(19) österreichisches patentamt

(10) **AT 522625 A1 2020-12-15**

(12) Österreichische Patentanmeldung

(21) Anmeldenummer: A 50536/2019
(22) Anmeldetag: 14.06.2019
(43) Veröffentlicht am: 15.12.2020

(51) Int. Cl.: ***F02D 41/26*** (2006.01)
G06F 30/33 (2020.01)
G06F 30/20 (2020.01)
G06F 30/15 (2020.01)

(56) Entgegenhaltungen:
WO 2016170063 A1
EP 1150186 A1
WO 2017178015 A1
SCHULDT Fabian et al. "Effiziente systematische Testgenerierung für Fahrerassistenzsysteme in virtuellen Umgebungen" 10.07.2013; Technische Universität Braunschweig, Institut für Regelungstechnik & Vokswagen AG; abgerufen im Internet am 30.04.2020 unter dem Link <URL:https://publikationsserver.tu-braunschweig.de/servlets/MCRFileNodeServlet/dbbs_derivate_00031187/AAET_Schuldt_Saust_Lichte_Maurer_Scholz.pdf>
SPARSH Sharma et al. "A survey on Intrusion Detection Systems and Honeypot based proactive security mechanisms in VANETs and VANET Cloud" 20.04.2018; Vehicular Communications12 (2018); abgerufen im Internet am 30.04.2020 unter dem Link <https://www.sciencedirect.com/science/article/pii/S2214209617302784>

(71) Patentanmelder:
AVL List GmbH
8020 Graz (AT)

(72) Erfinder:
Priller Peter Dipl.Ing.
8111 Gratwein-Straßengel (AT)
Marksteiner Stefan
8076 Vasoldsberg (AT)

(74) Vertreter:
Patentanwälte Pinter & Weiss OG
1040 Wien (AT)

AT 522625 A1 2020-12-15

(54) Verfahren zur Sicherheitsüberprüfung einer Technikeinheit

(57) Auf einem Prüfcomputersystem (2) ausgeführtes Verfahren zur Sicherheitsüberprüfung einer Technikeinheit (1), wobei zumindest eine erste plausible Modellvariante und gegebenenfalls eine oder mehrere alternative Modellvarianten ermittelt werden und wobei das Verfahren die folgenden Schritte aufweist: Zuordnen bekannter Schwachstellen zu Komponenten der Modellvarianten, Definieren eines Angriffsziels, Erstellen zumindest eines auf das Angriffsziel bezogenen Angriffsmodells für jede Modellvariante, Gewichten der Knoten des Angriffsmodells hinsichtlich zumindest einer Bewertungsvariable, Ermitteln einer Bewertung zumindest eines Testvektors des Angriffsmodells hinsichtlich der Bewertungsvariable, Ermitteln eines Sicherheitswerts als pessimaler Werts aller Bewertungen und Ausgeben einer Sicherheitsbestätigung, wenn der Sicherheitswert einem Sicherheitskriterium entspricht.

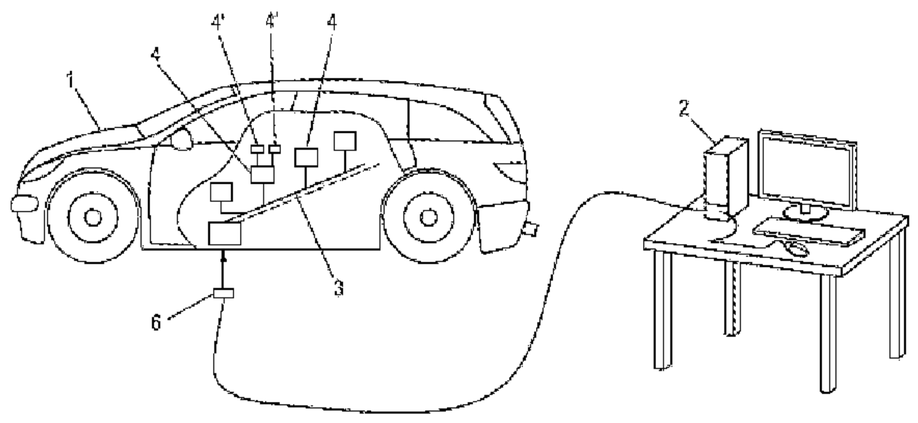

Fig. 1

Zusammenfassung

Auf einem Prüfcomputersystem (2) ausgeführtes Verfahren zur Sicherheitsüberprüfung einer Technikeinheit (1), wobei zumindest eine erste plausible Modellvariante und gegebenenfalls eine oder mehrere alternative Modellvarianten ermittelt werden und wobei das Verfahren die folgenden Schritte aufweist: Zuordnen bekannter Schwachstellen zu Komponenten der Modellvarianten, Definieren eines Angriffsziels, Erstellen zumindest eines auf das Angriffsziel bezogenen Angriffsmodells für jede Modellvariante, Gewichten der Knoten des Angriffsmodells hinsichtlich zumindest einer Bewertungsvariable, Ermitteln einer Bewertung zumindest eines Testvektors des Angriffsmodells hinsichtlich der Bewertungsvariable, Ermitteln eines Sicherheitswerts als pessimaler Werts aller Bewertungen und Ausgeben einer Sicherheitsbestätigung, wenn der Sicherheitswert einem Sicherheitskriterium entspricht.

Fig. 1

Verfahren zur Sicherheitsüberprüfung einer Technikeinheit

Die gegenständliche Offenbarung betrifft ein auf einem Prüfcomputersystem ausgeführtes Verfahren zur Sicherheitsüberprüfung einer Technikeinheit, ein Verfahren zur Ermittlung zumindest einer plausiblen Konfiguration einer Technikeinheit, ein Computerprogrammprodukt und ein Prüfcomputersystem.

Ab einem gewissen Komplexitätsgrad weisen moderne technische Geräte, insbesondere Fahrzeuge, eine Vielzahl an eingebetteten und untereinander vernetzten Komponenten auf, die jeweils mit eigenen Prozessoren oder Microcontrollern versehen sind. Die gegenständliche Offenbarung ist jedoch nicht nur auf Fahrzeuge beschränkt, sondern kann auch in Verbindung mit anderen Einheiten und technischen Geräten verwendet werden, die eine Vielzahl untereinander vernetzter Komponenten aufweisen, und die im Zusammenhang mit der gegenständlichen Offenbarung allgemein als „Technikeinheit“ bezeichnet werden. Zu Beispielen von Technikeinheiten zählen unter anderem Kombinationen unterschiedlicher Geräte. Beispielsweise können bestimmte Aufgaben von einer autonomen Computereinheit, wie etwa einem Tablet oder Smartphone, ausgeführt werden, das mit einer anderen Einheit, etwa einem (autonomen) Fahrzeug kommuniziert, z.B. als Fahrtenschreiber. Andererseits können auch mehrere Fahrzeuge untereinander z.B. über Funk kommunizieren, um gemeinsame Aufgaben auszuführen, etwa um im Sinne einer virtuellen Deichsel aneinandergekoppelt zu werden, oder es kann eine Einheit, beispielsweise ein Spezialfahrzeug im Baubereich, der Landwirtschaft, von Einsatzkräften etc., mit einem oder mehreren Onboard-Geräten verbunden sein. Solche kombinierten Einheiten können im Sinne der gegenständlichen Offenbarung als Technikeinheiten angesehen werden.

Üblicherweise verfügen die Komponenten einer solchen Technikeinheit über eigene Speicher und Kommunikationsschnittstellen und sie können daher jeweils als eigenes Computersystem betrachtet werden. Solche Komponenten werden auch als „Embedded Systems – ES“ oder „Cyber-Physical Systems – CPS“ bezeichnet. Die Komplexität solcher Technikeinheiten wird schnell unüberschaubar hoch. Beispielsweise weist ein Fahrzeug üblicherweise dutzende Steuergeräte auf, auf denen zusammen Software mit mehreren 10 Millionen Zeilen Programmcode ausgeführt wird. Als Beispiel für Kommunikationsschnittstellen können alleine die verschiedenen drahtlosen Verbindungsprotokolle angeführt werden, die teilweise gleichzeitig im Einsatz sind. Aufgrund der Komplexität und der vielfältigen Kommunikationsschnittstellen entsteht für solche Fahrzeuge eine große Angriffsfläche („Attack Surface“) für Cyber-Angriffe. Angriffe können dabei nicht nur über die eigentlichen Kommunikationsschnittstellen erfolgen, sondern beispielsweise auch über Sensoren, wie etwa einem LIDAR- oder Radarsystem. Diese könnten beispielsweise mit Fake Signals oder mittels DoS/flooding angegriffen werden.

Als „Cyber-Angriff“ wird im Zusammenhang mit der gegenständlichen Offenbarung ein von außen oder innen auf die Technikeinheit einwirkendes Ereignis bezeichnet, das das Ziel hat, die Technikeinheit in unzulässiger Weise zu beeinflussen und/oder Daten der Technikeinheit in unzulässiger Weise an Dritte weiterzuleiten.

Aufgrund der physikalischen Fähigkeiten von Fahrzeugen (Masse und Geschwindigkeit, damit hohe kinetische Energie, direkte Interaktion mit potentiell vielen Menschen), der großen Anzahl (Fahrzeugflotten) und der Entwicklung hin zu autonomen Fahrzeugen, können solche Angriffe ein enormes Gefährdungspotential entwickeln. Dies betrifft nicht nur die große Anzahl an Landfahrzeugen, wie etwa KFZ, LKW oder schienengebundene Fahrzeuge, sondern auch Wasser- oder Luftfahrzeuge.

Die gegenständliche Offenbarung beschäftigt sich mit dem Ziel, derartige Fahrzeuge und andere Technikeinheiten gegen Cyberattacken abzusichern und zu dessen Resilienz beizutragen. Als „Resilienz“ wird im Zusammenhang mit der gegenständlichen Offenbarung die Fähigkeit einer Technikeinheit bezeichnet, das beabsichtigte Ergebnis unabhängig von einwirkenden Ereignissen (wie etwa Cyber-Attacken) kontinuierlich zu erbringen.

Um Technikeinheiten gegen Cyberattacken abzusichern und resilient zu machen, gilt es, Schwachstellen in der Entwicklung möglichst zu verhindern, bzw. möglicherweise gefährdete Einzelkomponenten möglichst zu isolieren und redundante Sicherheitsmaßnahmen zu treffen. In der Konzeptphase geschieht das durch Architekturmaßnahmen (wie sie zum Beispiel in der Publikation "Secure Vehicular CommunicationSystems: Design and Architecture" von Papadimitratos, P., Buttyan, L., Holczer, T., Schoch, E., Freudiger, J., Raya, M., Ma, Z., Kargl, F., Kung, A., & Hubaux, J.-P., 2008, IEEE Communications Magazine, 46(11), 100-109, beschrieben sind), während der Umsetzung des Konzepts durch entsprechende Entwicklungsprozesse, wie etwa Best Practice, Source Code Review, etc.

Nach vollständigem Zusammenbau der Technikeinheit und der Integration der Komponenten in dieselbe ergibt sich in jedem Fall der Bedarf für einen Test bzw. eine Sicherheitsüberprüfung, um möglichst alle relevanten Schwachstellen (auch jene, die sich erst durch Kombination der Teilsysteme ergeben), finden zu können. Solch eine Sicherheitsprüfung wird auch als Cybersecurity-Test bezeichnet.

Um eine Schwachstelle finden zu können, ist es hilfreich, Kenntnisse über deren Existenz zu haben (allerdings existieren auch Techniken zum Auffinden von Schwachstellen, die kein Vorwissen erfordern, wie etwa Fuzzing). Die einer Sicherheitsprüfung zugrundeliegenden Schwachstellen können beispielsweise aus öffentlich frei zugänglichen oder kostenpflichtigen Datenbanken, oder aus internen Datenbanken erhalten werden. Interne Datenbanken können die im Zuge eigener Schwachstellen-Analysen entdeckten

Schwachstellen enthalten, manche bislang unentdeckten Schwachstellen werden auch im Darknet gegen Bezahlung angeboten.

Die Sicherheitsüberprüfung soll es Herstellern (z.B. „Original Equipment Manufacturer“ - OEM), staatlichen Stellen (z.B. Zulassungsbehörden), und anderen Interessensvertretern (z.B. Verbraucherverbände, kommerzielle Flottenbetreiber, etc.) ermöglichen, das konkrete Cybersecurity-Risiko einer Technikeinheit bzw. eines Fahrzeugs bewerten zu können. Dies kann bei der Weiterentwicklung bzw. Verbesserung der Fahrzeuge, für die Abnahme oder auch Zertifizierung und ähnliche Aufgaben zur Anwendung kommen.

Beispielsweise werden Sicherheitsüberprüfungen sowohl während der Entwicklung eines neuen Fahrzeugs beim OEM, bei der Markteinführung/Typisierung/Homologisierung, als auch später kontinuierlich während der gesamten Lebenszeit des Fahrzeugs benötigt. Die Notwendigkeit einer wiederholten Sicherheitsüberprüfung auf Systemtest-Ebene und damit der laufenden Überprüfung der Cybersicherheit ergibt sich aufgrund änderbarer Konfigurationen, laufender Updates von (Teilen der) Software, geänderter Umgebungsbedingungen (beispielsweise Vehicle-to-Infrastructure - V2I, Vehicle-to-Vehicle - V2V: Änderungen bei Interaktionspartnern), neu bekannt gewordener Testvektoren (auch aus eigener Sicherheitsforschung) etc. Die Sicherheitsüberprüfung kann dabei durch Hersteller, möglicherweise auch durch (Flotten)Betreiber, Zulassungsbehörden und spezialisierte Drittfirmen durchgeführt werden.

Aufgrund verteilter Entwicklung, Produktion, Konfiguration und Wartung in der automotiven Wertschöpfungskette kann bei der Sicherheitsüberprüfung nicht oder nur sehr eingeschränkt auf Wissen über die konkrete interne Implementierung der Technikeinheit zugegriffen werden. Vor allem für eine Sicherheitsüberprüfung durch andere Akteure als den Hersteller selbst, wie beispielsweise durch Anwender oder Behörden, sind die Systemarchitektur, Konfigurationsdaten, Sourcecodes, etc. der zu testenden Technikeinheit kaum bekannt. Die Sicherheitsüberprüfung entspricht daher weitgehend einem "Blackbox Testing" bzw. "Greybox Testing“, d.h. Tests, die ohne bzw. mit nur geringen oder teilweisen Kenntnissen über die innere Funktionsweise bzw. Implementierung der zu testenden Einheit entwickelt werden.

Damit ergibt sich das Problem, die passenden Testfälle und Test- bzw. Angriffsvektoren für die Sicherheitsüberprüfung auszuwählen. Durch die hohe Komplexität entsteht aufgrund der kombinatorischen Vielfalt eine extrem hohe Anzahl an Testfällen, die in der real zur Verfügung stehenden Zeit auch mit hochwertigen Computersystemen nicht vollständig abgearbeitet werden kann.

Die gegenständliche Erfindung hat daher die Aufgabe, Verfahren und Vorrichtungen bereitzustellen, mit denen die Anzahl an zu überprüfenden Testfällen auf ein technisch

bewältigbares Maß reduziert werden kann. Weiters soll die Sicherheitsüberprüfung weitgehend automatisiert durchführbar sein.

Diese und weitere Aufgaben werden durch ein Verfahren zur Ermittlung zumindest einer ersten plausiblen Modellvariante einer Konfiguration einer Technikeinheit mittels eines Prüfcomputersystems gelöst, wobei die Technikeinheit zumindest eine Datenübertragungseinrichtung und eine Vielzahl an Komponenten aufweist, welche zu einer Datenkommunikation über die Datenübertragungseinrichtung befähigt sind, und wobei das Verfahren die folgenden Schritte aufweist:

- Herstellen einer Verbindung zwischen einer Prüfschnittstelle des Prüfcomputersystems und der Datenübertragungseinrichtung der Technikeinheit,
- Ermitteln einer initialen Instanz eines Modells der Konfiguration der Technikeinheit,
- Entwickeln von spezifizierten Instanzen des Modells ausgehend von der initialen Instanz durch eine Abfolge von Spezifizierungsvorgängen, die jeweils zumindest die folgenden Schritte aufweisen:
    - Gegebenenfalls Ausführen einer Herausforderungsaktion,
    - Ermitteln eines für die Technikeinheit charakteristischen Verhaltens,
    - Analysieren des charakteristischen Verhaltens und Rückschließen auf zumindest ein Merkmal der tatsächlichen Konfiguration der Technikeinheit,
    - spezifizieren des Modells mit dem zumindest einem ermittelten Merkmal,

  wobei zumindest ein Spezifizierungsvorgang von dem Prüfcomputersystem automatisiert ausgeführt wird, und
- Identifizieren einer spezifizierten Instanz des Modells als die erste plausible Modellvariante, wenn zumindest eine Bestimmtheitsbedingung erfüllt ist.

Mithilfe dieses Verfahrens ist es möglich, die kombinatorische Vielfalt an Testfällen, die für eine Sicherheitsüberprüfung getestet werden müssen, auf eine Anzahl zu reduzieren, die mithilfe des Prüfcomputersystems in einem zur Verfügung stehenden Zeitraum vollständig abgearbeitet werden kann, um das Vorliegen einer Sicherheitsbestätigung für die Technikeinheit zu überprüfen.

Als „Komponente“ der Technikeinheit wird im Zusammenhang mit der gegenständlichen Offenbarung eine mit zumindest einem elektronischen Schaltkreis (insbesondere einem integrierten Schaltkreis, gegebenenfalls mit einem Prozessor, Microcontroller, einem FPGA, einem künstlichen neuronalen Netz, oder ähnliches) versehene Einheit bezeichnet, die über eine Datenkommunikationsfähigkeit verfügt und die, direkt oder indirekt, an zumindest eine Datenübertragungseinrichtung der Technikeinheit angeschlossen ist. Die Komponenten

können gemäß der gegenständlichen Offenbarung in einem engeren Sinn auch als „elektronische Komponenten“ oder „Daten verarbeitende Komponenten“ bezeichnet werden.

Als „Unterkomponente“ der Technikeinheit wird im Zusammenhang mit der gegenständlichen Offenbarung eine Komponente bezeichnet, die entweder an eine einzige Komponente angeschlossen ist, oder die – unabhängig von der Art der Datenkommunikation – einer einzigen Komponente zugeordnet ist.

Als „Datenübertragungseinrichtungen“ werden im Zusammenhang mit der gegenständlichen Offenbarung allgemein Mittel bezeichnet, die eine Übertragung von Daten von einem Sender (z.B. eine Komponente, Unterkomponente oder eine externe Datenquelle) zu einem Empfänger (z.B. eine Komponente, Unterkomponente oder einer externen Datensenke) ermöglichen. Datenübertragungseinrichtungen können entweder kabelgebunden oder kabellos sein, wobei die Datenkommunikation über die jeweilige Datenübertragungseinrichtung gemäß einem definierten Verbindungsprotokoll ausgeführt wird. Zu Beispielen von kabellosen Verbindungsprotokolle zählen beispielsweise, ohne darauf beschränkt zu sein, 3G/4G/5G Mobilnetz, Bluetooth, WLAN, V2X, RFID, etc. Zu Beispielen von Kabelgebundenen Verbindungsprotokollen zählen beispielsweise CAN, FlexRay, MOST, (Automotive) Ethernet, etc.

Als „Prüfcomputersystem“ wird im Zusammenhang mit der gegenständlichen Offenbarung ein beliebiges Computersystem bezeichnet, über das die entsprechenden Schritte der hierin offenbarten Verfahren ausgeführt werden.

Als „Prüfschnittstelle“ wird im Zusammenhang mit der gegenständlichen Offenbarung eine Datenverbindung zwischen dem Prüfcomputersystem und der Datenübertragungseinrichtung der Technikeinheit bezeichnet. Die Prüfschnittstelle kann ein beliebiges Verbindungsprotokoll nutzen, das eine solche Kommunikation erlaubt. Beispielsweise kann die Prüfschnittstelle eine kabellose oder kabelgebundene Schnittstelle sein. Die Prüfschnittstelle kann gegebenenfalls auch mehrere unterschiedliche Verbindungsprotokolle unterstützen, beispielsweise wenn das von einer Datenübertragungseinrichtung der Technikeinheit genutzte Verbindungsprotokoll anfänglich unbekannt ist. Als Schnittstellen können beispielsweise USB-Schnittstellen, Bluetooth-Schnittstellen oder Diagnoseschnittstellen der Technikeinheit verwendet werden. Das Herstellen einer Verbindung zwischen der Prüfschnittstelle und der Datenübertragungseinrichtung kann beispielsweise über herkömmliche Steckerverbindungen oder kabellos erfolgen. Als „Herstellen einer Verbindung“ wird in diesem Zusammenhang jeglicher Vorgang bezeichnet, der dem Prüfcomputersystem eine Datenkommunikation mit der Datenübertragungseinrichtung ermöglicht. Gegebenenfalls kann das Prüfcomputersystem mehrere voneinander unabhängige Prüfschnittstellen aufweisen.

Als „Konfiguration“ wird im Zusammenhang mit der gegenständlichen Offenbarung eine definierte Gruppe an Merkmalen der Technikeinheit bezeichnet, wobei die Gruppe insbesondere die folgenden Merkmale enthalten kann:

- Anzahl und Art der vorhandenen Komponenten und/oder Unterkomponenten
- Modellinformation von vorhandenen Komponenten und/oder Unterkomponenten
- Anzahl und Art der vorhandenen Datenübertragungseinrichtungen
- Verbindungsprotokoll einer vorhandenen Datenübertragungseinrichtungen
- Physische Anordnung einer Komponente und/oder Unterkomponente in der Technikeinheit
- Kommunikationsbefähigung einer Komponente über eine oder mehrere Datenübertragungseinrichtungen
- Anzahl und Art von Unterkomponenten einer Komponente
- Identifikation und Versionsinformation einer Firmware, die auf einer Komponente oder Unterkomponente vorhanden ist
- Identifikation und Versionsinformation einer Software, die auf einer Komponente oder Unterkomponente vorhanden ist
- Kommunikationsverbindungen von Komponenten und/oder Unterkomponenten untereinander
- Gegenseitige funktionelle Abhängigkeiten zwischen Komponenten und/oder Unterkomponenten (beispielsweise funktioniert Komponente A ohne Komponente B nicht)
- (gegebenenfalls verteilte) Verantwortlichkeit von Komponenten und/oder Unterkomponenten für eine Funktion des Gesamtsystems (beispielsweise die Steuerung des oder auch das Zusammenwirken mehrerer Steuerchips am Bremssystem eines Fahrzeugs)
- Komponentenversionen (Hardware, Software, Firmware)
- Version und Revisionsnummer von Chips
- Eventuelle Metainformationen (beispielsweise Hersteller)
- Timing-Info, wie etwa Taktfrequenz, Übertragungsgeschwindigkeit, Laufzeit (Rechenzeit), Perioden von zyklischen Aufgaben, etc.)
- Softwarekonfiguration (z.B. Task-Priorität, zugeordnete Speicherbereiche, etc.).

Als „Modell“ bzw. „Konfigurationsmodell“ wird im Zusammenhang mit der gegenständlichen Offenbarung eine systematische Abbildung der Konfiguration der Technikeinheit, gegebenenfalls unter Berücksichtigung von der Technikeinheit zugeordneter Einheiten bezeichnet. Je nach Detaillierungsgrad kann das Modell einige oder alle der für die Konfiguration definierten Merkmale umfassen. Ein Modell kann einerseits Merkmale der Technikeinheit umfassen, deren Übereinstimmung mit der realen Technikeinheit bestätigt ist, andererseits kann das Modell auch Merkmale umfassen, deren Übereinstimmung mit der Technikeinheit nicht bestätigt ist. Das Modell kann auch „Unbekannte“ oder „Platzhalter“ für Merkmale enthalten, von denen bekannt ist, dass sie in der Technikeinheit vorhanden sein müssen, deren genauere Identität jedoch nicht bekannt ist. Als Unbekannte wird in dem Zusammenhang eine Variable bezeichnet, der kein Wert zugeordnet ist. Als Platzhalter wird ein generischer Modellknoten bezeichnet, dem Merkmale ohne spezifische Informationen zugeordnet sind. Solche Platzhalter können beispielsweise für Komponenten verwendet werden, von denen bekannt ist, dass sie in der Technikeinheit vorhanden sein müssen, bei denen aber nicht bekannt ist, um welche Baureihe der Komponente es sich handelt und wo genau sich die Komponente befindet. Platzhalter können auch für andere Merkmale der Technikeinheit verwendet werden, etwa für Software, Firmware, Datenübertragungseinrichtungen etc.

Die Darstellung bzw. der Aufbau des Modells kann beliebig gewählt werden, wobei ein strukturierter Aufbau, bei dem Merkmale zusammengehöriger Einheiten (wie etwa einer Komponente) zu Modellknoten zusammengefasst werden und wobei Beziehungen zwischen den Komponenten (z.B. hierarchische Abhängigkeiten, Datenflüsse, Steuerflüsse, etc.) als Verbindungen zwischen den Modellknoten dargestellt werden können (hierin allgemein als „Verbindungskanten“ bezeichnet). Der Modellierung kann eine beliebige geeignete Systematik zugrunde liegen, wobei jedoch eine einfache Struktur, beispielsweise eine hierarchische Anordnung der Modellknoten in einer Baumstruktur oder eine Anordnung in einer Netzstruktur, für die gegenständlichen Lehren ausreichend ist und die Komplexität der Modelle auf ein überschaubares Ausmaß verringert. Die gegenständliche Offenbarung ist jedoch nicht auf diese Strukturen beschränkt, da auch andere Strukturen für die Modellierung verwendet werden können.

Für bestimmte Tests ist es auch erforderlich, Komponenten in das Modell einzubeziehen, die im Grunde zwar nicht der Technikeinheit an sich sind, die aber mit der Technikeinheit in einer Wechselbeziehung stehen. Der Begriff „Technikeinheit“ ist in diesem Fall breit auszulegen und kann auch solche „externen“ Komponenten umfassen.

Beispielsweise kann die zu analysierende und modellierende Technikeinheit ein Fahrzeug sein, das aber für bestimmte Funktionen einen Kommunikationspartner benötigt. Dieser Kommunikationspartner kann beispielsweise ein zweites Fahrzeug (bei V2x – Vehicle-to-

Everything) sein, oder bei vernetzten Fahrzeugen eine Applikation, die in der Cloud läuft (V2C, Vehicle-to-Cloud). Gegebenenfalls können solche Kommunikationspartner bzw. Komponenten davon in die Modellierung der Technikeinheit miteinbezogen werden, wobei die Komponenten und Merkmale dieser „externen“ Kommunikationspartner im Zusammenhang mit den hierin offenbarten Verfahren analog zu den Komponenten und Merkmalen der eigentlichen Technikeinheit verwendet werden können.

Als „erste plausible Modellvariante“ wird im Zusammenhang mit der gegenständlichen Offenbarung ein Konfigurationsmodell bezeichnet, das einer Bestimmtheitsbedingung entspricht. Die Übereinstimmung der plausiblen Modellvariante mit der tatsächlichen Konfiguration kann zwar nicht mit Sicherheit bestätigt werden, es kann aber auch nicht ausgeschlossen werden, dass es mit der tatsächlichen Konfiguration der betreffenden Technikeinheit übereinstimmt. Plausible Modellvarianten können auch „Platzhalter“ von Komponenten enthalten.

Als „initiale Instanz des Modells“ wird im Zusammenhang mit der gegenständlichen Offenbarung ein üblicherweise unvollständiges Modell bezeichnet, von dem aber vermutet wird, dass möglichst viele bekannten Merkmale des Modells mit der tatsächlichen Technikeinheit übereinstimmen. Das Modell kann weiterhin Unbekannte oder Platzhalter für bislang nicht identifizierte Merkmale enthalten. Bei der initialen Instanz kann es sich beispielsweise um ein generisches Modell der Technikeinheit handeln. Gegebenenfalls kann auch ein spezifischeres Modell als das initiale Modell gewählt werden, etwa auf Basis von Vorinformationen, wie etwa einer Typenbezeichnung der Technikeinheit. Das Ermitteln der initialen Instanz kann vor oder nach dem Herstellen der Verbindung zwischen dem Prüfcomputersystem und der Technikeinheit erfolgen. Beispielsweise kann aufgrund einer Benutzereingabe in das Prüfcomputersystem (z.B. eine Typenbezeichnung der Technikeinheit) eine initiale Instanz des Modells aus einer Datenbank ausgewählt werden. Gegebenenfalls kann die initiale Instanz auch von dem Prüfcomputersystem selbstständig auf Basis von Daten ausgewählt werden, die nach dem Herstellen der Verbindung von der Technikeinheit erhalten wurden. Gegebenenfalls können zur Ermittlung der initialen Instanz auch vordefinierte Testfälle an der Technikeinheit durchgeführt werden, um die initiale Instanz auf Basis von Erfahrungen mit ähnlichen Technikeinheiten zu ermitteln.

Als „spezifizierten Instanz des Modells“ wird im Zusammenhang mit der gegenständlichen Offenbarung eine veränderte Version des Modells bezeichnet, die eine höhere Übereinstimmung mit der tatsächlichen Technikeinheit aufweist, als die initiale Instanz (und gegebenenfalls als vorhergehenden spezifizierten Instanzen).

Als „Spezifizierungsvorgang“ wird im Zusammenhang mit der gegenständlichen Offenbarung das Erzeugen einer spezifizierten Instanz des Modells aus der initialen Instanz oder aus

einer vorhergehenden spezifizierten Instanz bezeichnet. Die Bezeichnung „Entwickeln von spezifizierten Instanzen des Modells“ bezieht sich auf eine iterativ durchgeführte Abfolge von Spezifizierungsvorgängen.

Der Begriff „automatisiert ausführen“ bedeutet im Zusammenhang mit der gegenständlichen Offenbarung, dass das Prüfcomputersystem den entsprechenden Vorgang ohne die Notwendigkeit eins Benutzereingriffs durchführt. Allgemein ist es beabsichtigt, die Anzahl der erforderlichen Benutzereingriffe auf das nötige Mindestmaß zu reduzieren.

Als „Herausforderungsaktion“ wird im Zusammenhang mit der gegenständlichen Offenbarung eine Handlung bezeichnet, die erwarteter Weise ein charakteristisches Verhalten der Technikeinheit, beispielsweise eine charakteristische Datenkommunikation über die Datenübertragungseinrichtung der Technikeinheit, bewirkt. Eine Herausforderungsaktion kann beispielsweise Datenverkehr sein, der vom Prüfcomputersystem über die Prüfschnittstelle zur Datenübertragungseinrichtung übermittelt wird. Gegebenenfalls kann das Prüfcomputersystem Herausforderungsaktionen auch über andere Schnittstellen bewirken, wobei beispielsweise Aktoren verwendet werden können, die auf Teile der Technikeinheit wirken. Gegebenenfalls kann das Prüfcomputersystem auch den Benutzer anweisen, bestimmte Herausforderungsaktionen zu tätigen, beispielsweise das Betätigen von Bedienelementen der Technikeinheit oder das Manipulieren einer Komponente in einer bestimmten Weise. Eine Herausforderungsaktion kann beispielsweise eine speziell gestaltete Datenkommunikation oder auch ein testweise durchgeführter Cyber-Angriff sein. Gegebenenfalls kann anstelle der Herausforderungsaktion auch ein rein passives Beobachten der Technikeinheit erfolgen.

Als „für die Technikeinheit charakteristisches Verhalten“ wird im Zusammenhang mit der gegenständlichen Offenbarung jegliches Verhalten bezeichnet, aus dem sich Rückschlüsse auf zumindest ein Merkmal der Konfiguration der Technikeinheit ziehen lassen. Das charakteristische Verhalten kann dabei beispielsweise das Auftreten einer bestimmten Datenkommunikation über die Datenübertragungseinrichtung oder ein bestimmter Messwert sein, der für die Technikeinheit bzw. für Komponenten der Technikeinheit charakteristisch ist. Beispielsweise können durch eine Messung der Impedanz einer Leitung, die als Datenübertragungseinrichtung verwendet wird, Rückschlüsse auf die Anzahl der Komponenten gezogen werden, die an diese Leitung angeschlossen sind. Das charakteristische Verhalten kann auch über beliebige andere Messungen ermittelt werden.

Das Analysieren des charakteristischen Verhaltens und Rückschließen auf zumindest ein Merkmal der tatsächlichen Konfiguration der Technikeinheit kann beispielsweise durch eine Abfrage einer Datenbank erfolgen, in der charakteristische Verhalten bekannter Technikeinheiten bzw. Komponenten gespeichert sind. Die Datenbank kann entweder extern

oder in das Prüfcomputersystem integriert sein und sie kann gegebenenfalls vom Prüfcomputersystem automatisch aktualisiert werden.

Als „Bestimmtheitsbedingung“ wird im Zusammenhang mit der gegenständlichen Offenbarung eine Bedingung bezeichnet, welche feststellt, dass eine Instanz des Modells ausreichend bestimmt ist, um eine Sicherheitsüberprüfung in einer vorgegebenen Zeit zu ermöglichen. Dabei kann beispielsweise bewertet werden, wieviele Varianten an tatsächlich möglichen Konfigurationen (bzw. Modellvarianten) basierend auf der Instanz existieren. Beispielsweise könnte die Bestimmtheitsbedingung erfordern, dass die Anzahl an möglichen Varianten einer Instanz unterhalb eines bestimmten Schwellenwerts liegt. Es sind jedoch auch komplexere Bestimmtheitsbedingungen möglich. Beispielsweise kann von der Bestimmtheitsbedingung auch berücksichtigt werden, wie erfolgreich die zuletzt durchgeführten Spezifizierungsvorgänge waren, um die Entwicklung der spezifizierten Instanzen nicht zu früh abzubrechen. Die Bestimmtheitsbedingung kann gegebenenfalls auch berücksichtigen, dass die Anzahl der Modellvarianten im Zuge der Durchführung der Sicherheitsüberprüfung weiter eingeschränkt werden kann.

In einer vorteilhaften Ausführungsform des hierin offenbarten Verfahrens kann der Schritt des Ermittelns eines für die Technikeinheit charakteristischen Verhaltens das Abhören von über die Datenübertragungseinrichtung übermittelten Daten durch das Prüfcomputersystem umfassen. Durch das Abhören lassen sich, gegebenenfalls nach einer Herausforderungsaktion, zahlreiche Merkmale der tatsächlichen Konfiguration der Technikeinheit ermitteln.

In vorteilhafter Weise können Merkmale der tatsächlichen Konfiguration der Technikeinheit ausgewählt sein aus zumindest einem Merkmal einer Komponente und/oder zumindest einer Beziehung zwischen Komponenten. Die Beziehung kann beispielsweise eine funktionelle Beziehung oder eine Kommunikationsbeziehung sein. Merkmale einer Komponente können beispielsweise eine Typenbezeichnung der Komponente und/oder eine Modellversion der Komponente und/oder eine Firmwareversion und/oder auf der Komponente laufende Software und/oder deren Version sein. Eine funktionelle Beziehung zwischen Komponenten kann beispielsweise die Anordnung von miteinander kommunizierenden Komponenten an bestimmten Datenübertragungseinrichtungen sein, die Tatsache, von welcher Komponente eine bestimmte Software ausgeführt wird oder auch das Mitwirken mehrerer Komponenten an einer übergeordneten Funktion. Die „übergeordnete Funktion“ kann beispielsweise ein gemeinsam erzielter Effekt sein. Beispielsweise können mehrere Sensoren an einem Bremssystem mitwirken. Sie müssen aber dabei nicht notwendigerweise untereinander kommunizieren. Ihre Daten könnten durch eine andere (möglicherweise sogar noch nicht im spezifischen Modell entdeckte) Einheit verarbeitet werden.

In einer weiteren vorteilhaften Ausführungsform des hierin offenbarten Verfahrens werden auf Basis der ersten plausiblen Modellvariante zumindest eine alternative Modellvariante und vorzugsweise eine Vielzahl an alternativen Modellvarianten erstellt. Dadurch ist es möglich, bei einer nachfolgenden Sicherheitsüberprüfung Komponenten und Merkmale zu berücksichtigen, die im Zuge des Entwickelns der spezifizierten Instanz nicht herausgefunden werden konnten. Dabei werden für unbekannte Merkmale mehrere spekulative Annahmen getroffen, und für jede Annahme jeweils eine Modellvariante erstellt. In Abhängigkeit von der Rechenkapazität des Prüfcomputersystems und der Komplexität der Technikeinheit kann die Gesamtanzahl an alternativen Modellvarianten so hoch sein, dass sie den Rahmen des geistig erfassbaren weit überschreiten und auch einer „manuellen“ Verarbeitung nicht mehr zugänglich sind. Dennoch ist die Menge der alternativen Modellvarianten klein genug, um in einer überschaubaren Zeit einer computergestützten Analyse unterzogen werden zu können, beispielsweise im Zuge einer Sicherheitsprüfung.

Als „alternative Modellvariante“ wird im Zusammenhang mit der gegenständlichen Offenbarung somit eine Abwandlung der ersten plausiblen Modellvariante bezeichnet, bei der zumindest ein unbekanntes Merkmal bzw. ein „Platzhalter“ der Konfiguration durch zumindest ein konkretes Merkmal ersetzt ist, dessen Eigenschaften bekannt sind, von dem aber nicht bekannt ist, ob es in der tatsächlichen Konfiguration der Technikeinheit vorhanden ist. Alternative Modellvarianten können beispielsweise auch anstelle einer einzigen Komponente mehrere Komponenten aufweisen, durch die die eine Komponente gemeinsam realisiert wird. Alternative Modellvarianten können beispielsweise vollständig definiert sein, d.h. alle Platzhalter und Unbekannte können durch spekulative aber konkrete Annahmen ersetzt sein. Als „spekulative Annahme“ wird im Zusammenhang mit der gegenständlichen Offenbarung ein konkretes Merkmal der Konfiguration bezeichnet, dessen tatsächliche Implementierung in der Technikeinheit bislang nicht bestätigt werden konnte.

In einem weiteren Aspekt betrifft die gegenständliche Offenbarung ein auf einem Prüfcomputersystem ausgeführtes Verfahren zur Sicherheitsüberprüfung einer Technikeinheit, wobei zumindest eine erste plausible Modellvariante und gegebenenfalls eine Anzahl an alternativen Modellvarianten ermittelt werden, und wobei das Verfahren die folgenden Schritte aufweist:

- Zuordnen bekannter Schwachstellen zu Komponenten der Modellvarianten,
- Definieren eines Angriffsziels,
- Ermitteln zumindest eines auf das Angriffsziel bezogenen Angriffsmodells für die Modellvarianten,
- Gewichten der Knoten des Angriffsmodells hinsichtlich zumindest einer Bewertungsvariable,

- Ermitteln einer Bewertung zumindest eines Testvektors des Angriffsmodells hinsichtlich der Bewertungsvariable,
- Ermitteln eines Sicherheitswerts als pessimaler Werts aller Bewertungen und
- Ausgeben einer Sicherheitsbestätigung, wenn der Sicherheitswert einem Sicherheitskriterium entspricht.

Das Verfahren erlaubt es somit, sogar dann eine Aussage über die Sicherheit der Technikeinheit zu treffen, wenn nicht alle Komponenten und Merkmale der Konfiguration der Technikeinheit bekannt sind. Das Verfahren kann weitgehend automatisiert ausgeführt werden, sodass der Schulungsaufwand für Benutzer minimiert werden kann.

Als „Schwachstelle“ oder „Vulnerability“ wird im Zusammenhang mit der gegenständlichen Offenbarung ein in der Technikeinheit vorhandener, aber möglicherweise unerkannter Weg bezeichnet, auf dem ein Cyber-Angriff möglich ist. Diese kann dazu führen, dass eine Bewertung eines Testvektors eines Angriffsmodells einem Sicherheitskriterium nicht mehr entspricht.

Als „Sicherheitsüberprüfung “ wird im Zusammenhang mit der gegenständlichen Offenbarung ein Vorgang bezeichnet, bei dem bestätigt (oder verneint) wird, dass die geprüfte Technikeinheit bestimmten Sicherheitsanforderungen entspricht. Die Sicherheitsanforderung kann zum Beispiel bestimmen, dass für ein oder mehrere Angriffsziele eine Sicherheitsbestätigung vorliegt.

Als „Angriffsziel“ wird im Zusammenhang mit der gegenständlichen Offenbarung ein Ereignis bezeichnet, das sich ein Angreifer zum Ziel gesetzt haben kann. Ein Angriffsziel kann beispielsweise sein, eine Kontrolle über die Softwarefunktionen einer Komponente zu erhalten oder bestimmte Komponenten zu beschädigen. Zu praktischen Beispielen für ein Angriffsziel im Fahrzeugumfeld zählen etwa das Manipulieren der Motorsteuerung, das Verändern der Einspritzsteuerung oder ähnliches. Ein Angriffsziel bildet üblicherweise den initialen Knoten eines Angriffsmodells (beispielsweise eines Angriffsbaums oder -netzes).

Als „Angriffsmodell“ wird im Zusammenhang mit der gegenständlichen Offenbarung die modellhafte Beschreibung eines Angriffs bezeichnet, bei der ausgehend von einem initialen Knoten (dem Angriffsziel) Punkte zugeordnet sind, wie dieses Angriffsziel erreicht werden kann. Diese Punkte bilden dem initialen Knoten zugeordnete Knoten, denen stufenweise weitere Knoten zugeordnet sein können. Insbesondere weist das Modell eine baum- oder netzartige Struktur auf. Das Konzept der Angriffsmodelle ist im Fachbereich bekannt und wurde beispielsweise in der Form von „Attack Trees“ in der Publikation „Attack trees“ von Schneier, B. (1999), Dr. Dobb’s journal, 24(12), 21-29 oder auch in der Form von Attack Nets in der Publikation „Attack Net Pentration Testing“ von McDermott, J.P. (2000), Proceedings

of the 2000 workshop on New security paradigms, 15-21 bzw. in „Software fault tree and coloured Petri net-based specification, design and implementation of agent-based intrusion detection systems“ von Helmer et al. (2007), International Journal of Information and Computer Security, 1(1), 109-142 beschrieben; eine (nicht taxative) Übersicht über Angriffsmodelle bietet „An empirical evaluation of the effectiveness of attack graphs and fault trees in cyber-attack perception“ von Lallie, H. S., Debattista, K., & Bal, J. (2017), IEEE Transactions on Information Forensics and Security, 13(5), 1110-1122. Seitdem wurde das Konzept der Angriffsmodelle in einschlägigen Publikationen definiert beziehungsweise vertieft. Im Zusammenhang mit der gegenständlichen Offenbarung wird davon ausgegangen, dass der Fachmann fundierte Kenntnisse des Konzepts der Angriffsmodelle besitzt.

Ein Angriffspfad ausgehend von einem in der Stufenhierarchie des Angriffsmodells zugeordneten Knoten bis zum initialen Knoten wird im Zusammenhang mit der gegenständlichen Offenbarung als „Testvektor“ (oder auch „Angriffsvektor“) bezeichnet und definiert eine Abfolge an Schritten, die erforderlich sind, um das Angriffsziel zu erreichen.

Jeder Knoten des Angriffsmodells ist mit einer Bewertungsvariable gewichtet, die den Aufwand repräsentiert, den ein Angreifer tätigen muss, um den Knoten auszuführen. Die Bewertungsvariable kann als Kosten oder Preis interpretiert werden, wobei die Einheit der Bewertungsvariable beispielsweise in Zeit, Geld, Manpower, in anderen Ressourcen oder in Kombinationen daraus definiert werden kann.

Die Knoten von Angriffsmodellen sind üblicherweise einer definierten Untereinheit der Testeinheit zugeordnet, beispielsweise einer bestimmten Komponente oder einer bestimmten Software, die zur Überwindung des Knotens manipuliert werden muss.

Als „Bewertung des Testvektors“ wird im Zusammenhang mit der gegenständlichen Offenbarung die Summe aller Bewertungsvariablen der Knoten eines Testvektors bezeichnet. Die Bewertung lässt sich somit als Aufwand interpretieren, der für die Ausführung eines Angriffs entlang eines Testvektors notwendig ist. Da jedes Angriffsmodell zahlreiche Testvektoren umfasst, ist für die Beurteilung der Sicherheit der schlechteste bzw. pessimale Wert der Bewertungen aller Testvektoren aller getesteten Angriffsmodelle von Interesse. Dieser pessimale Wert definiert den Testvektor, der mit dem geringsten Aufwand ausgeführt werden kann. Als „pessimal“ wird im Zusammenhang mit der gegenständlichen Offenbarung der Wert bezeichnet, der den geringsten Aufwand für einen erfolgreichen Angriff definiert.

Dieser pessimale Wert aller Bewertungen der Testvektoren eines Angriffsmodells wird im Zusammenhang mit der gegenständlichen Offenbarung als Sicherheitswert bezeichnet. Der Sicherheitswert definiert den minimalen Aufwand für die Erreichung des Angriffsziels. Wenn

der Sicherheitswert ein definiertes Sicherheitskriterium erfüllt, dann kann die Sicherheit des Angriffsmodells bestätigt werden.

Als „Sicherheitskriterium“ wird im Zusammenhang mit der gegenständlichen Offenbarung somit eine Bedingung bezeichnet, die ein Sicherheitswert erfüllen muss, damit die Sicherheit bestätigt werden kann. Als Bedingung kann beispielsweise ein Schwellenwert dienen, z.B. ein Aufwand (definiert z.B. in Geld, Zeit, Manpower, etc.), unterhalb dessen der Sicherheitswert nicht liegen darf.

Als „Sicherheitsbestätigung“ wird im Zusammenhang mit der gegenständlichen Offenbarung eine Aussage bezeichnet, die angibt, dass das die getestete Technikeinheit im Bezug auf das Angriffsziel und den definierten Sicherheitswert als sicher (das heißt einem definierten Sicherheitskriterium entsprechend) anzusehen ist.

In vorteilhafter Weise kann das Verfahren weiters die folgenden Schritte aufweisen:

- Ausführen zumindest eines auf Basis der ermittelten Schwachstellen ausgewählten Cyber-Angriffs auf die Technikeinheit,
- Auswerten des mit dem Cyber-Angriff erzielten Effekts und
- Eliminieren von Modellvarianten, für die der erzielte Effekt nicht schlüssig ist.

Dadurch lässt sich die Anzahl der Modellvarianten während der Prüfung weiter reduzieren und die Kenntnisse über die tatsächliche Konfiguration können vertieft werden.

Bei einem Cyber-Angriff wird beispielsweise auf Basis eines Testvektors ein Exploit ausgewählt und ausgeführt. Als „Exploit“ wird im Zusammenhang mit der gegenständlichen Offenbarung eine Abfolge an Befehlen bzw. Handlungen bezeichnet, die ein Angriffsziel entlang eines Pfads eines Angriffsmodells (d.h. entlang eines Testvektors) verfolgen. Exploits nutzen dabei bekannte Schwachstellen aus. Neben Exploits kann ein Cyber-Angriff auch Fuzzing beinhalten. Als „Fuzzing“ wird im Zusammenhang mit der gegenständlichen Offenbarung das automatisierte (massenhafte) Ausführen von Zufallshandlungen (zum Beispiel das massenhafte Einspielen von Zufallsdaten über eine Datenübertragungseinrichtung) bezeichnet, mit dem Zweck dadurch auf bisher unbekannte Schwachstellen zu treffen und diese auszunützen.

Der Effekt des Cyber-Angriffs kann beispielsweise darin liegen, dass der Angriff erfolgreich ist, dass der Angriff scheitert, oder dass auf andere Weise Informationen erhalten werden, die Rückschlüsse über die Konfiguration ermöglichen. Falls ein Angriff erfolgreich sein sollte, kann im Grunde auf die gesamte Kette an beteiligten Hard- und Softwareelementen rückgeschlossen werden und es lässt sich das Wissen über die tatsächliche Konfiguration der Technikeinheit erheblich vertiefen.

„Eliminieren“ von Modellvarianten bedeutet in diesem Zusammenhang, dass die entsprechenden Modellvarianten für die weitere Sicherheitsüberprüfung nicht mehr berücksichtigt werden, da bekannt ist, dass sie nicht mit der tatsächlichen Konfiguration der Technikeinheit übereinstimmen. Dies kann beispielsweise entweder direkt dadurch erkannt werden, dass eine spezifizierte Komponente tatsächlich eine andere Konfiguration aufweist oder auch indirekt dadurch, dass eine Modellvariante Komponenten oder Konfigurationen aufweist, die durch eine erkannte Konfiguration einer anderen Komponente unplausibel werden.

In vorteilhafter Weise kann das Verfahren weiters die folgenden Schritte aufweisen:

- Ermitteln zumindest einer Software und/oder Firmware, die auf einer Komponente der Technikeinheit installiert ist,
- Aktualisieren der Software und/oder Firmware mit dem Prüfcomputersystem.

Dies kann zum Beispiel dazu dienen, Sicherheitsmängel die mit dem Update (bzw. Aktualisieren) der entsprechenden Software und/oder Firmware auf eine neuere Version behoben werden können, automatisch zu beheben. Die Sicherheitsprüfung kann dann mit der Aktualisierung entsprechend spezifizierten Modellvarianten (d.h. Modellvarianten, die das Update berücksichtigen) fortgesetzt werden.

Als „Software“ werden im Zusammenhang mit der gegenständlichen Offenbarung alle nicht technisch-physikalischen Funktionsbestandteile eines Computers bezeichnet. Im engeren Sinne werden als Software Datenstrukturen bezeichnet, einschließlich Programmen, Dokumentationen und eventuell zugehörigen Daten.

Als „Hardware“ werden im Zusammenhang mit der gegenständlichen Offenbarung die physischen Bestandteile (d.h. die elektronischen und mechanischen Bestandteile) der Technikeinheit bezeichnet.

Als „Firmware“ wird im Zusammenhang mit der gegenständlichen Offenbarung eine Software bezeichnet, die einer bestimmten Hardware (insbesondere einer bestimmten Komponente der Technikeinheit) fix zugeordnet ist und die Funktionalität dieser Hardware grundlegend bestimmt, wobei die Hardware ohne die Firmware nicht nutzbar ist. Firmware ist üblicherweise nur mit speziellen Mitteln bzw. Funktionen austauschbar.

In einer weiteren vorteilhaften Ausführungsform kann das Verfahren weiters die folgenden Schritte aufweisen:

- Ermitteln einer Software und/oder Firmware, die auf einer Komponente der Technikeinheit installiert ist,

- Erstellen simulierter Modellvarianten, welche eine spezifizierte Version der Software und/oder Firmware enthalten,
- Ermitteln eines Sicherheitswerts anhand der simulierten Modellvarianten.

Als „simulierte Modellvariante“ wird im Zusammenhang mit der gegenständlichen Offenbarung eine Modellvariante bezeichnet, die sich in bekannter Weise von der tatsächlichen Konfiguration der Technikeinheit unterscheidet. Insbesondere kann sich die simulierte Modellvariante hinsichtlich der Version von Software und/oder Firmware von der tatsächlich vorhandenen unterscheiden.

In analoger Weise ist es auch möglich, Hardware (also z.B. Komponenten der Technikeinheit) in simulierten Modellvarianten gegen andere Hardware „auszutauschen“ und die Auswirkungen auf die Sicherheit in einer Simulation zu prüfen.

Mithilfe der simulierten Modellvarianten lassen sich Prognosen und Sicherheitsempfehlungen erstellen, die gegebenenfalls auch umgehend umgesetzt werden können.

In vorteilhafter Weise kann die Technikeinheit ein Fahrzeug, und insbesondere ein automatisiertes oder autonomes Fahrzeug gemäß einer der SAE-Stufen 0 bis 5 gemäß der Norm SAE J3016 sein. Diese Angabe bezieht sich auf die Norm SAE J3016 in der zum Zeitpunkt des Prioritätstages der gegenständlichen Anmeldung gültigen Fassung.

In einem weiteren Aspekt betrifft die gegenständliche Offenbarung ein Computerprogrammprodukt, das direkt in den internen Speicher eines digitalen Computers geladen werden kann und Softwarecodeabschnitte umfasst, mit denen die Schritte des hierin offenbarten Verfahrens ausgeführt werden, wenn das Produkt auf dem Computer läuft.

Weiters betrifft die Offenbarung ein Prüfcomputersystem auf dem ein solches Computerprogrammprodukt läuft.

Die gegenständliche Erfindung wird nachfolgend unter Bezugnahme auf die Figuren 1 bis 7 näher erläutert, die beispielhaft, schematisch und nicht einschränkend vorteilhafte Ausgestaltungen der Erfindung zeigen. Dabei zeigt

Fig.1 eine schematische Darstellung einer Technikeinheit und eines Prüfcomputersystems,

Fig. 2 eine beispielhafte Blockdarstellung einer initialen Instanz eines Modells der Konfiguration der Technikeinheit,

Fig. 3 eine Blockdarstellung der initialen Instanz des Modells wobei zusätzlich ein Datenfluss dargestellt ist,

Fig. 4 eine Blockdarstellung einer spezifizierten Instanz des Modells, das mit zusätzlicher Information über Merkmale der Konfiguration der Technikeinheit ergänzt wurde,

Fig. 5 eine Blockdarstellung einer ersten plausiblen Modellvariante der Technikeinheit,

Fig. 6 eine Blockdarstellung einer Vielzahl von alternativen Modellvarianten, die auf Basis der ersten plausiblen Modellvariante erstellt wurden,

Fig. 7 eine Blockdarstellung gemäß Fig. 6, wobei in die Modellvarianten Referenzen auf bekannte Schwachstellen angeführt sind.

Fig. 1 zeigt in schematisierter Weise ein Technikeinheit 1 und ein Prüfcomputersystem 2, die über eine Prüfschnittstelle 6 miteinander verbunden werden können.

Das Prüfcomputersystem 2 kann ein herkömmliches Computersystem sein, auf welchem ein Computerprogrammprodukt ausgeführt wird, welches Softwarecodeabschnitte umfasst, mit denen die hierin beschriebenen, von dem Prüfcomputersystem 2 auszuführenden Schritte ausgeführt werden, wenn das Computerprogrammprodukt auf dem Prüfcomputersystem 2 läuft. Das Prüfcomputersystem 2 kann beispielsweise zumindest eine Anzeige, wie etwa einen Computerbildschirm, und Eingabegeräte, wie etwa eine Maus, ein Keyboard, ein Touchpad und/oder für die Anwendung spezifische Ein- und Ausgabegeräte sowie entsprechende Peripheriegeräte umfassen. Das Prüfcomputersystem 2 weist eine Prüfschnittstelle 6 auf, mit der eine Datenkommunikation mit einer Datenübertragungseinrichtung 3 der Technikeinheit 1 möglich ist.

Die Prüfschnittstelle 6 kann ein Kabel mit einem Stecker aufweisen, der zur Herstellung einer physischen Verbindung mit der Datenübertragungseinrichtung 3 in eine an der Technikeinheit 1 vorgesehene Buchse eingesteckt werden kann. Die Buchse kann beispielsweise eine Diagnoseschnittstelle des Fahrzeugs oder eine andere Schnittstelle, wie etwa ein USB-Anschluss sein. Gegebenenfalls kann die Prüfschnittstelle 6 auch eine kabellose Schnittstelle sein, die eine Verbindung mit einer kabellosen Datenübertragungseinrichtung 3 mittels eines entsprechenden Verbindungsprotokolls herstellt.

Die Datenübertragungseinrichtung der Technikeinheit 1 kann mit einer Vielzahl an Komponenten 4 in Verbindung stehen, deren Konfiguration vorerst weitgehend unbekannt sein kann. Die Konfiguration kann insbesondere durch die Merkmale definiert werden, die die Komponenten 4, Datenübertragungseinrichtung(en) 3 und deren Anordnung und gegenseitigen Beziehungen betreffen. In Fig. 1 ist der Übersichtlichkeit halber nur eine einzige Datenübertragungseinrichtung 3 (etwa in der Art eines Bussystems, wie etwa ein CAN-Bus) dargestellt, es ist aber als bekannt vorauszusetzen, dass eine Technikeinheit 1

mehrere unterschiedliche und gegebenenfalls miteinander vernetzte Datenübertragungseinrichtungen 3 aufweisen kann, an die unterschiedliche Komponenten angeschlossen sein können. Gegebenenfalls kann das Prüfcomputersystem 2 mehrere Prüfschnittstellen 6 aufweisen, die jeweils einer unterschiedlichen Datenübertragungseinrichtung 3 der Technikeinheit zugeordnet sind. Die Komponenten 4 können gegebenenfalls Unterkomponenten 4‘ aufweisen, die nicht direkt an die Datenübertragungseinrichtung 3 angeschlossen sind, sondern direkt an eine Komponente 4.

Im Zusammenhang mit den Darstellungen der Fig. 2 bis 5 wird im Folgenden beispielhaft die Anwendung eines Verfahrens beschrieben, mit dem die (anfänglich oftmals weitgehend unbekannte) Konfiguration der Technikeinheit 1 mithilfe des Prüfcomputersystems 2 so modelliert werden kann, dass ein schlussendlich erhaltenes Modell 5 (dieses wird als „erste plausible Modellvariante bezeichnet) einer Sicherheitsprüfung zugänglich ist. Dabei soll es möglich sein, die Sicherheitsüberprüfung in einer ökonomisch rationalen Weise durchzuführen. Im Umfeld von Sicherheitsüberprüfungen von Fahrzeugen soll eine Sicherheitsüberprüfung dabei innerhalb weniger Arbeitsstunden möglich sein. Tiefe Scans können gegebenenfalls auch länger dauern, beispielsweise mehrerer Tage, aber eine menschliche Interaktion nur gelegentlich oder gar nicht erfordern. Der Maßstab der ökonomischen Rationalität richtet sich dabei nach der jeweiligen Anwendung: Für die Sicherheitsüberprüfung von neuen Technikeinheiten und Technikeinheiten im Entwicklungsstadium kann sich auch ein verhältnismäßig großer Aufwand rechnen. Eine routinemäßige Sicherheitsüberprüfung eines bereits zugelassenen Straßenfahrzeugs, zum Beispiel, sollte nach Möglichkeit wesentlich schneller abgeschlossen werden können. Unter günstigen Umständen könne eine Sicherheitsüberprüfung innerhalb einer Stunde oder weniger, möglicherweise sogar innerhalb weniger Minuten abgeschlossen werden.

Das im folgenden beschriebenen Beispiel einer solchen Modellierung basiert auf einem motorgetriebenen Fahrzeug (etwa einem Elektrofahrzeug, einem Fahrzeug mit Verbrennungsmotor, einem Fahrzeug mit einem Hybridantrieb, einem Fahrzeug mit Brennstoffzellen, etc.). Anfänglich sind dem Prüfer (bzw. dem Benutzer des Prüfcomputersystems) von diesem Fahrzeug nur grundlegende Daten bekannt, beispielsweise dass das Fahrzeug einen Elektromotor oder einen Verbrennungsmotor hat, um welches Fahrzeugmodell es sich handelt, etc. Diese Informationen können vom Benutzer in das Prüfcomputersystem 2 eingegeben werden, gegebenenfalls kann das Prüfcomputersystem 2 solche Informationen auch automatisch ermitteln, sobald die Verbindung über die Prüfschnittstelle 6 hergestellt wurde. Die grundlegenden Daten können auch einen Mix aus den Informationen, die direkt eingegeben werden (z.B. „hat ein Fahrerassistenzsystem“) und solchen, die indirekt ermittelt werden (z.B. durch Angabe der Fahrzeug-Identifikationsnummer (VIN) könnte aus einer Datenbank viele dieser Attribute

automatisch abgefragt werden) enthalten. Auf Basis dieser grundlegenden Informationen kann das Prüfcomputersystem 2 eine initiale Instanz 100 eines Modells 5 wählen, wie es in Fig. 2 und 3 schematisch dargestellt ist. Die initiale Instanz 100 des Modells 5 kann beispielsweise aus einer Bibliothek möglicher Templates für die entsprechende Technikeinheit 1, beispielsweise aus einer Bibliothek möglicher Templates für vernetzte Fahrzeuge, ausgewählt werden.

Das Modell 5 bildet hierarchisch den Aufbau bzw. die Konfiguration der Technikeinheit ab, wobei der dargestellte Fall auf einer Baumstruktur basiert. In der Baumstruktur werden die einzelnen Merkmale in Modellknoten (1000, 1001, etc.) zusammengefasst, die beispielsweise einzelne Komponenten oder Subkomponenten umfassen können.

Das Modell 5 ist in mehreren hierarchischen Ebenen aufgebaut, wobei die hierarchischen und/oder sonstigen Beziehungen zwischen einzelnen Modellknoten durch Verbindungskanten 10 dargestellt sind, die beispielsweise die Struktur funktioneller Abhängigkeiten repräsentieren (beispielsweise zwischen einem System und einem Subsystem). Der Aufbau des Modells und dessen Beziehungen können aber auch beliebig anders gegliedert werden, beispielsweise nach physischen Verbindungen mit einem Eingangsknoten, der direkt mit der Prüfschnittstelle 6 verbunden ist, als Wurzel des Baumes. Die oberste hierarchische Ebene bildet eine Identifikationsebene 201, die im obersten Modellknoten 1000 die modellierte Technikeinheit 1 identifiziert (z.B. als Fahrzeugtype und Fahrgestellnummer). Darunterliegend wird im Modellknoten 1001 die Modellvariante identifiziert. Jedes Modell 5 kann mehrere Varianten aufweisen, wie dies durch den in Strichlinien dargestellten Modellknoten 1001‘ angedeutet ist. Die Struktur und Eigenschaften der Modellvarianten werden untenstehend insbesondere im Zusammenhang mit Fig. 6 und 7 beschrieben.

Die nächste hierarchische Ebene kann als Komponentenebene 202 bezeichnet werden. Darin sind die einzelnen Komponenten 4 der Technikeinheit 1 repräsentiert, wobei beispielsweise ein Modellknoten 1002a eine erste Komponente 4 repräsentiert und die weitern Modellknoten 1002b, 1002c, etc., weitere Komponenten 4 der Technikeinheit repräsentieren. Zu Beispielen solcher Komponenten zählen etwa die Motorsteuerung, die Fahrdynamikregelung, Fahrerassistenzsysteme, Kombiinstrumentensteuerung, etc.

Darunterliegend ist eine Unterkomponentenebene 203 vorgesehen, deren Modellknoten 1003a, 1003b, etc. Unterkomponenten betreffen, die jeweils einem einzelnen Modellknoten der Komponentenebene 202 zugeordnet sind.

Die unterste hierarchische Ebene kann als Interaktionsebene 204 bezeichnet werden. Die darin angeführten Modellknoten 1004a, 1004b, etc. können jeweils Aktoren, Sensoren, Benutzerschnittstellen, etc. betreffen. Die Modellknoten 1004 der Interaktionsebene 204 sind

jeweils einem hierarchisch übergeordneten Modellknoten zugeordnet, wobei sie entweder einem Modellknoten der Unterkomponentenebene 203 oder einem Modellknoten der Komponentenebene 202 zugeordnet sein können (die zweitere Option ist in Fig. 2 nicht dargestellt).

Die Bezeichnungen der einzelnen hierarchischen Ebenen dient lediglich zur Veranschaulichung und ist keinesfalls einschränkend auszulegen. Insbesondere können alle Modellknoten als „Komponenten“ der Technikeinheit 1 angesehen werden und das Modell könnte auch mehr oder weniger Ebenen aufweisen.

Die Verbindungskanten 10 können beispielsweise eine hierarchische Anordnung bzw. hierarchische Abhängigkeiten, andere Beziehungen und/oder Datenkommunikationspfade darstellen. Allgemein können mithilfe der Modellknoten und der Verbindungskanten 10 des in Fig. 1 dargestellten Modells 5 eine Vielzahl an Merkmalen definiert werden, zu denen beispielsweise die folgenden Informationen Zählen:

- Teilsysteme und Systemgrenzen,
- Schnittstellen, Sensoren, Aktuatoren,
- Funktionalitäten (wie etwa implementierte Funktionen, Protokolle, Standards, etc.),
- Beschreibungen der technischen Realisierung, wie etwa
  - Informationen über Software, inkludierte Bibliotheken, Laufzeitumgebung etc., mit genauer Informationen über die jeweilige Version und Angaben zum Erstellungstool (Compiler, Linker, etc.), Angaben zu Debugger Info, etc.
  - Hardware (Chiphersteller, Revision, etc.), Angaben zu Debugger-Schnittstellen (JTAG), etc.
  - Datenpfade zwischen Komponenten

Die initiale Instanz 100 des Modells 5 kann unvollständige Informationen über bestimmte Merkmale und Modellknoten aufweisen, die als Unbekannte oder Platzhalter bezeichnet werden.

Die initiale Instanz 100 des Modells 5 kann eine weitere Darstellungsebene aufweisen, die von der hierarchischen Struktur unabhängig ist, beispielsweise um Datenflüsse und Kommunikationsbeziehungen darzustellen, die zwischen den einzelnen Modellknoten auftreten können. Ein solcher Datenfluss 11 ist beispielsweise in Fig. 3 durch eine Stich-Punkt-Linie dargestellt.

Umgelegt auf einen praktischen Anwendungsfall kann der Datenfluss 11 beispielsweise der Übermittlung der aktuellen Motordrehzahl von einem Motorsteuergerät (ECU) zu einem Getriebesteuergerät (TCU) betreffen. Das Motorsteuergerät kann beispielsweise durch den

Modellknoten 1002a repräsentiert sein. Dieser enthält über den Modellknoten 1003a eines Untersystems (das z.B. eine Sensoren- und Schnittstellensteuerung repräsentiert) einen Messwert, der von einem Drehzahlsensor erhalten wird, der durch den Knoten 1004a repräsentiert ist. Die Motorsteuerung (Modellknoten 1002a) übermittelt den Messwert (bzw. aus dem Messwert abgeleitete Daten) an den Knoten 1003b, der die Daten wiederum an den Modellknoten 1003a weiterleitet. Der Knoten 1003b könnte in diesem Beispiel etwa ein Messkonten sein (und beispielsweise eine Analog-Digital-Umwandlung beinhalten) oder eine Messwert-Vorverarbeitung (z.B. eine Skalierung) durchführen. Es ist möglich, dass der (physische) Sensor, der durch den Knotens 1004a repräsentiert wird, und die Einheit (z.B. Mess-Vorverarbeitung), die durch den Knoten 1003a repräsentiert wird, in einem gemeinsamen Gehäuse verbaut sind, aber logisch trotzdem getrennt betrachtet werden können und daher auch so modelliert werden. Danach werden die Daten zum Modellknoten 1004c übermittelt, der beispielsweise eine CAN-Schnittstelle repräsentiert. Der Modellknoten 1004c leitet dann die Daten über den CAN-Bus an das Getriebesteuergerät weiter, das durch den Modellknoten 1002c repräsentiert ist. Auf analoge Weise können zahlreiche weitere mögliche Datenflüsse und Kommunikationsverbindungen in dem Modell 5 dargestellt werden.

Die im Zusammenhang mit der Beschreibung der Fig. 2 und 3 offenbarten Eigenschaften sind sinngemäß auch auf alle im Folgenden beschriebenen Modellvarianten anzuwenden, die aus der initialen Instanz 100 des Modells 5 entwickelt werden. Dabei werden in iterativen Spezifizierungsvorgängen Unbekannte und Platzhalter durch konkrete Merkmale ersetzt, wie dies im Folgenden unter Bezugnahme auf Fig. 4 und 5 beschrieben wird.

Fig. 4 zeigt eine Blockdarstellung einer spezifizierten Instanz 101 des Modells 5, wobei die spezifizierte Instanz 101 mit zusätzlichen Informationen (die in Fig. 4 als Informationsblock 1103a schematisch dargestellt sind) über die Unterkomponente des Modellknotens 1003a ergänzt wurde. Der Informationsblock kann beispielsweise Informationen über ein verwendetes Verbindungsprotokoll, eine Typenbezeichnung, ein Entwicklungsstadium, verwendete Software und Softwareversion, eine Typenbezeichnung und weitere Infos über eine CPU- oder einen Microcontroller, etc., enthalten.

Eine Möglichkeit, um anfänglich zusätzliche Informationen zu erhalten, kann beispielsweise in einer Benutzerabfrage bestehen. Der Benutzer kann zum Beispiel durch eine Sichtinspektion ermitteln, ob eine bestimmte Komponente in der Technikeinheit 1 verbaut ist, sofern dies durch eine Sichtkontrolle erkennbar ist. Weitere Informationen können von dem Prüfcomputersystem 2 durch Spezifizierungsvorgänge teil- oder vollautomatisch über die Prüfschnittstelle 6 durchgeführt werden. Als „teilautomatisch“ wird ein Spezifizierungsvorgang bezeichnet, bei dem ein Benutzereingriff erforderlich ist, ein vollautomatischer Spezifizierungsvorgang erfordert hingegen keinen Benutzereingriff.

Zur Ausführung von teil- und vollautomatischen Spezifizierungsvorgängen kann das Prüfcomputersystem 2 beispielsweise Scans durchführen, wobei bekannt Methoden aus dem Reverse Engineering angewendet werden. Zu Beispielen solcher Scans zählen:

- Das Ermitteln von implementierten Verbindungsprotokollen und deren Version durch Protokoll-Sniffer,
- Die Messungen zusätzlicher Attribute, wie etwa eine Latenzzeit, und das Ermitteln von Details der Implementierung der Verbindungsprotokolle (Software, Hardware),
- Erkennen von Komponenten und/oder Protokollen durch eine speziell gestaltete Datenkommunikation (Herausforderungsaktion)
- Das Erkennen von Software, indem Speicher (RAM, Flash, etc.) durchsucht und mittels Pattern-Matching auf Signaturen bekannter Softwarekomponenten geschlossen wird,
- Untersuchung der Programmablauf-Struktur in bereits kompilierter Software („Control flow integrity checks“), wobei beispielsweise bekannte Fehleranalysetools, wie etwa Valgrind, verwendet werden können.

Gegebenenfalls können für die obigen Scans zusätzliche Informationen durch Expertenwissen vom Benutzer erhalten werden. Dies ist insbesondere für Technikeinheiten, die sich noch in einer frühen Entwicklungsphase befinden oder zu denen nur geringe Erfahrungswerte vorhanden sind, vorteilhaft.

Immer, wenn auf Basis eines Ergebnisses eines Scanvorgangs ein charakteristisches Verhalten erkannt wird, das einen Rückschluss auf zumindest ein Merkmal der tatsächlichen Konfiguration der Technikeinheit 1 erlaubt, wird das Modell 5 mit dieser Information spezifiziert. Somit wird durch Anwenden der automatisierbaren Scan-Vorgänge der Informationsstand über die Konfiguration schrittweise erweitert und in den schrittweise entwickelten spezifizierten Instanzen 101 des Modell 5 abgebildet.

Ein Scanvorgang kann entweder eine Reaktion analysieren und auswerten, die durch eine Herausforderungsaktion ausgelöst wurde, oder es kann ein Verhalten der Technikeinheit 1 ausgewertet werden, das von der Technikeinheit 1 selbst ausgelöst wurde, und nicht als Reaktion auf eine Herausforderungsaktion aufgetreten ist. Beispielsweise kann der Datenverkehr auf einem Datenbus (beispielsweise einem CAN-Bus eines Fahrzeugs) vom Prüfcomputersystem 2 rein passiv „abgehört“ werden. Die auf dem Bus auftretenden Datenkommunikationsereignisse können dann analysiert und ausgewertet werden, um auf Merkmale der Technikeinheit rückschließen zu können. Ein solches „Abhören“ von Datenkommunikationsereignissen ist ohne Herausforderungsaktion möglich, die damit erzielbaren Erkenntnisse sind jedoch beschränkt. Um weitere Informationen zu erhalten kann

daher versucht werden, die Datenkommunikation mittels einer Herausforderungsaktion gezielt auszulösen. Die Herausforderungsaktion kann beispielsweise darin bestehen, dass das Prüfcomputersystem 2 einen eigenen Datenverkehr auf der Datenübertragungseinrichtung 3 generiert, und die Reaktionen darauf analysiert und auswertet. Es können jedoch auch komplexere Herausforderungsaktionen erfolgen, beispielsweise indem Benutzerhandlungen ausgeführt werden, die vom Prüfcomputersystem 2 einem vorgegeben werden.

Die Spezifizierungsvorgänge können von dem Prüfcomputersystem 2 so lange ausgeführt werden, bis die vollständige Konfiguration gefunden wurde. Üblicherweise ist dies jedoch in einer vorgegebenen Zeit nicht möglich, sodass die Spezifizierungsvorgänge beendet werden, sobald eine Bestimmtheitsbedingung erfüllt ist. Das Ergebnis ist ein verfeinertes, konkretisiertes Modell, das zwar immer noch Lücken enthalten kann, das aber einen deutlich höheren Detaillierungsgrad aufweist, als die initiale Instanz 100 des Modells. Die Bestimmtheitsbedingung kann beispielsweise darin bestehen, dass der Anteil an nicht identifizierten Merkmalen einen gewissen Anteil unterschreitet. Gegebenenfalls können die einzelnen Merkmale hinsichtlich ihrer Relevanz gewichtet sein, wobei die Bestimmtheitsbedingung erfüllt sein kann, wenn das summierte Gewicht der nicht identifizierten Merkmale einen vorbestimmten Wert unterschreitet. Alternativ oder zusätzlich kann die Bestimmtheitsbedingung andere Kriterien umfassen, etwa eine bestimmte Testzeit oder es kann beispielsweise auch der Erfolg der zuletzt durchgeführten Spezifizierungsschritte bewertet werden. Solange die Spezifizierungsschritte dabei erfolgreich neue Informationen generieren, werden die Spezifizierungsvorgänge weiter ausgeführt. Wenn dem Aufwand für die Spezifizierungsvorgänge nur mehr geringe Fortschritte gegenüberstehen, gegebenenfalls in Kombination mit weiteren Bestimmtheitsbedingungen, können die Spezifizierungsvorgänge beendet werden.

Das mithilfe der Spezifizierungsvorgänge entwickelte Modell (d.h. die vollständigste Version der spezifizierten Instanzen 101 des Modells 5) wird im Zusammenhang mit der gegenständlichen Offenbarung als „erste plausible Modellvariante 102“ bezeichnet.

Fig. 5 zeigt eine schematische Blockdarstellung einer solchen ersten plausiblen Modellvariante 102 der Technikeinheit 1. Zu den Modellknoten 1002a, 1002b, 1003a und 1004c konnten bestimmte Informationen ermittelt werden, wie dies durch die Informationsblöcke 1102a, 1102b, 1103a und 1104c dargestellt ist.

Der Anteil der Spezifizierungsvorgänge, die vom Prüfcomputersystem 2 vollautomatisch durchgeführt werden können, steigt mit der Anzahl der an ähnlichen oder gleichen Technikeinheiten 1 durchgeführten Prüfungen, da hierbei Datenbanken über mögliche Konfigurationen erweitert werden, die eine zunehmend automatischen Verfahrensablauf

ermöglichen. Es handelt sich somit um ein lernendes System. Sobald eine anfängliche Lernphase überwunden, und ausreichend Information in den Datenbanken hinterlegt wurde, können immer komplexere Aufgaben in kürzerer Zeit automatisch ausgeführt werden.

Sobald eine erste plausible Modellvariante 102 identifiziert worden ist, erfolgt eine weitere Detaillierung spekulativ. Dies ist in Fig. 6 beispielhaft dargestellt. Fig. 6 zeigt mehrere als überlagerte Ebenen dargestellte alternative Modellvarianten 103, 103‘ und 103“, die auf Basis der ersten plausiblen Modellvariante 102 erstellt werden. Bei der Erstellung der alternativen Modellvarianten 103 werden zuerst alle fehlenden Merkmale ermittelt, die für eine Sicherheitsprüfung relevant sind. Danach werden für jedes dieser Merkmale mehrere spekulative Annahmen getroffen, die jeweils eine mögliche Implementierung darstellen. Dann wird für jede der unter diesen Annahmen möglichen Merkmalskombinationen eine alternative Modellvariante erstellt.

Zum Beispiel könnte bei der ersten plausiblen Modellvariante 102 nicht bekannt sein, welche konkrete Implementierung in einer bestimmten Steuergerät (z.B. einem durch den Modellblock 1003c repräsentierten Steuergerät) als TCP/IP-Stack verwendet wurde. Aus diesem Grund werden jetzt N Annahmen mit möglichen Implementierungen getroffen. Sollte dies die einzige Unbekannte der ersten plausiblen Modellvariante 102 sein, ergibt dies genau N alternative Modellvarianten. Üblicher Weise ist es jedoch erforderlich, mögliche Implementierungen von mehreren unbekannten Merkmalen zu erstellen, wobei für jedes dieser Merkmale eine Anzahl an möglichen Implementierungen (M, O, ...) erstellt wird. Die Gesamtanzahl der alternativen Modellvarianten ergibt sich somit als das Produkt der Anzahl der jeweiligen alternativen Modellvarianten (N x M x O ...). Die Gesamtanzahl der alternativen Modellvarianten 103 erreicht somit üblicherweise eine Größenordnung, die nur noch von leistungsfähigen Prüfcomputersystemen 2 untersucht und geprüft werden können. Im Unterschied zum Ausgangspunkt, der initialen Instanz 100 des Modells, ist die Aufgabe jedoch in einer vorgegebenen Zeit lösbar, da die erste plausible Modellvariante 102 ja die Bestimmtheitsbedingung erfüllt.

Nachdem die alternativen Modellvarianten erstellt wurden, kann die eigentliche Sicherheitsüberprüfung der Technikeinheit 1 erfolgen.

Den einzelnen alternativen Modellvarianten 103 werden dazu bereits bekannte Schwachstellen zugeordnet. Dabei werden die identifizierten Merkmale und die getroffenen Annahmen mit Sammlungen bekannter Schwachstellen abgeglichen. Solche Sammlungen können im Internet frei oder entgeltlich verfügbar sein (z.B.: http://cve.mitre.org/ oder https://www.automotiveisac.com/) und/oder es können auch interner Sammlungen von Herstellern, Verbänden, etc. verwendet werden. Nach diesem Zuordnen wird eine Vielzahl alternativer Modellvarianten 103 erhalten, denen jeweils bekannte Schwachstellen

zugeordnet sind. Fig. 7 zeigt eine Blockdarstellung der in Fig. 6 gezeigten alternativen Modellvarianten, gemäß wobei mehrere Referenzen 104 auf bekannte Schwachstellen angeführt und einem bestimmten Modellknoten zugeordnet sind. Gegebenenfalls können dabei sowohl mehrere Schwachstellen einem Modellknoten als auch eine Schwachstelle mehreren Modellknoten zugeordnet werden.

Weiters wird ein Angriffsziel definiert, beziehungsweise kann das Angriffsziel aus einer Liste an abzuarbeitenden Angriffszielen ausgewählt werden. Die Durchführung der Sicherheitsüberprüfung wird im Folgenden im Zusammenhang mit diesem einen Angriffsziel beschrieben. Gegebenenfalls kann die Sicherheitsüberprüfung jedoch auch mehrere Angriffsziele umfassen, wobei sie dann für jedes Angriffsziel in analoger Weise abgearbeitet wird.

Bezogen auf das Angriffsziel wird nun für jede alternative Modellvariante ein Angriffsmodell erstellt, der für die einzelnen Modellknoten die bekannten Schwachstellen berücksichtigt. Jedem Knoten in diesem Angriffsmodell entspricht üblicherweise ein Knoten in der jeweiligen Modellvariante. Die Schwachstellen (und eventuell implementierte Gegenmaßnahmen) bestimmen den Aufwand um einen Knoten zu kompromittieren und damit als Hindernis auf dem Pfad zum Angriffsziel zu überwinden (siehe unten). Die hierarchische Struktur der Angriffsmodelle erlaubt es, für bekannte Modellknoten auf bereits für diesen Modellknoten entwickelte Angriffsmodelle zurückzugreifen, und diese im jeweiligen Angriffsmodell zu benutzen.

Gegebenenfalls können auch „spekulative Schwachstellen“ berücksichtigt werden, etwa für Knoten, bei denen es noch keine bekannte Schwachstelle gibt, bei der aber vermutet wird (z.B. von Experten), dass so eine Schwachstelle in vertretbarer Zeit gefunden werden könnte. Diesem Knoten kann dann eine spekulative Schwachstelle zugeordnet werden. Spekulative Schwachstellen dienen dazu, auch Test zu ermöglichen, wenn die Schwachstellen-Datenbanken noch unvollständig und nur schwach besetzt sind. Spekulative Schwachstellen können beispielsweise durch besondere Techniken zum Auffinden von Schwachstellen, über die kein Vorwissen besteht, getestet werden, wie etwa durch Fuzzing.

Die Knoten des Angriffsmodells sind jeweils durch eine Bewertungsvariable hinsichtlich eines Aufwands gewichtet, der dem Knoten einen Aufwand zu dessen Überwindung zuordnet, beispielsweise in Geld, Manpower, Zeit, anderen Ressourcen, etc. Für das definierte Angriffsziel kann nun für jeden Pfad des Angriffsmodells (d.h. für jeden Testvektor) unter Ausnützen der am jeweiligen Knoten bekannten Schwachstellen und der jeweiligen Bewertungsvariable eine Bewertung durchgeführt werden.

Für die Sicherheitsüberprüfung ist es jedoch nicht erforderlich, eine Bewertung jedes einzelnen Testvektors jeder alternativen Modellvariante zu errechnen, da nur der pessimale

Wert aller Testvektoren von Interesse ist. Die Bewertung eines Testvektors kann daher abgebrochen bzw. ausgelassen werden, wenn klar ist, dass die Bewertung dieses Testvektors höher sein wird, als der bisher ermittelte pessimale Wert. Zum Beispiel kann auf die Bewertung von Testvektoren ganz verzichtet werden, die einen Knoten aufweisen, der eine bessere Bewertung hat, als der bisher ermittelte pessimale Wert eines ganzen Testvektors. Solche alternativen Testvektoren können jedoch dann relevant, wenn sich das spezifizierte Modell ändert und daher eine Neubewertung eines Angriffsmodells beziehungsweise dessen Pfade impliziert.

Sollte eine Bewertung eines Testvektors gefunden werden, die unter dem Sicherheitskriterium liegt, das für die Sicherheitsbestätigung definiert wurde, kann die Sicherheitsüberprüfung entweder abgebrochen werden, oder es können Maßnahmen empfohlen oder vom Prüfcomputersystem 2 umgesetzt werden, die die Sicherheit der Technikeinheit 1 erhöhen, beispielsweise ein Software- oder Firmwareupdate einer oder mehrerer Komponenten. Danach kann die Sicherheitsüberprüfung mit einer neuerlichen Ermittlung der Modellvarianten wiederholt werden, wobei diesmal die bereits ermittelten Merkmale von Anfang an verwendet werden können.

Ansonsten wird die Bewertung der Testvektoren durchgeführt, bis ein pessimaler Wert aller Testvektoren aller Angriffsmodelle aller alternativen Modellvarianten ermittelt wurde. Wenn dieser pessimale Wert (der auch als Sicherheitswert bezeichnet werden kann) über dem zuvor definierten Sicherheitskriterium liegt, kann eine Sicherheitsbestätigung („Security Verification“) für die Technikeinheit ausgegeben werden. Zusätzlich könne Empfehlungen gegeben werden, wie die Sicherheit weiter erhöht werden kann, beispielsweise durch Identifizieren von Schutzmaßnahmen, wie etwa Softwareupdates. Die Auswirkungen solcher Softwareupdates auf den erreichbaren Sicherheitswert können gegebenenfalls in einer Simulierten Sicherheitsüberprüfung vorab getestet werden. Gegebenenfalls kann nach einer oder mehreren ausgeführten Schutzmaßnahmen eine neuerliche Sicherheitsüberprüfung ausgeführt werden, wobei auf die bisher ermittelten Informationen zurückgegriffen werden kann.

Die Schritte der Sicherheitsüberprüfung können iterativ durchgeführt werden, wobei Sicherheitsmaßnahmen ausgeführt werden, sobald ein Testvektor gefunden wurde, dessen Bewertung unterhalt des Sicherheitskriteriums liegt, und wobei das Verfahren dann auf Basis der neuen Erkenntnisse fortgesetzt wird.

Bei der Ausführung des Verfahrens ist darauf bedacht zu nehmen, dass viele Testvektoren der Angriffsmodelle, die auf den alternativen Modellvarianten basieren, Knoten umfassen, die auf nicht bestätigten Komponenten bzw. Merkmalen basieren, da die Merkmale auf Basis von spekulativen Annahmen ausgewählt wurden. Sobald in der Vielzahl der alternativen

Modellvarianten ein Testvektor gefunden wird, der über einen Knoten mit einer spekulativen Annahme führt, wobei der Knoten eine Schwachstelle offenbart, kann versucht werden, diese Schwachstelle an der realen Technikeinheit 1 auszunutzen, indem durch das Prüfcomputersystem 2 ein entsprechender Cyber-Angriff ausgeführt wird. Auch bestätigte Knoten und Testvektoren können auf diese Weise überprüft werden (z.B. durch entsprechende Tools, wie etwa Penetration-Tester). Diese „tatsächliche“ Attacke kann dann dazu dienen, den Befund zu validieren. Unter Umständen kann es sich vielleicht sogar ergeben, dass ein Angriff noch einfacher ist als gedacht, und damit die „Kosten“ (d.h. die Bewertung) in der Realität niedriger liegen. (Beispielsweise könnte ein default-Passwort vergeben worden sein, das leicht zu erraten ist. In dem Fall muss kein brute-force Durchprobieren angewendet werden).

Beispielsweise kann bekannt sein, dass eine bestimmte Komponente (die einen Knoten eines Testvektors betrifft) auf eine DDoS-Attacke anfällig ist. Das Prüfcomputersystem 2 kann dann eine solche DDoS-Attacke gemäß einem auf dem Testvektor basierenden Exploit durchführen. Falls der Cyber-Angriff auf dieses Weise erfolgreich ist, können alle Modellvarianten eliminiert werden, bei denen der entsprechende Testvektor diese Schwachstelle nicht aufweist. Sollte hierbei nur eine einzige Modellvariante übrig bleiben, kann daraus auf weitere tatsächliche Merkmale der Technikeinheit 1 geschlossen werden. Dadurch kann die Vielfalt der alternativen Modellvarianten erheblich eingeschränkt werden und gegebenenfalls kann es auf diese Weise sogar möglich sein, die Konfiguration der Technikeinheit vollständig im Modell abzubilden (d.h. es gibt dann nur mehr eine alternative Modellvariante, deren vollständige Übereinstimmung mit der Technikeinheit 1 bestätigt ist). Das verwenden von Exploits kann von zusätzlicher Relevanz sein um die tatsächliche Implikation einer Schwachstelle zu prüfen; so kann eine Schwachstelle durch leichte Änderungen in der Konfiguration einer Software oder durch zusätzliche Schutzmaßnahmen nicht ausnutzbar sein, obwohl die Software prinzipiell durch diese Schwachstelle betroffen wäre.

Durch einen erfolgreich ausgeführten Cyber-Angriff lässt sich üblicherweise die gesamte Kette an Komponenten, die von den Knoten des Testvektors betroffen sind, vollständig identifizieren.

Sobald keine Testvektoren mehr gefunden werden, deren Bewertung unterhalb des Sicherheitskriteriums liegt, kann das System als „ausreichend sicher“ betrachtet werden, und es wird eine Sicherheitsbestätigung ausgegeben.

Bei jeder Sicherheitsüberprüfung werden die gewonnenen Erkenntnisse ausgewertet und für zukünftige Sicherheitsüberprüfungen in entsprechenden Datenbanken gespeichert. Werden beispielsweise Testvektoren gefunden, die einen Cyber-Angriff ermöglichen (d.h.

Schwachstellen) können daraus automatisch entsprechende Testfälle, Testvektoren, und gegebenenfalls Exploits generiert werden, die bei zukünftigen Sicherheitsüberprüfungen ähnlicher Technikeinheiten verwendet werden können.

Als „Testfall“ wird im Zusammenhang mit der gegenständlichen Offenbarung ein automatisierter Ablauf an Testschritten bezeichnet, der auf Mustern basiert, die bei zuvor ausgeführten Sicherheitsüberprüfungen bei ähnlichen Technikeinheiten erkannt wurden. Solche Testfälle können das hierin offenbarte Verfahren erheblich abkürzen. Beispielsweise kann auf Basis früherer Sicherheitsüberprüfungen bekannt sein, dass eine bestimmte Art oder ein bestimmtes Modell einer Technikeinheit häufig eine Anfälligkeit hinsichtlich bestimmter Testvektoren aufweist. Mithilfe der Testfälle können nun bereits im Zuge der Modellierung entsprechende Exploits ausgeführt werden, deren Erfolg oder Misserfolg Rückschlüsse auf die tatsächliche Konfiguration der Technikeinheit erlauben. Die Exploits eines Testfalls können dabei im Zusammenhang mit der gegenständlichen Offenbarung als „Herausforderungsaktion“ betrachtet werden, wobei das Ergebnis das charakteristische Verhalten der Technikeinheit repräsentiert.

Die oben beschrieben Vorgehensweise erlaubt die Implementierung einer weitestgehend automatisierten Testdurchführung und Testauswertung, wobei funktionale und nicht-funktionale Fehler bzw. allgemein Unregelmäßigkeiten in der Technikeinheit 1 erkannt werden können.

Im Zuge der Sicherheitsüberprüfung (oder als Ergebnis derselben) können gegebenenfalls Sicherheits- und/oder Verbesserungsmaßnahmen vorgeschlagen und gegebenenfalls auch ausprobiert werden. Die Vorschläge ergeben sich aus fiktiv angenommenen bzw. simulierten Veränderungen der Konfiguration, die den Angriffsmodell bzw. zumindest einen Testvektor davon verändern, z.B. ein Softwareupdate einer durch einen Knoten repräsentierten Komponente. Die Validierung der vorgeschlagenen Verbesserungsmaßnahme kann dabei beispielsweise in den folgenden drei Ausprägungen erfolgen:

- Simulation am Angriffsmodell (rein rechnerisch im Modell)
- Simulation in einer Simulationsumgebung (d.h. die Technikeinheit wird zumindest zum Teil in virtuellen Simulationssystemen abgebildet, die mit den darauf laufenden Softwareversionen simuliert werden)
- Testen an der tatsächlichen Testeinheit (zum Beispiel an einem physischen Fahrzeug in einem Prüfstand), wobei gegebenenfalls einzelne Komponenten der Technikeinheit in Form einer (Co-)Simulation durch virtuelle Äquivalente ersetzt sein können.

Die Validierung erfolgt dann entsprechend dem hierin offenbarten Verfahren zur Sicherheitsüberprüfung, wobei anstelle der realen Technikeinheit die teilweise oder vollständig simulierte Technikeinheit tritt.

Die hierin beschrieben Verfahren erlauben es, für die Sicherheitsüberprüfung Testfälle automatisiert zu finden, zu priorisieren, zugehörige Testvektoren zu identifizieren und Exploits zu generieren, eine automatisierte Durchführung der Sicherheitsüberprüfung zu definieren und die Auswertung der Testergebnisse automatisiert zu unterstützten. Dadurch lassen sich mit begrenzten (d.h. vorgegebenen) Testressourcen (zum Beispiel einer maximalen Testzeit) der größtmögliche Testerfolg erzielen. Das bedeutet, dass möglichst viele der relevanten (hoch-prioritären) Schwachstellen im Gesamtsystem (d.h. der Technikeinheit) mit möglichst hoher Wahrscheinlichkeit identifiziert werden können.

Das Verfahren erlaubt weiters, unter vorgegebenen Umständen (z.B. im Zuge eines „Black-Box-Testing“) bei zu Beginn nicht oder unvollständig vorhandener Information über die Technikeinheit (beispielsweise fehlende Details zur Systemarchitektur, den Anhängigkeiten der Komponenten und Unterkomponenten, den Merkmalen der Komponenten, den bekannten Schwachstellen, etc.), die relevanten Testvektoren zu identifizieren und die nötigen Testfälle auszuwählen bzw. zu generieren.

Bezugszeichen:

Technikeinheit 1

Prüfcomputersystem 2

Datenübertragungseinrichtung 3

Komponente 4

Modell 5

Prüfschnittstelle 6

Verbindungskanten 10

initiale Instanz 100

spezifizierte Instanz 101

erste plausible Modellvariante 102

alternative Modellvariante 103

Referenzen 104

Identifikationsebene 201

Komponentenebene 202

Unterkomponentenebene 203

Interaktionsebene 204

Modellknoten 100x

Informationsblock 110x

Patentansprüche

1. Verfahren zur Ermittlung zumindest einer ersten plausiblen Modellvariante einer Konfiguration einer Technikeinheit (1) mittels eines Prüfcomputersystems (2), wobei die Technikeinheit (1) zumindest eine Datenübertragungseinrichtung (3) und eine Vielzahl an Komponenten (4) aufweist, welche zu einer Datenkommunikation über die Datenübertragungseinrichtung (3) befähigt sind, und wobei das Verfahren die folgenden Schritte aufweist:

- Herstellen einer Verbindung zwischen einer Prüfschnittstelle (6) des Prüfcomputersystems (2) und der Datenübertragungseinrichtung (3) der Technikeinheit (1),
- Ermitteln einer initialen Instanz eines Modells (5) der Konfiguration der Technikeinheit (1),
- Entwickeln von spezifizierten Instanzen des Modells (5) ausgehend von der initialen Instanz durch eine Abfolge von Spezifizierungsvorgängen die jeweils zumindest die folgenden Schritte aufweisen:
  - Gegebenenfalls Ausführen einer Herausforderungsaktion,
  - Ermitteln eines für die Technikeinheit charakteristischen Verhaltens,
  - Analysieren des charakteristischen Verhaltens und Rückschließen auf zumindest ein Merkmal der tatsächlichen Konfiguration der Technikeinheit (1),
  - spezifizieren des Modells (5) mit dem zumindest einem ermittelten Merkmal,

  wobei zumindest ein Spezifizierungsvorgang von dem Prüfcomputersystem (2) automatisiert ausgeführt wird, und
- Identifizieren einer spezifizierten Instanz des Modells (5) als die erste plausible Modellvariante, wenn zumindest eine Bestimmtheitsbedingung erfüllt ist.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass der Schritt des Ermittelns eines für die Technikeinheit charakteristischen Verhaltens das Abhören von über die Datenübertragungseinrichtung (3) übermittelten Daten durch das Prüfcomputersystem (2) umfasst.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass Merkmale der tatsächlichen Konfiguration der Technikeinheit ausgewählt sind aus zumindest einem Merkmal einer Komponente (4) und/oder zumindest Beziehung zwischen Komponenten (4).

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass auf Basis der ersten plausiblen Modellvariante zumindest eine alternative Modellvariante erstellt wird.

5. Auf einem Prüfcomputersystem (2) ausgeführtes Verfahren zur Sicherheitsüberprüfung einer Technikeinheit (1), wobei zumindest eine erste plausible Modellvariante und gegebenenfalls eine Anzahl alternativer Modellvarianten ermittelt werden, vorzugsweise gemäß einem Verfahren nach einem der Ansprüche 1 bis 4, und wobei das Verfahren die folgenden Schritte aufweist:

- Zuordnen bekannter Schwachstellen zu Komponenten der Modellvarianten,
- Definieren eines Angriffsziels,
- Ermitteln zumindest eines auf das Angriffsziel bezogenen Angriffsmodells für die Modellvarianten,
- Gewichten der Knoten des Angriffsmodells hinsichtlich zumindest einer Bewertungsvariable,
- Ermitteln einer Bewertung zumindest eines Testvektors des Angriffsmodells hinsichtlich der Bewertungsvariable,
- Ermitteln eines Sicherheitswerts als pessimaler Werts aller Bewertungen und
- Ausgeben einer Sicherheitsbestätigung, wenn der Sicherheitswert einem Sicherheitskriterium entspricht.

6. Verfahren nach Anspruch 5, dadurch gekennzeichnet, dass das Verfahren weiters die folgenden Schritte aufweist:

- Ausführen zumindest eines auf Basis der ermittelten Schwachstellen ausgewählten Cyber-Angriffs auf die Technikeinheit (1),
- Auswerten des mit dem Cyber-Angriff erzielten Effekts und
- Eliminieren von Modellvarianten, für die der erzielte Effekt nicht schlüssig ist.

7. Verfahren nach Anspruch 5 oder 6, dadurch gekennzeichnet, dass das Verfahren weiters die folgenden Schritte aufweist:

- Ermitteln zumindest einer Software und/oder Firmware, die auf einer Komponente (4) der Technikeinheit (1) installiert ist,
- Spezifizieren der Software und/oder Firmware mit dem Prüfcomputersystem (2).

8. Verfahren nach einem der Ansprüche 5 bis 7, dadurch gekennzeichnet, dass das Verfahren weiters die folgenden Schritte aufweist:

- Ermitteln einer Software, die auf einer Komponente (4) der Technikeinheit (1) installiert ist,
- Erstellen simulierter Modellvarianten, welche eine spezifizierte Version der Software enthalten,
- Ermitteln eines Sicherheitswerts anhand der simulierten Modellvarianten.

9. Verfahren nach einem der Ansprüche 1 bis 8 dadurch gekennzeichnet, dass die Technikeinheit (1) ein Fahrzeug, und insbesondere ein autonomes Fahrzeug gemäß einer der SAE-Stufen 0 bis 5 gemäß der Norm SAE J3016 ist.

10. Computerprogrammprodukt, das direkt in den internen Speicher eines digitalen Computers geladen werden kann und Softwarecodeabschnitte umfasst, mit denen die Schritte gemäß einem der Ansprüche 1 bis 9 ausgeführt werden, wenn das Produkt auf dem Computer läuft.

11. Prüfcomputersystem (2) auf dem ein Computerprogrammprodukt gemäß Anspruch 10 läuft.

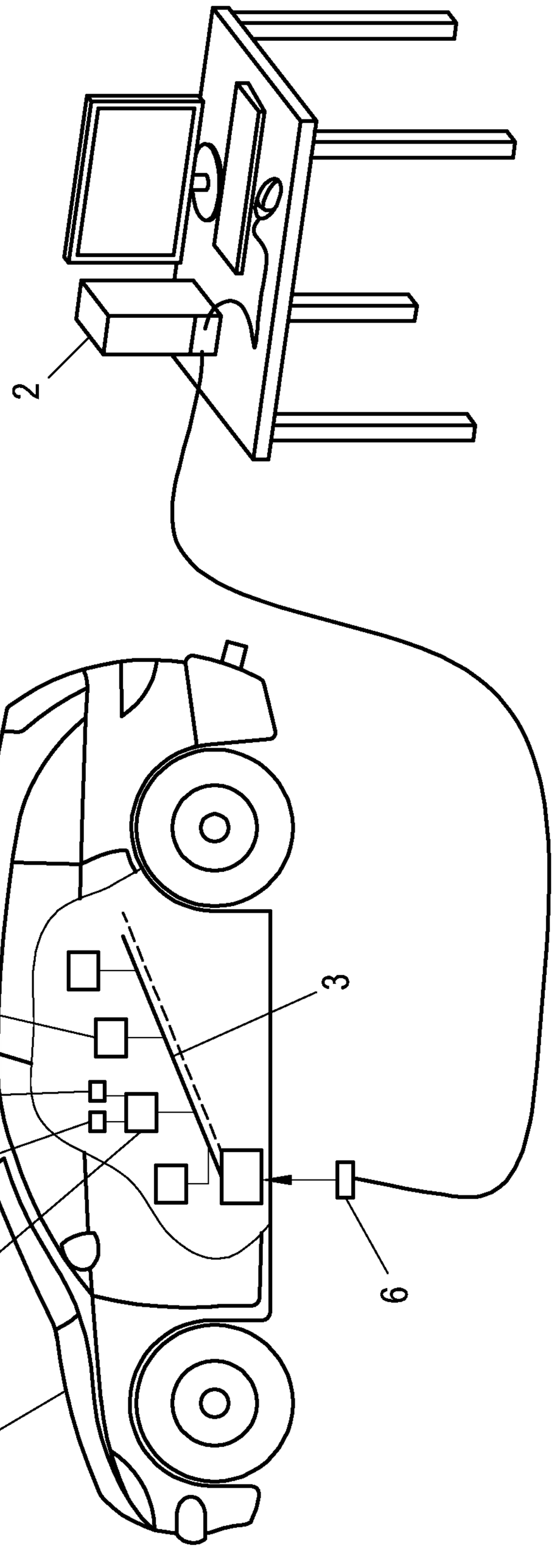

Fig. 1

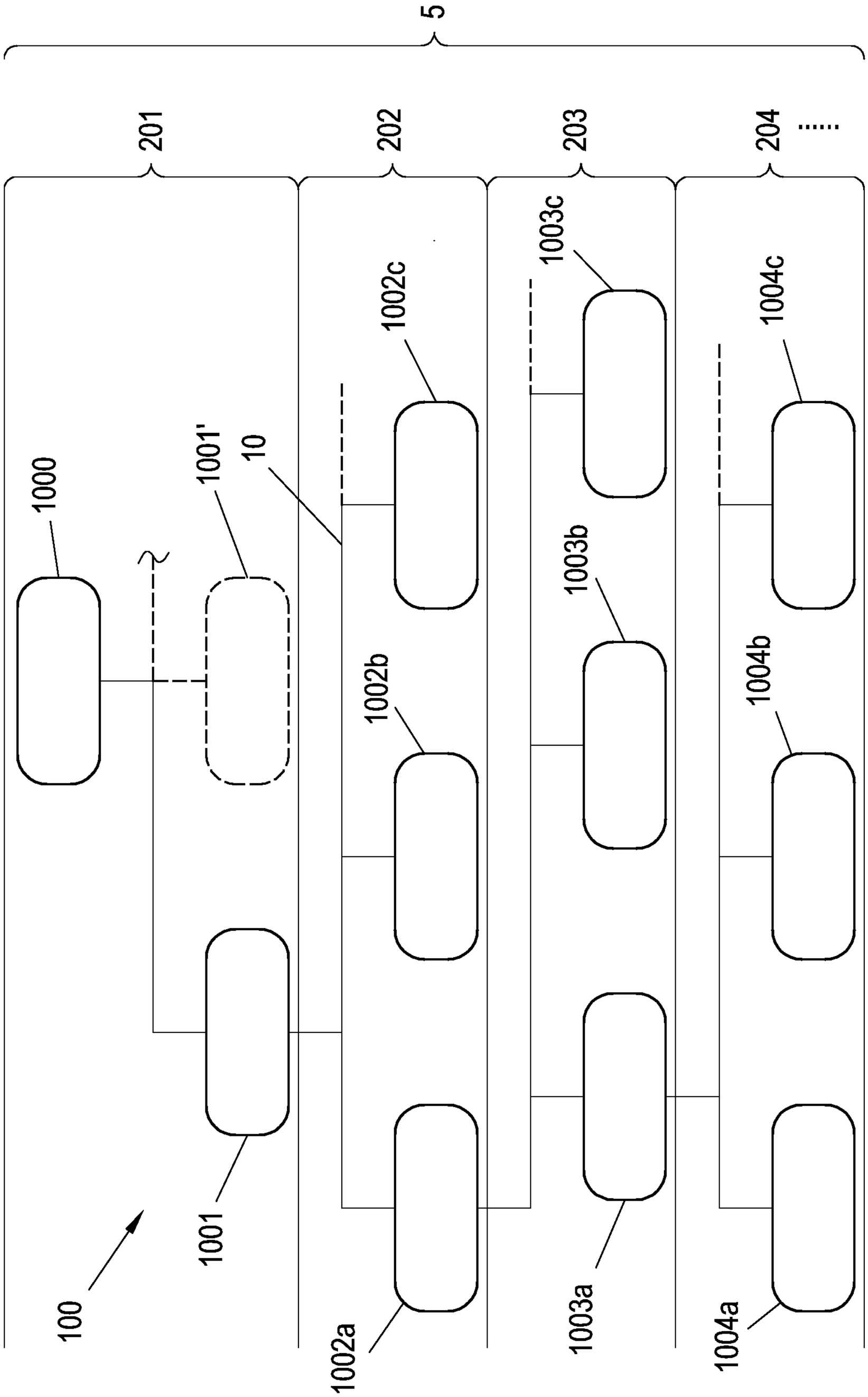
5
201
202
203
204
.....
1000
1001'
10
1002c
1003c
1004c
1003b
1002b
1004b
1001
100
1002a
1003a
1004a

Fig. 2

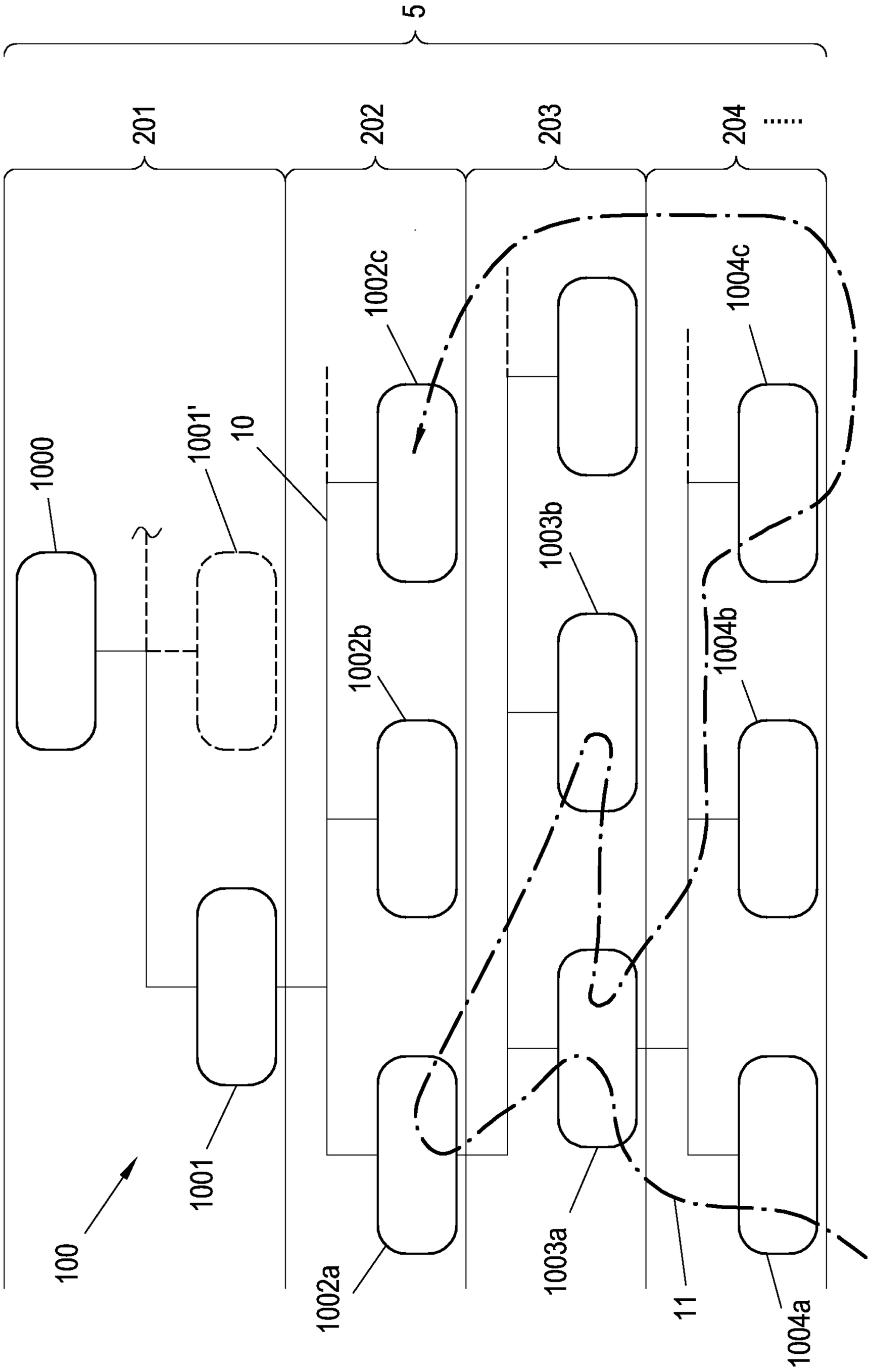
5
201
202
203
204
.....
1000
1001'
10
1002c
1004c
1003b
1002b
1004b
1001
100
1002a
1003a
11
1004a

Fig. 3

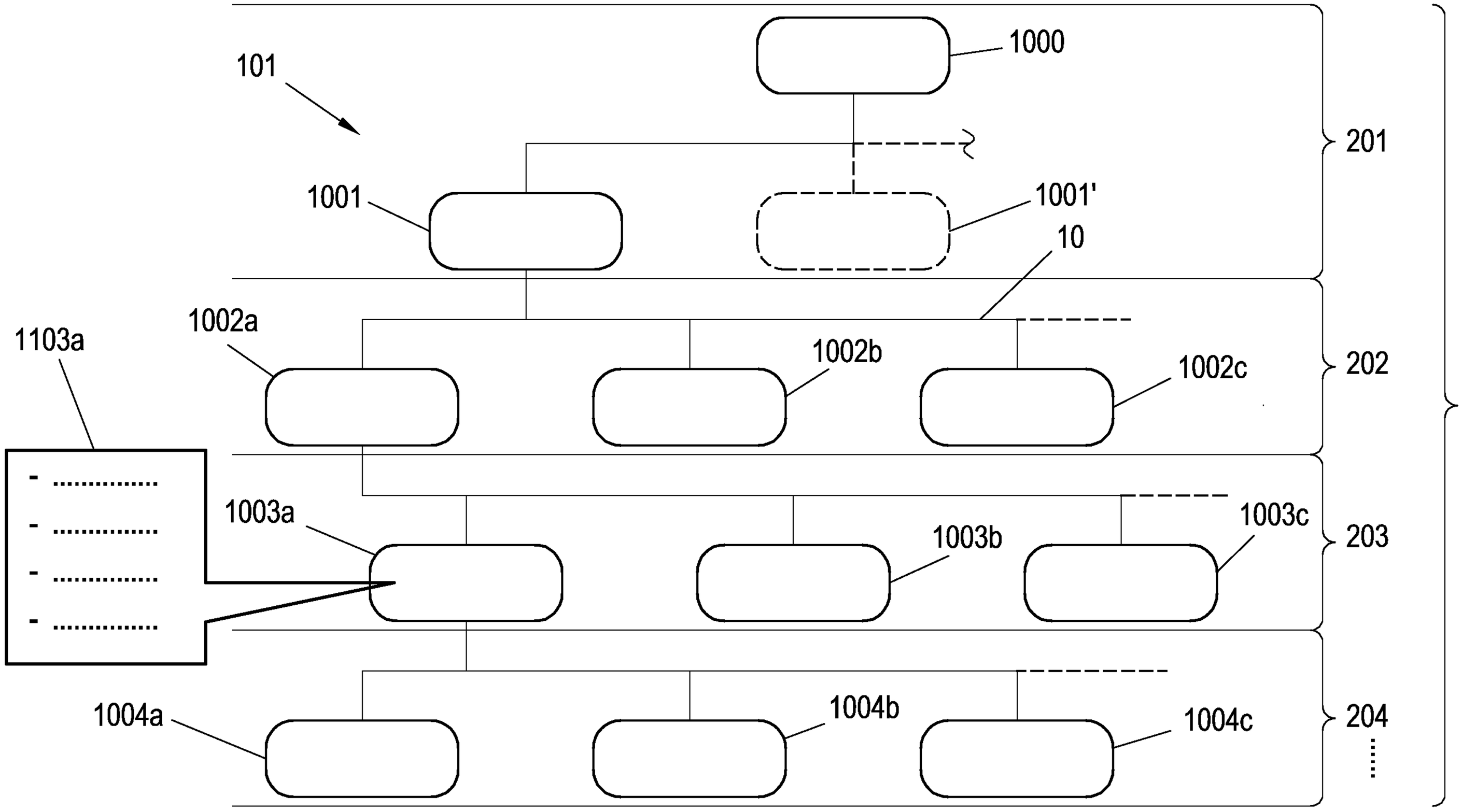
101
1000
1001
1001'
10
201
1002a
1002b
1002c
202
1103a
1003a
1003b
1003c
203
1004a
1004b
1004c
204
5

Fig. 4

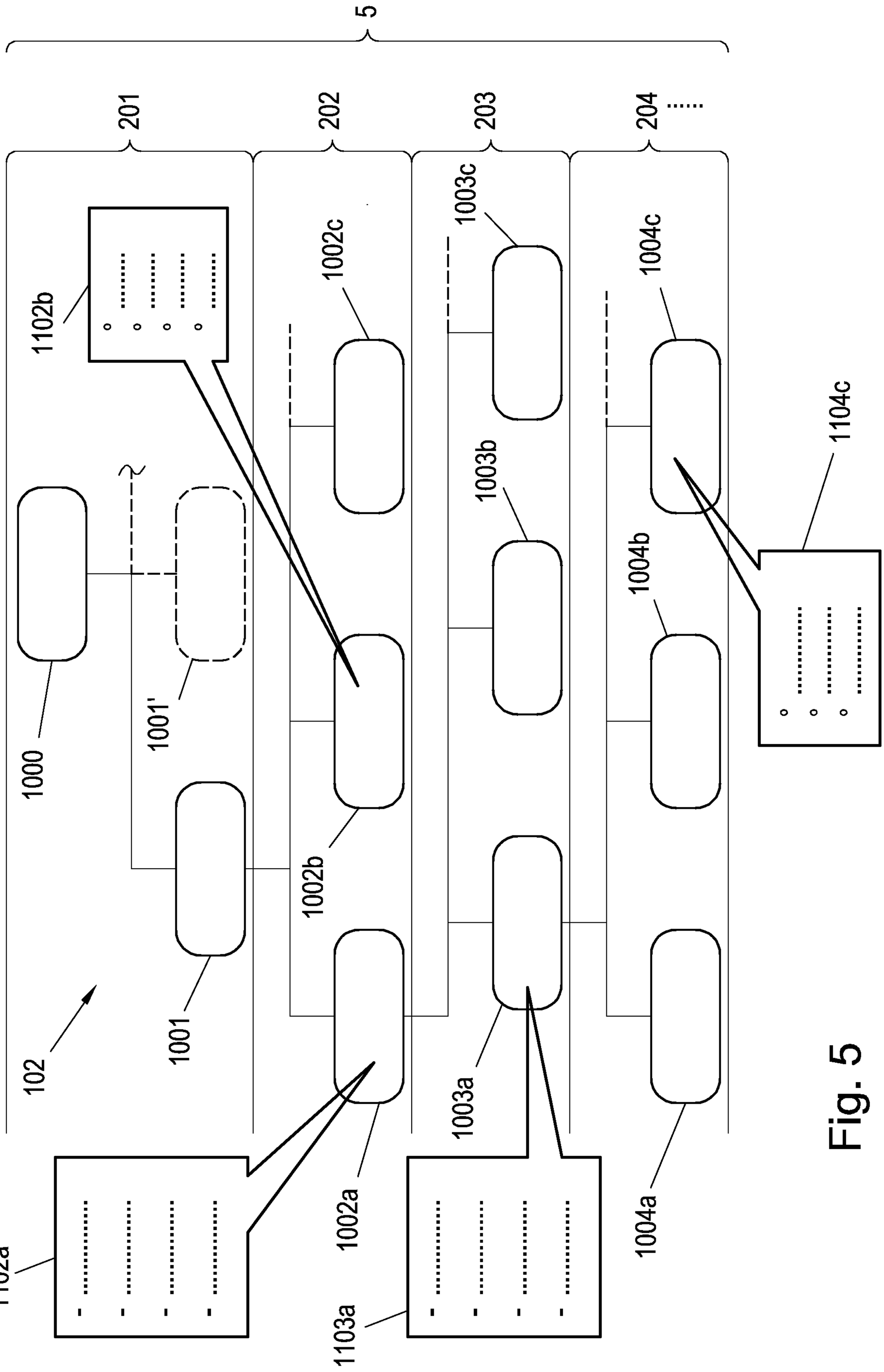
5
201
202
203
204
.....
1102b
1002c
1003c
1004c
1001'
1000
1001
1002b
1003b
1004b
1104c
102
1003a
1002a
1004a
1102a
1103a

Fig. 5

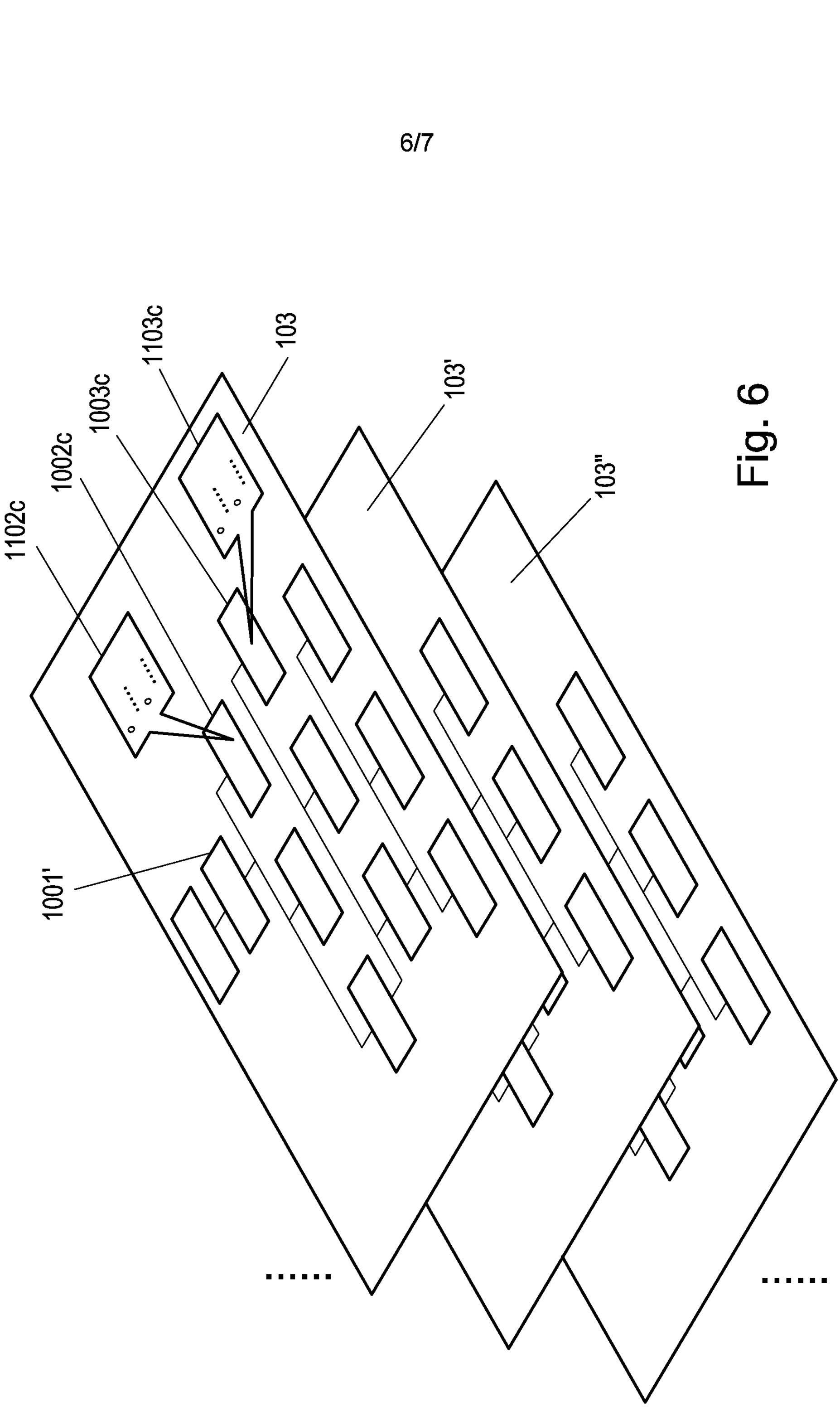

Fig. 6

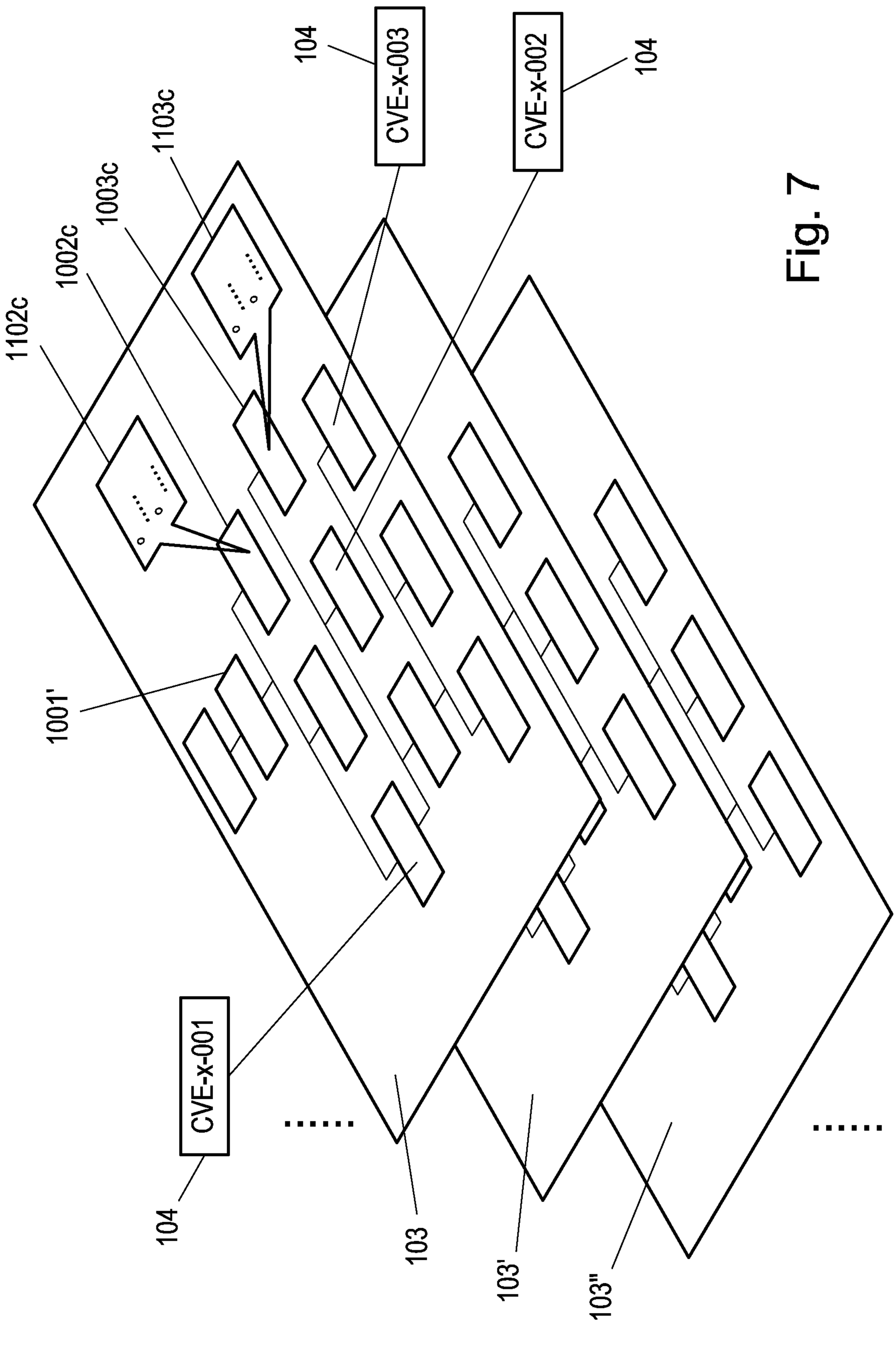
1001'
CVE-x-001
104
CVE-x-002
104
CVE-x-003
104
1102c
1002c
1003c
1103c
103
103'
103"

Fig. 7

Recherchenbericht zu **A 50536/2019**

österreichisches patentamt

Klassifikation des Anmeldungsgegenstands gemäß IPC: ***F02D 41/26*** (2006.01); ***G06F 30/33*** (2020.01); ***G06F 30/20*** (2020.01); ***G06F 30/15*** (2020.01)
Klassifikation des Anmeldungsgegenstands gemäß CPC: ***F02D 41/26*** (2013.01); ***G06F 30/33*** (2020.01); ***G06F 30/20*** (2020.01); ***G06F 30/15*** (2020.01)
Recherchierter Prüfstoff (Klassifikation): F02D, G06F
Konsultierte Online-Datenbank: WPIAP; EPODOC; TXTEN; TXTDE; INSPEC; NPL; Internet
Dieser Recherchenbericht wurde zu den am **14.06.2019** eingereichten Ansprüchen **1-11** erstellt.

Kategorie*)	Bezeichnung der Veröffentlichung: Ländercode, Veröffentlichungsnummer, Dokumentart (Anmelder), Veröffentlichungsdatum, Textstelle oder Figur soweit erforderlich	Betreffend Anspruch
X	WO 2016170063 A1 (AVL LIST GMBH) 27. Oktober 2016 (27.10.2016) Siehe besonders Zusammenfassung; Fig. 6, 10, 12 und die dazugehörigen Figuren- beschreibungen; Seite 5, Zeilen 22 - Seite 6, Zeile 7; Seite 6, Zeile 3; Seite 17, Zeilen 4-17; Patentansprüche 1 bis 25	1, 3, 4, 10 und 11
A		2, 5-9
A	EP 1150186 A1 (AVL LIST GMBH [AT]) 31. Oktober 2001 (31.10.2001) Siehe besonders Zusammenfassung; Fig. 2 und die dazugehörige Figurenbeschreibung; Paragraphen 1 bis 4 (insbesonders Paragraphen 4, 5 und 18); Patentansprüche 1 bis 11	1-4
A	WO 2017178015 A1 (IAV GMBH INGENIEURGESELLSCHAFT AUTO & VERKEHR) 19. Oktober 2017 (19.10.2017) Siehe besonders Zusammenfassung; Fig. 1; Figuren-beschreibung; Seiten 1 bis 12; Patentansprüche 1 bis 10	1-4
A	SCHULDT Fabian et al. "Effiziente systematische Testgenerierung für Fahrerassistenzsysteme in virtuellen Umgebungen" 10.07.2013; Technische Universität Braunschweig, Institut für Regelungstechnik & Vokswagen AG; abgerufen im Internet am 30.04.2020 unter dem Link <URL:https://publikationsserver.tu-braunschweig.de/servlets/MCRFileNodeServlet/dbbs_derivate_00031187/AAET_Schuldt_Saust_Lichte_Maurer_Scholz.pdf> Siehe Seiten 1 bis 20	5-11
A	SPARSH Sharma et al. "A survey on Intrusion Detection Systems and Honeypot based proactive security mechanisms in VANETs and VANET Cloud" 20.04.2018; Vehicular Communications12 (2018); abgerufen im Internet am 30.04.2020 unter dem Link <https://www.sciencedirect.com/science/article/pii/S2214209617302784> Siehe Seiten 138-164	5-11

Datum der Beendigung der Recherche:	Seite 1 von 2	Prüfer(in):
30.04.2020		KÖGL Christian

*) **Kategorien** der angeführten Dokumente:

X Veröffentlichung **von besonderer Bedeutung**: der Anmeldungsgegenstand kann allein aufgrund dieser Druckschrift nicht als neu bzw. auf erfinderischer Tätigkeit beruhend betrachtet werden.

Y Veröffentlichung **von Bedeutung**: der Anmeldungsgegenstand kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren weiteren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese **Verbindung für einen Fachmann naheliegend** ist.

A Veröffentlichung, die den allgemeinen **Stand der Technik** definiert.

P Dokument, das von **Bedeutung** ist (Kategorien **X** oder **Y**), jedoch **nach dem Prioritätstag** der Anmeldung veröffentlicht wurde.

E Dokument, das **von besonderer Bedeutung** ist (Kategorie **X**), aus dem ein „**älteres Recht**“ hervorgehen könnte (früheres Anmeldedatum, jedoch nachveröffentlicht, Schutz ist in Österreich möglich, würde Neuheit in Frage stellen).

& Veröffentlichung, die Mitglied der selben **Patentfamilie** ist.

Fortsetzung des Recherchenberichts zu **A 50536/2019**
Seite 2 von 2

österreichisches patentamt

Kategorie*)	Bezeichnung der Veröffentlichung: Ländercode, Veröffentlichungsnummer, Dokumentart (Anmelder), Veröffentlichungsdatum, Textstelle oder Figur soweit erforderlich	Betreffend Anspruch

Patentansprüche

1. Verfahren zur Sicherheitsüberprüfung einer Technikeinheit (1), wobei die Technikeinheit (1) zumindest eine Datenübertragungseinrichtung (3) und eine Vielzahl an Komponenten (4) aufweist, welche zu einer Datenkommunikation über die Datenübertragungseinrichtung (3) befähigt sind, wobei aus einer initialen Instanz eines Konfigurationsmodells der Technikeinheit durch Spezifizierungsvorgänge zumindest eine erste plausible Modellvariante und gegebenenfalls eine Anzahl alternativer Modellvarianten ermittelt werden, wobei jedes Konfigurationsmodell und jede Modellvariante einer systematischen Abbildung der Konfiguration der Technikeinheit entspricht, wobei die erste plausible Modellvariante einer Bestimmtheitsbedingung entspricht, wobei die Bestimmtheitsbedingung feststellt, dass die erste plausible Modellvariante ausreichend bestimmt ist, um eine Sicherheitsüberprüfung in einer vorgegebenen Zeit zu ermöglichen, wobei das Verfahren auf einem Prüfcomputersystem (2) ausgeführt wird, und wobei das Verfahren die folgenden Schritte aufweist:

   - Zuordnen bekannter Schwachstellen zu Komponenten der Modellvarianten,
   - Definieren eines Angriffsziels durch Auswählen aus einer Liste an abzuarbeitenden Angriffszielen,
   - Ermitteln zumindest eines auf das Angriffsziel bezogenen Angriffsmodells für die Modellvarianten,
   - Gewichten der Knoten des Angriffsmodells hinsichtlich zumindest einer Bewertungsvariable,
   - Ermitteln einer Bewertung zumindest eines Testvektors des Angriffsmodells hinsichtlich der Bewertungsvariable,
   - Ermitteln eines Sicherheitswerts als pessimaler Werts aller Bewertungen und
   - Ausgeben einer Sicherheitsbestätigung, wenn der Sicherheitswert einem Sicherheitskriterium entspricht.

2. Verfahren nach Anspruch 1, wobei die zumindest eine erste plausible Modellvariante und gegebenenfalls die Anzahl alternativer Modellvarianten gemäß einem Verfahren zur Ermittlung zumindest einer ersten plausiblen Modellvariante einer Konfiguration der Technikeinheit (1) mittels des Prüfcomputersystems (2) ermittelt werden, welches die folgenden Schritte aufweist:

   - Herstellen einer Verbindung zwischen einer Prüfschnittstelle (6) des Prüfcomputersystems (2) und der Datenübertragungseinrichtung (3) der Technikeinheit (1),

- Ermitteln einer initialen Instanz eines Modells (5) der Konfiguration der Technikeinheit (1), wobei die initiale Instanz des Modells (5) ein generisches Modell oder ein spezifischeres Modell der Technikeinheit ist,
- Entwickeln von spezifizierten Instanzen des Modells (5) ausgehend von der initialen Instanz durch eine Abfolge von Spezifizierungsvorgängen die jeweils zumindest die folgenden Schritte aufweisen:
    - Gegebenenfalls Ausführen einer Herausforderungsaktion,
    - Ermitteln eines für die Technikeinheit charakteristischen Verhaltens durch Abhören einer Datenkommunikation über die Datenübertragungseinrichtung oder durch eine andere Messung,
    - Analysieren des charakteristischen Verhaltens und Rückschließen auf zumindest ein Merkmal der tatsächlichen Konfiguration der Technikeinheit (1),
    - spezifizieren des Modells (5) mit dem zumindest einem ermittelten Merkmal,

  wobei zumindest ein Spezifizierungsvorgang von dem Prüfcomputersystem (2) automatisiert ausgeführt wird, und
- Identifizieren einer spezifizierten Instanz des Modells (5) als die erste plausible Modellvariante, wenn zumindest eine Bestimmtheitsbedingung erfüllt ist.

3. Verfahren zur Ermittlung zumindest einer ersten plausiblen Modellvariante einer Konfiguration einer Technikeinheit (1) mittels eines Prüfcomputersystems (2), wobei die Technikeinheit (1) zumindest eine Datenübertragungseinrichtung (3) und eine Vielzahl an Komponenten (4) aufweist, welche zu einer Datenkommunikation über die Datenübertragungseinrichtung (3) befähigt sind, und wobei das Verfahren die folgenden Schritte aufweist:

- Herstellen einer Verbindung zwischen einer Prüfschnittstelle (6) des Prüfcomputersystems (2) und der Datenübertragungseinrichtung (3) der Technikeinheit (1),
- Ermitteln einer initialen Instanz eines Modells (5) der Konfiguration der Technikeinheit (1), wobei die initiale Instanz des Modells (5) ein generisches Modell oder ein spezifischeres Modell der Technikeinheit ist,
- Entwickeln von spezifizierten Instanzen des Modells (5) ausgehend von der initialen Instanz durch eine Abfolge von Spezifizierungsvorgängen die jeweils zumindest die folgenden Schritte aufweisen:
    - Gegebenenfalls Ausführen einer Herausforderungsaktion,

- Ermitteln eines für die Technikeinheit charakteristischen Verhaltens durch Abhören einer Datenkommunikation über die Datenübertragungseinrichtung oder durch eine andere Messung,
- Analysieren des charakteristischen Verhaltens und Rückschließen auf zumindest ein Merkmal der tatsächlichen Konfiguration der Technikeinheit (1),
- spezifizieren des Modells (5) mit dem zumindest einem ermittelten Merkmal, wobei zumindest ein Spezifizierungsvorgang von dem Prüfcomputersystem (2) automatisiert ausgeführt wird, und
  - Identifizieren einer spezifizierten Instanz des Modells (5) als die erste plausible Modellvariante, wenn zumindest eine Bestimmtheitsbedingung erfüllt ist, wobei die Bestimmtheitsbedingung feststellt, dass die erste plausible Modellvariante ausreichend bestimmt ist, um eine Sicherheitsüberprüfung in einer vorgegebenen Zeit zu ermöglichen.

4. Verfahren nach Anspruch 2 oder 3, dadurch gekennzeichnet, dass der Schritt des Ermittelns eines für die Technikeinheit charakteristischen Verhaltens das Abhören von über die Datenübertragungseinrichtung (3) übermittelten Daten durch das Prüfcomputersystem (2) umfasst.

5. Verfahren nach einem der Ansprüche 2 bis 4, dadurch gekennzeichnet, dass Merkmale der tatsächlichen Konfiguration der Technikeinheit ausgewählt sind aus zumindest einem Merkmal einer Komponente (4) und/oder zumindest Beziehung zwischen Komponenten (4).

6. Verfahren nach einem der Ansprüche 2 bis 5, dadurch gekennzeichnet, dass auf Basis der ersten plausiblen Modellvariante zumindest eine alternative Modellvariante erstellt wird.

7. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass das Verfahren weiters die folgenden Schritte aufweist:

- Ausführen zumindest eines auf Basis der ermittelten Schwachstellen ausgewählten Cyber-Angriffs auf die Technikeinheit (1),
- Auswerten des mit dem Cyber-Angriff erzielten Effekts und
- Eliminieren von Modellvarianten, für die der erzielte Effekt nicht schlüssig ist.

8. Verfahren nach Anspruch 1 oder 7, dadurch gekennzeichnet, dass das Verfahren weiters die folgenden Schritte aufweist:

- Ermitteln zumindest einer Software und/oder Firmware, die auf einer Komponente (4) der Technikeinheit (1) installiert ist,
- Spezifizieren der Software und/oder Firmware mit dem Prüfcomputersystem (2).

9. Verfahren nach einem der Ansprüche 1 oder 7 bis 8, dadurch gekennzeichnet, dass das Verfahren weiters die folgenden Schritte aufweist:

- Ermitteln einer Software, die auf einer Komponente (4) der Technikeinheit (1) installiert ist,
- Erstellen simulierter Modellvarianten, welche eine spezifizierte Version der Software enthalten,
- Ermitteln eines Sicherheitswerts anhand der simulierten Modellvarianten.

10. Verfahren nach einem der Ansprüche 1 bis 9 dadurch gekennzeichnet, dass das Verfahren an einer Technikeinheit (1) ausgeführt wird, die ein Fahrzeug, und insbesondere ein autonomes Fahrzeug gemäß einer der SAE-Stufen 0 bis 5 gemäß der Norm SAE J3016 ist.

11. Computerprogrammprodukt, das direkt in den internen Speicher eines digitalen Computers geladen werden kann und Softwarecodeabschnitte umfasst, mit denen die Schritte gemäß einem der Ansprüche 1 bis 10 ausgeführt werden, wenn das Produkt auf dem Computer läuft.

12. Prüfcomputersystem (2) auf dem ein Computerprogrammprodukt gemäß Anspruch 11 läuft.