorrichtung empfängt, bestätigt, ob die Kommunikationsvorrichtung die Kommunikationskennung hält, und
die Leseanforderung oder die Schreibanforderung annimmt, wenn die Kommunikationsvorrichtung die Kommunikationskennung hält, oder
die Leseanforderung oder die Schreibanforderung ablehnt, wenn die Kommunikationsvorrichtung die Kommunikationskennung nicht hält.

11. Fahrzeugmontiertes Netzwerksystem nach Anspruch 1, wobei die Authentifizierungsvorrichtung konfiguriert ist, um eine Verarbeitungsprozedur, die in der Authentifizierungsverarbeitung ausgeführt wird, zu aktualisieren.

12. Fahrzeugmontiertes Netzwerksystem nach Anspruch 1, wobei die Authentifizierungsvorrichtung die Authentifizierungsverarbeitung durch Verifizieren einer digitalen Signatur auf der Grundlage eines Verschlüsselungssystems mit öffentlichem Schlüssel ausführt.

13. Fahrzeugmontiertes Netzwerksystem nach Anspruch 1, wobei die Authentifizierungsvorrichtung die Authentifizierungsverarbeitung in einem Anforderungs- und Antwortsystem ausführt.

14. Fahrzeugmontiertes Netzwerksystem nach Anspruch 5, wobei die fahrzeugmontierte Steuervorrichtung ein Anforderungs- und Antwortsystem oder ein Nachrichten-ID-Sprungsystem verwendet, um zu bestätigen, ob eine Verbindung mit der Authentifizierungsvorrichtung besteht.

15. Fahrzeugmontiertes Netzwerksystem nach Anspruch 6, wobei die Authentifizierungsvorrichtung ein Anforderungs- und Antwortsystem oder ein Nachrichten-ID-Sprungsystem verwendet, um zu bestätigen, ob eine Verbindung mit der fahrzeugmontierten Steuervorrichtung besteht.

Es folgen 9 Blatt Zeichnungen

Anhängende Zeichnungen

FIG. 1

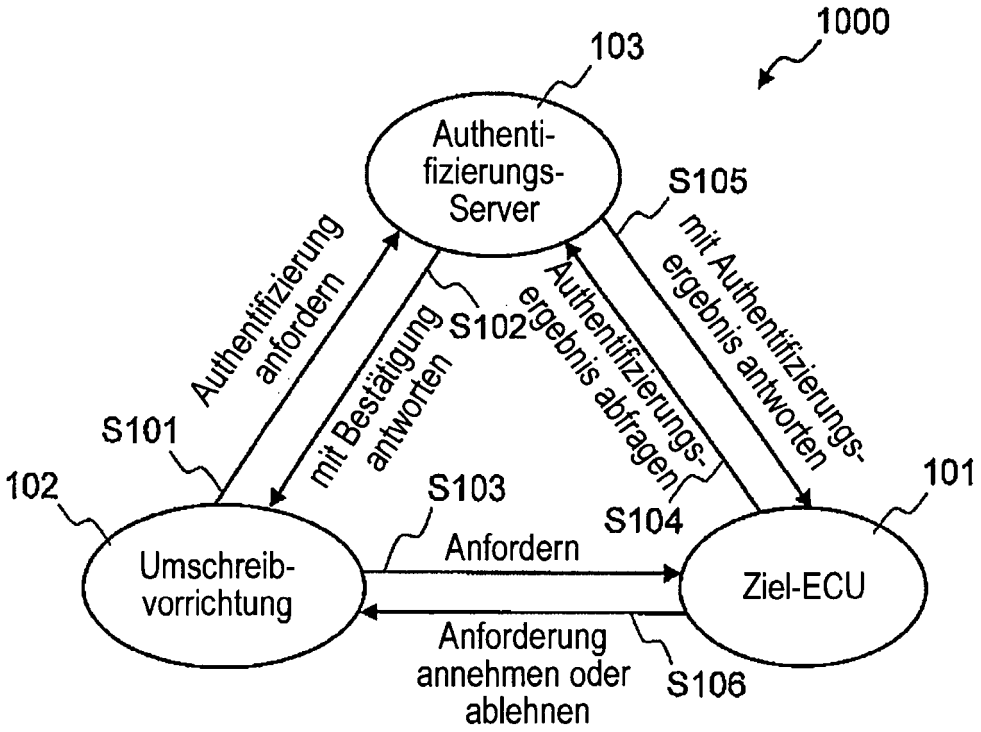


FIG. 2

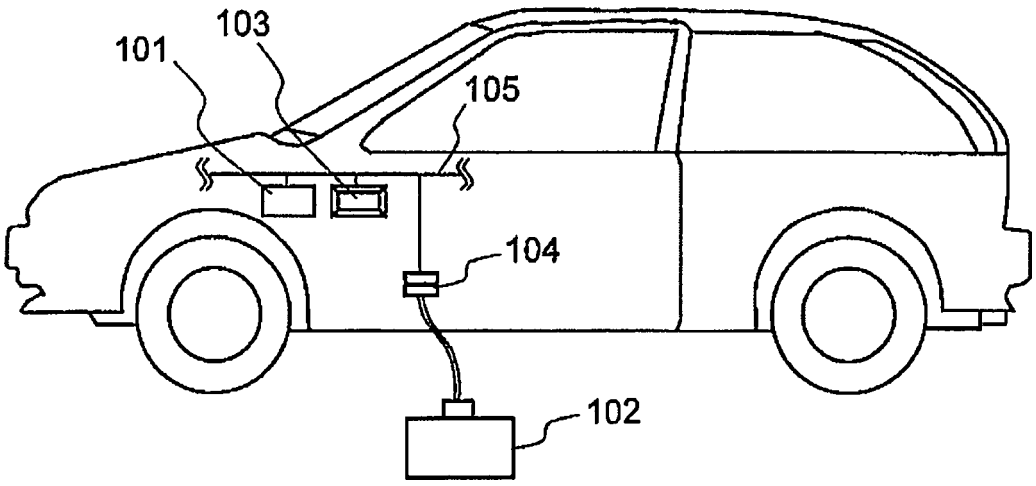


FIG. 3

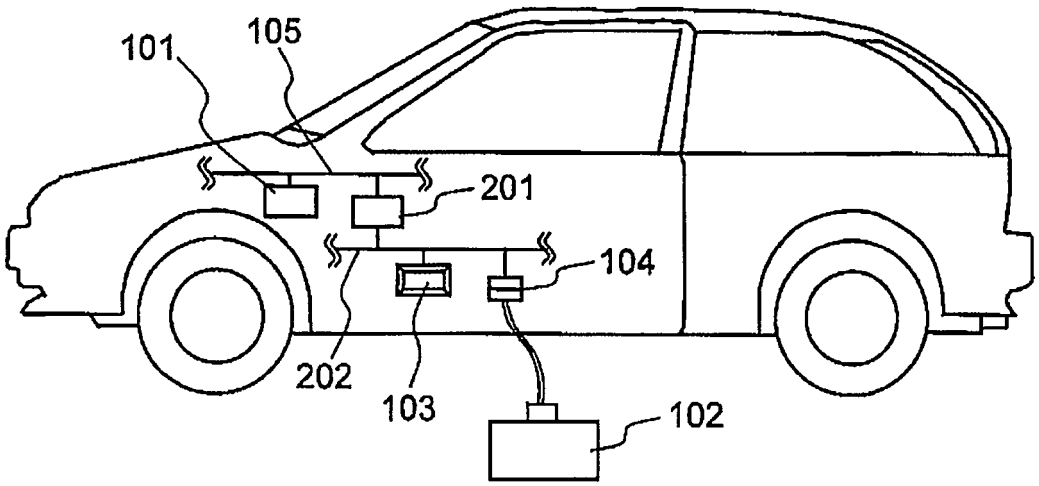


FIG. 4

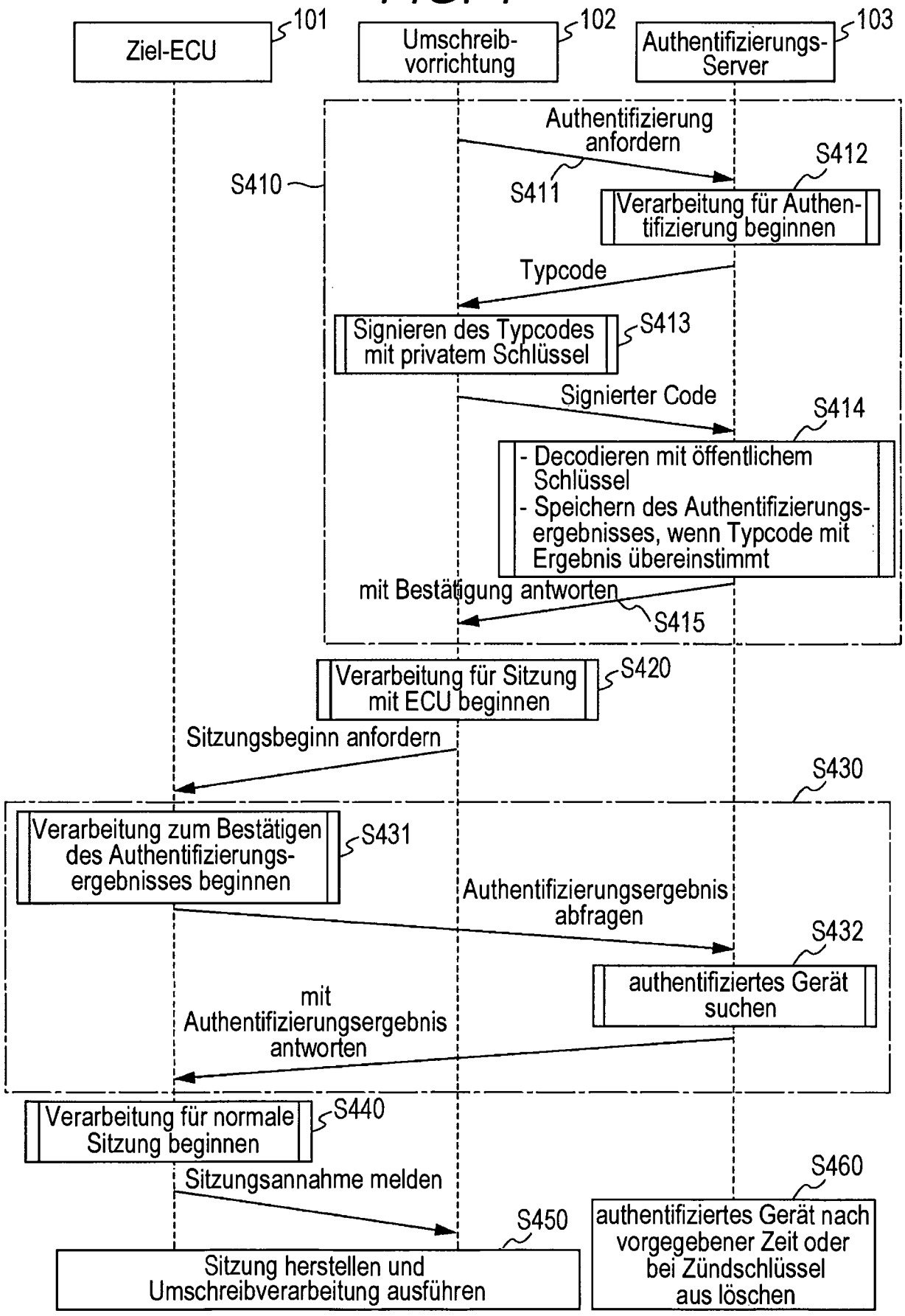

Ziel-ECU
101
Umschreib-vorrichtung
102
Authentifizierungs-Server
103
Authentifizierung anfordern
S411
S412
S410
Verarbeitung für Authen-tifizierung beginnen
Typcode
Signieren des Typcodes mit privatem Schlüssel
S413
Signierter Code
S414
- Decodieren mit öffentlichem Schlüssel
- Speichern des Authentifizierungs-ergebnisses, wenn Typcode mit Ergebnis übereinstimmt
mit Bestätigung antworten
S415
Verarbeitung für Sitzung mit ECU beginnen
S420
Sitzungsbeginn anfordern
S430
Verarbeitung zum Bestätigen des Authentifizierungs-ergebnisses beginnen
S431
Authentifizierungsergebnis abfragen
S432
authentifiziertes Gerät suchen
mit Authentifizierungsergebnis antworten
Verarbeitung für normale Sitzung beginnen
S440
Sitzungsannahme melden
S460
S450
Sitzung herstellen und Umschreibverarbeitung ausführen
authentifiziertes Gerät nach vorgegebener Zeit oder bei Zündschlüssel aus löschen

FIG. 5

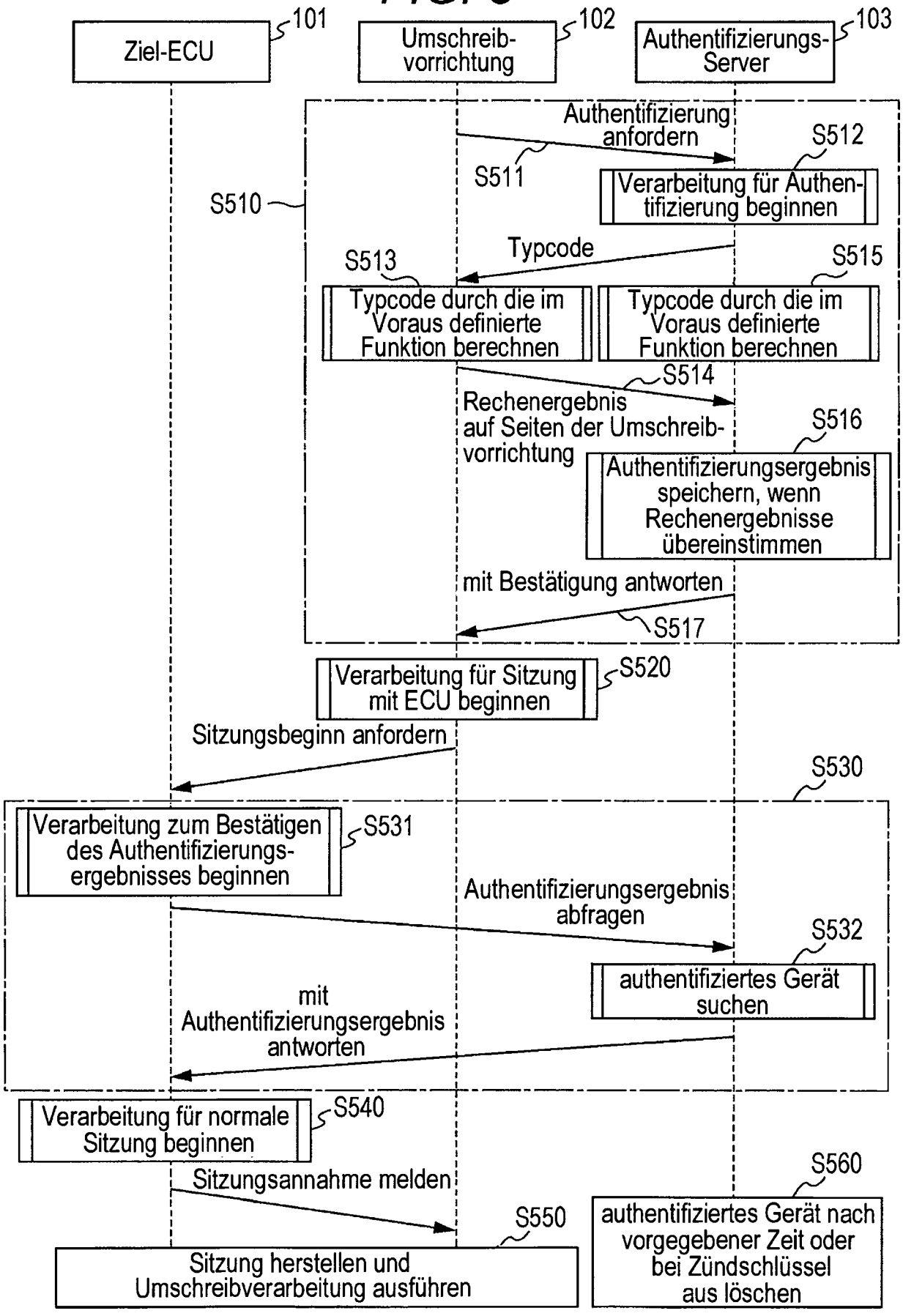

Ziel-ECU
101
Umschreib-vorrichtung
102
Authentifizierungs-Server
103
S510
Authentifizierung anfordern
S511
S512
Verarbeitung für Authen-tifizierung beginnen
Typcode
S513
S515
Typcode durch die im Voraus definierte Funktion berechnen
Typcode durch die im Voraus definierte Funktion berechnen
S514
Rechenergebnis auf Seiten der Umschreib-vorrichtung
S516
Authentifizierungsergebnis speichern, wenn Rechenergebnisse übereinstimmen
mit Bestätigung antworten
S517
Verarbeitung für Sitzung mit ECU beginnen
S520
Sitzungsbeginn anfordern
S530
Verarbeitung zum Bestätigen des Authentifizierungs-ergebnisses beginnen
S531
Authentifizierungsergebnis abfragen
S532
authentifiziertes Gerät suchen
mit Authentifizierungsergebnis antworten
Verarbeitung für normale Sitzung beginnen
S540
Sitzungsannahme melden
S550
Sitzung herstellen und Umschreibverarbeitung ausführen
S560
authentifiziertes Gerät nach vorgegebener Zeit oder bei Zündschlüssel aus löschen

FIG. 6

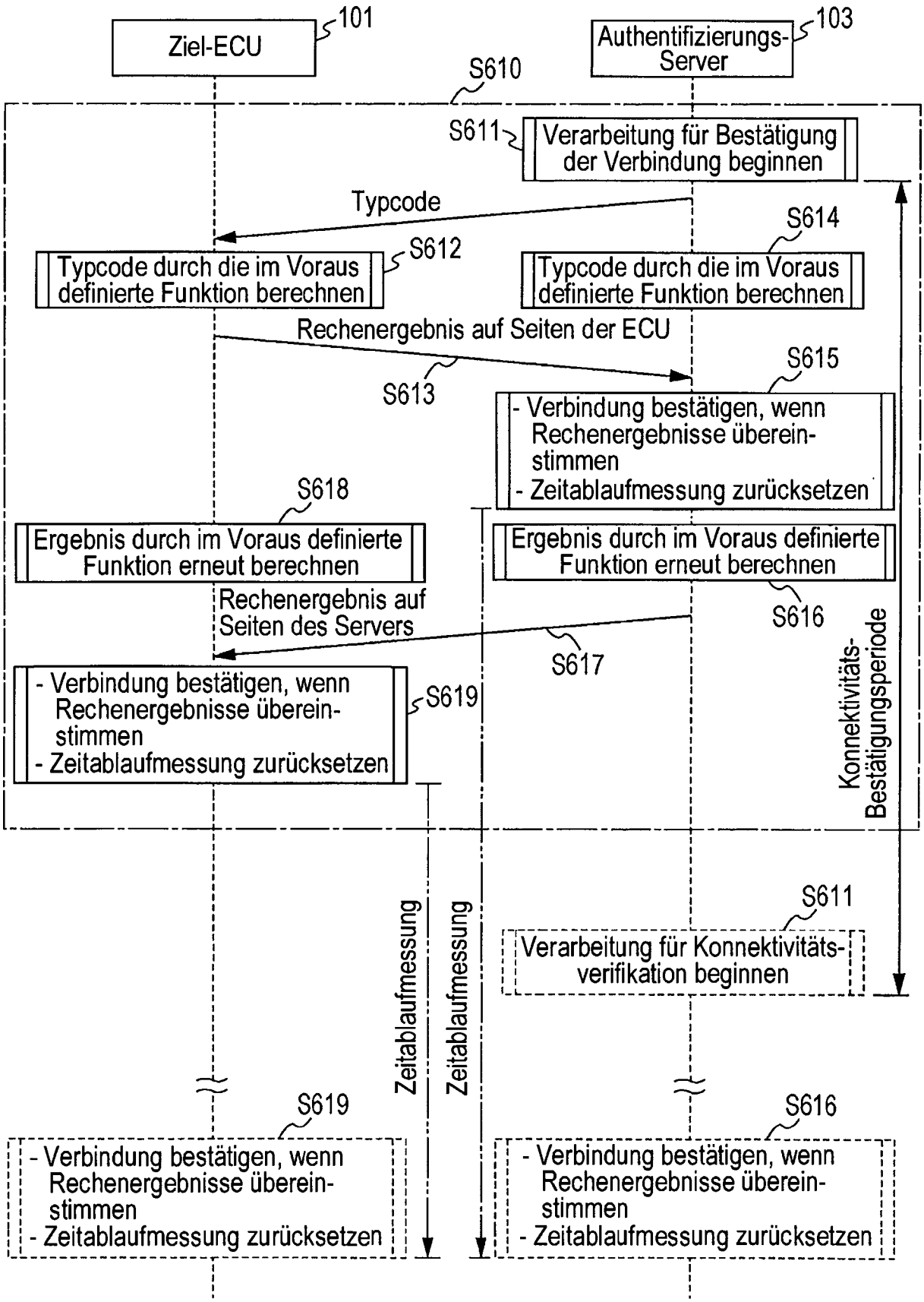

Ziel-ECU
101
Authentifizierungs-Server
103
S610
S611
Verarbeitung für Bestätigung der Verbindung beginnen
Typcode
S614
S612
Typcode durch die im Voraus definierte Funktion berechnen
Typcode durch die im Voraus definierte Funktion berechnen
Rechenergebnis auf Seiten der ECU
S613
S615
- Verbindung bestätigen, wenn Rechenergebnisse übereinstimmen
- Zeitablaufmessung zurücksetzen
S618
Ergebnis durch im Voraus definierte Funktion erneut berechnen
Ergebnis durch im Voraus definierte Funktion erneut berechnen
S616
Rechenergebnis auf Seiten des Servers
S617
- Verbindung bestätigen, wenn Rechenergebnisse übereinstimmen
- Zeitablaufmessung zurücksetzen
S619
Konnektivitäts-Bestätigungsperiode
Zeitablaufmessung
Zeitablaufmessung
S611
Verarbeitung für Konnektivitäts-verifikation beginnen
S619
- Verbindung bestätigen, wenn Rechenergebnisse übereinstimmen
- Zeitablaufmessung zurücksetzen
S616
- Verbindung bestätigen, wenn Rechenergebnisse übereinstimmen
- Zeitablaufmessung zurücksetzen

FIG. 7

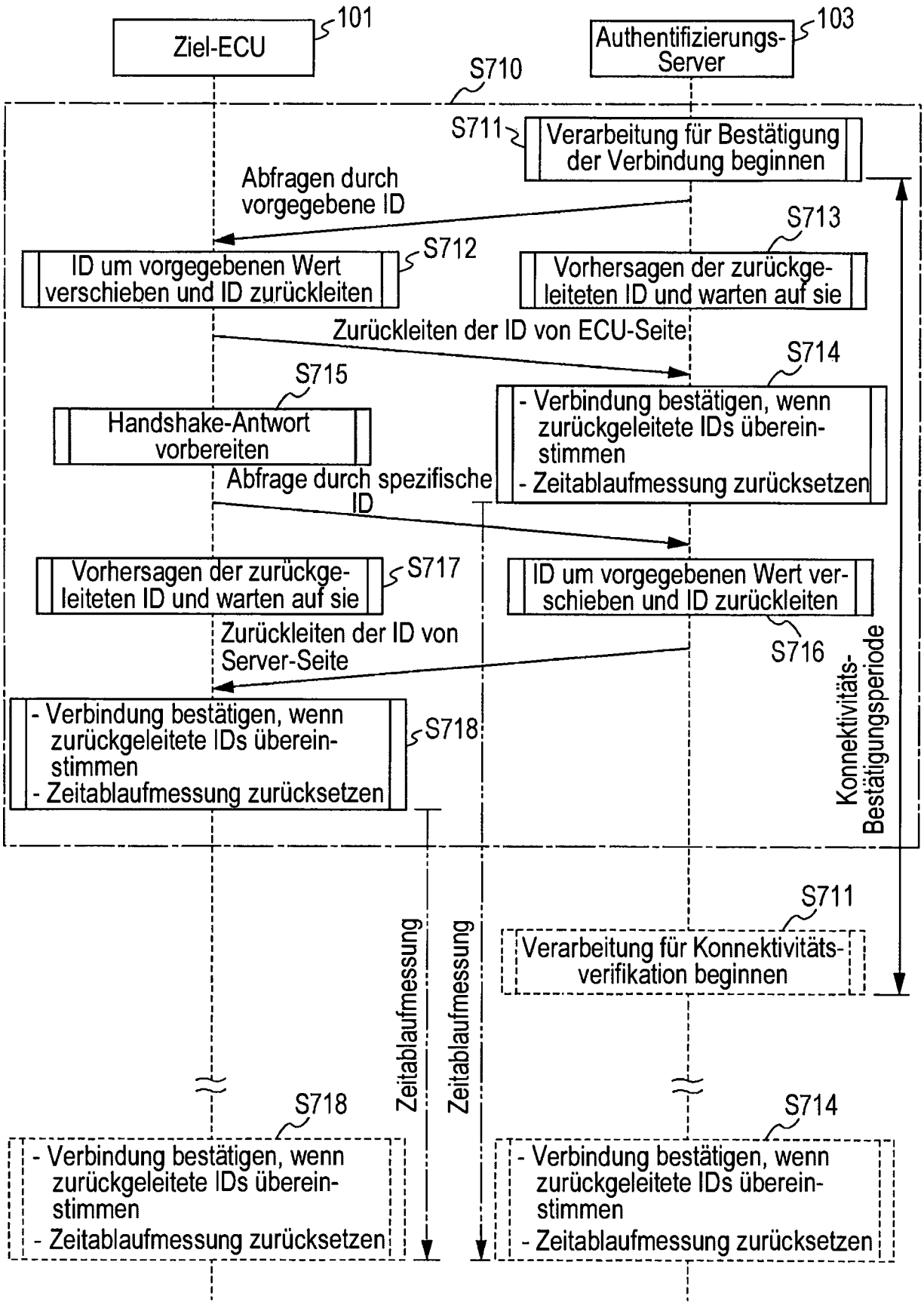

Ziel-ECU
101
Authentifizierungs-Server
103
S710
S711
Verarbeitung für Bestätigung der Verbindung beginnen
Abfragen durch vorgegebene ID
S713
S712
ID um vorgegebenen Wert verschieben und ID zurückleiten
Vorhersagen der zurückgeleiteten ID und warten auf sie
Zurückleiten der ID von ECU-Seite
S714
S715
Handshake-Antwort vorbereiten
- Verbindung bestätigen, wenn zurückgeleitete IDs übereinstimmen
- Zeitablaufmessung zurücksetzen
Abfrage durch spezifische ID
Vorhersagen der zurückgeleiteten ID und warten auf sie
S717
ID um vorgegebenen Wert verschieben und ID zurückleiten
S716
Zurückleiten der ID von Server-Seite
- Verbindung bestätigen, wenn zurückgeleitete IDs übereinstimmen
- Zeitablaufmessung zurücksetzen
S718
Konnektivitäts-Bestätigungsperiode
Zeitablaufmessung
Zeitablaufmessung
S711
Verarbeitung für Konnektivitäts-verifikation beginnen
S718
- Verbindung bestätigen, wenn zurückgeleitete IDs übereinstimmen
- Zeitablaufmessung zurücksetzen
S714
- Verbindung bestätigen, wenn zurückgeleitete IDs übereinstimmen
- Zeitablaufmessung zurücksetzen

FIG. 8

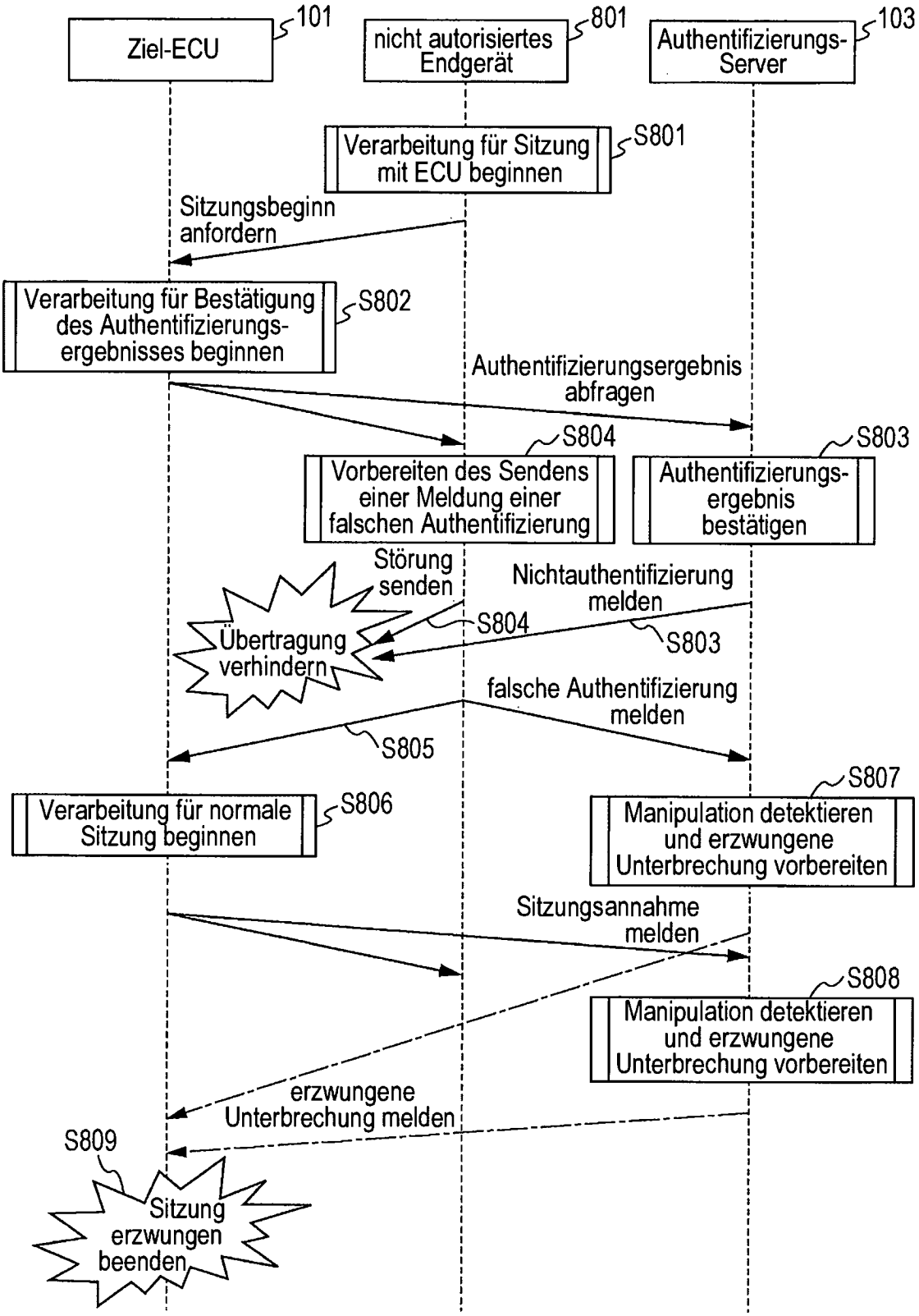

Ziel-ECU
101
nicht autorisiertes Endgerät
801
Authentifizierungs-Server
103
Verarbeitung für Sitzung mit ECU beginnen
S801
Sitzungsbeginn anfordern
Verarbeitung für Bestätigung des Authentifizierungs-ergebnisses beginnen
S802
Authentifizierungsergebnis abfragen
S804
S803
Vorbereiten des Sendens einer Meldung einer falschen Authentifizierung
Authentifizierungs-ergebnis bestätigen
Störung senden
Nichtauthentifizierung melden
S804
S803
Übertragung verhindern
falsche Authentifizierung melden
S805
S807
Verarbeitung für normale Sitzung beginnen
S806
Manipulation detektieren und erzwungene Unterbrechung vorbereiten
Sitzungsannahme melden
S808
Manipulation detektieren und erzwungene Unterbrechung vorbereiten
erzwungene Unterbrechung melden
S809
Sitzung erzwungen beenden

FIG. 9

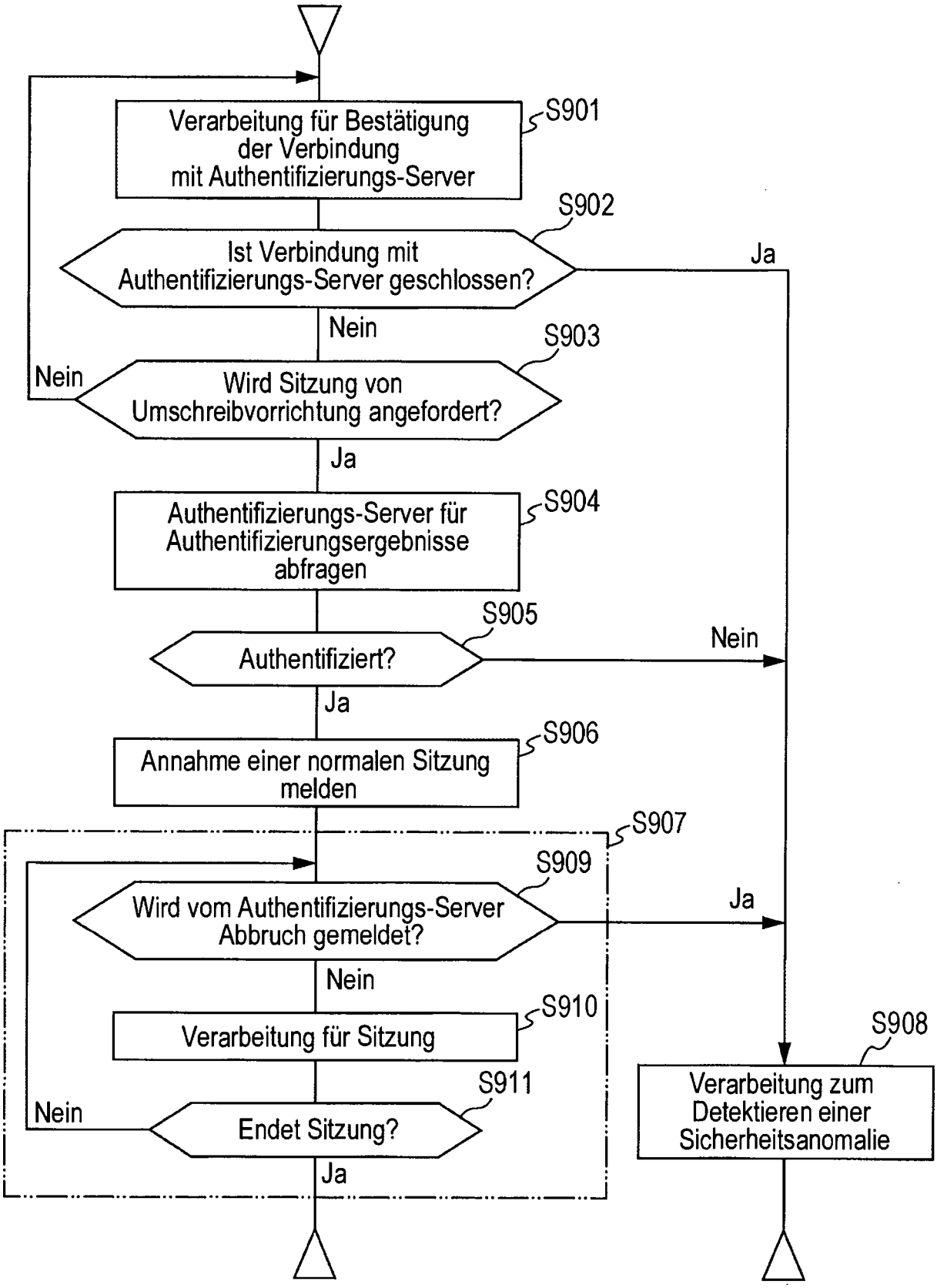
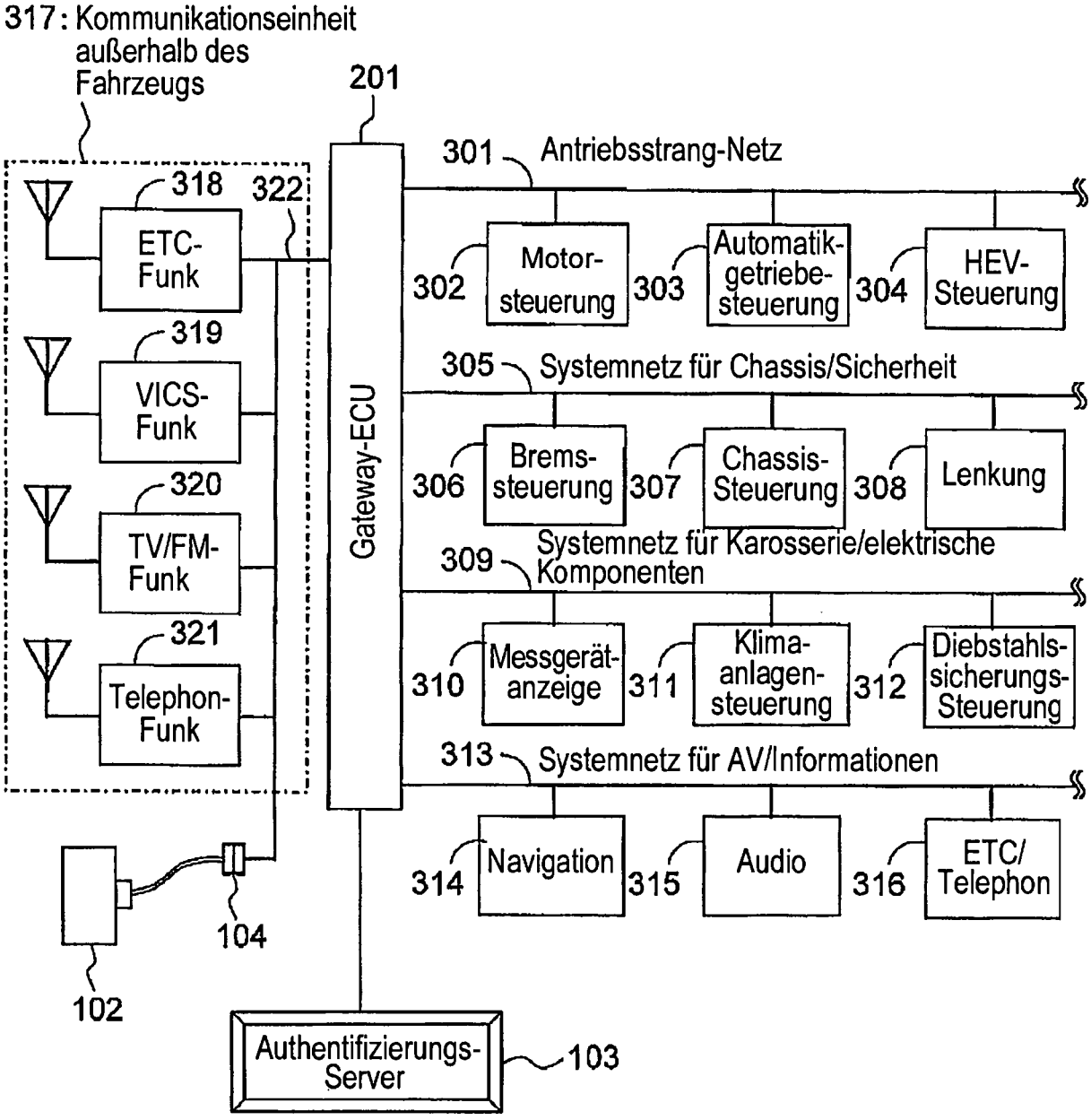

Verarbeitung für Bestätigung der Verbindung mit Authentifizierungs-Server
S901
Ist Verbindung mit Authentifizierungs-Server geschlossen?
S902
Ja
Nein
Wird Sitzung von Umschreibvorrichtung angefordert?
S903
Nein
Ja
Authentifizierungs-Server für Authentifizierungsergebnisse abfragen
S904
Authentifiziert?
S905
Nein
Ja
Annahme einer normalen Sitzung melden
S906
S907
Wird vom Authentifizierungs-Server Abbruch gemeldet?
S909
Ja
Nein
Verarbeitung für Sitzung
S910
Endet Sitzung?
S911
Nein
Ja
Verarbeitung zum Detektieren einer Sicherheitsanomalie
S908

FIG. 10


317: Kommunikationseinheit außerhalb des Fahrzeugs
201
Gateway-ECU
318
322
ETC-Funk
319
VICS-Funk
320
TV/FM-Funk
321
Telephon-Funk
104
102
301 Antriebsstrang-Netz
302 Motor-steuerung
303 Automatik-getriebe-steuerung
304 HEV-Steuerung
305 Systemnetz für Chassis/Sicherheit
306 Brems-steuerung
307 Chassis-Steuerung
308 Lenkung
309 Systemnetz für Karosserie/elektrische Komponenten
310 Messgerät-anzeige
311 Klima-anlagen-steuerung
312 Diebstahls-sicherungs-Steuerung
313 Systemnetz für AV/Informationen
314 Navigation
315 Audio
316 ETC/ Telephon
Authentifizierungs-Server
103