(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
3. Dezember 2015 (03.12.2015)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2015/180932 A1

(51) Internationale Patentklassifikation:
G06F 11/27 (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2015/059816

(22) Internationales Anmeldedatum:
5. Mai 2015 (05.05.2015)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2014 209 969.2 26. Mai 2014 (26.05.2014) DE

(71) Anmelder: **SIEMENS AKTIENGESELLSCHAFT** [DE/DE]; Wittelsbacherplatz 2, 80333 München (DE).

(72) Erfinder: **FRÖHLICH, Joachim**; Grillparzerstraße 31, 81675 München (DE). **ROTHBAUER, Stefan**; Dr.-Zamenhof-Str. 16, 86156 Augsburg (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

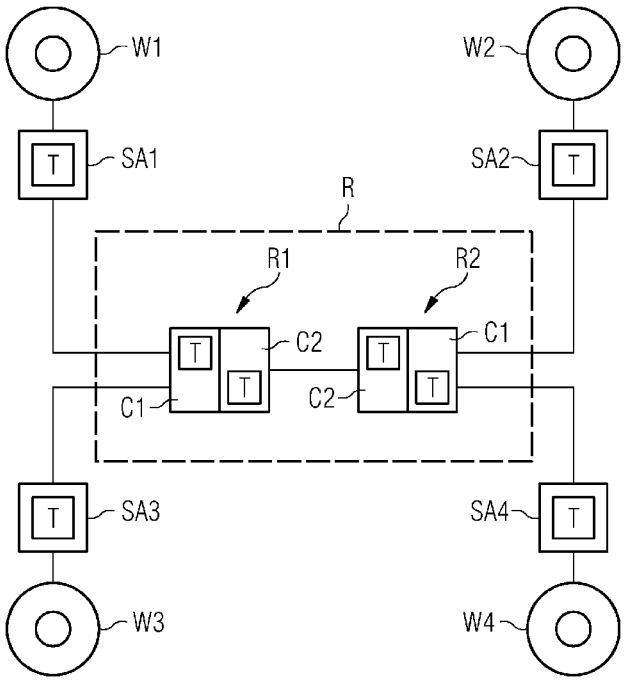
(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

[Fortsetzung auf der nächsten Seite]

(54) **Title**: METHOD FOR TESTING A TECHNICAL SYSTEM IN A COMPUTER-ASSISTED MANNER

(54) **Bezeichnung** : VERFAHREN ZUM RECHNERGESTÜTZTEN TESTEN EINES TECHNISCHEN SYSTEMS

FIG 1



(57) **Abstract**: The invention relates to a method for testing a technical system in a computer-assisted manner, wherein cyclically specified time slots which can be used solely for testing the technical system are reserved on the basis of a specified clock pulse, and a respective test probe (T) is integrated into one or more computer nodes (R1, R2,..., SA4) of the technical system. An internal test program (ITP) which is stored in each test probe (T) is ran by the respective test probe (T) when testing the technical system, and the respective test probe (T) accesses a system database (S-DB) by means of the internal test program (ITP), said database containing data in the form of state data of the technical system and being stored in the computer node (R1, R2, SA4) in which the respective test probe (T) is integrated.

(57) **Zusammenfassung**: Die Erfindung betrifft ein Verfahren zum rechnergestützten Testen eines technischen Systems, bei dem basierend auf einem vorgegebenen Takt zyklisch vorbestimmte

[Fortsetzung auf der nächsten Seite]

WO 2015/180932 A1

Veröffentlicht:

— *mit internationalem Recherchenbericht (Artikel 21 Absatz 3)*

Zeitschlitze reserviert werden, welche ausschließlich zum Testen des technischen Systems nutzbar sind, und in einem oder mehreren Rechnerknoten (R1, R2,..., SA4) des technischen Systems jeweils eine Testsonde (T) integriert ist. Durch eine jeweilige Testsonde (T) wird beim Testen des technischen Systems ein internes Testprogramm (ITP) ausgeführt, das in der jeweiligen Testsonde (T) hinterlegt ist, wobei die jeweilige Testsonde (T) mittels des internen Testprogramms (ITP) auf eine System-Datenbank (S-DB) zugreift, die Daten in der Form von Zustandsdaten des technischen Systems enthält und in dem Rechnerknoten (R1, R2,..., SA4) hinterlegt ist, in dem die jeweilige Testsonde (T) integriert ist.

Beschreibung

Verfahren zum rechnergestützten Testen eines technischen Systems

Die Erfindung betrifft ein Verfahren zum rechnergestützten Testen eines technischen Systems sowie ein technisches System.

In technischen Systemen und insbesondere in Software-intensiven, sicherheitskritischen technischen Systemen müssen Funktionen in Echtzeit zuverlässig ausgeführt werden. Mit Tests dieser Systeme wird die Funktionstüchtigkeit und Rechtzeitigkeit von Mechanismen geprüft, die das technische System zur Entdeckung und Behandlung seltener Situationen implementiert. Die Tests prüfen zum Beispiel, ob das technische System innerhalb einer bestimmten Zeitspanne nach einem permanenten Fehler sicher ausfällt oder einen betriebssicheren Funktionsmodus erreicht. Die Tests müssen dabei Ereignisse nachstellen, insbesondere zeitlich korreliert in unterschiedlichen Systemteilen (verteilt auf verschiedene Rechnerknoten), die den Sicherungsmechanismus punktgenau auslösen sollen, ohne Funktionen und Laufzeit des getesteten technischen Systems zu beeinträchtigen. Andernfalls sind Testresultate unzuverlässig, da sich bei Eintritt eines Fehlers das System im Testbetrieb anders verhält als im Produktivbetrieb.

Aus dem Stand der Technik sind verschiedene Standards bekannt, die bestimmte Tests für technische Systeme fordern (z.B. Standard IEC 61508). In technischen Systemen mit einem hohen Software-Anteil ist es oftmals schwierig, diese Systeme konform zu den entsprechenden Standards zu testen.

Aus dem Stand der Technik sind Ansätze bekannt, gemäß denen in einem technischen System Messsonden integriert werden, welche dauerhaft in dem technischen System eingebaut sind. Die Messsonden kommunizieren mit einem externen Testsystem. Mit diesem externen Testsystem werden die Tests durchgeführt.

Die Kommunikation zwischen Messsonden und externem Testsystem über ein Netzwerk verzögert Tests und verringert deren Genauigkeit und Aussagekraft.

Aufgabe der Erfindung ist es, ein Verfahren zum rechnergestützten Testen eines technischen Systems bereitzustellen, mit dem das technische System einfach und schnell getestet werden kann.

Diese Aufgabe wird durch die unabhängigen Patentansprüche gelöst. Weiterbildungen der Erfindung sind in den abhängigen Ansprüchen definiert.

Das erfindungsgemäße Verfahren dient zum rechnergestützten Testen eines technischen Systems, wobei basierend auf einem vorgegebenen Takt zyklisch vorbestimmte Zeitschlitze reserviert werden, welche ausschließlich zum Testen des technischen Systems nutzbar sind. Mit anderen Worten wird das erfindungsgemäße Verfahren für ein zeitgesteuertes technisches System eingesetzt, das in einem vorgegebenen Takt arbeitet und seine Funktionen nur innerhalb entsprechend definierter Zeitschlitze durchführt. Im Unterschied zu Ereignis-gesteuerten Systemen reagieren zeitgesteuerte Systeme zu genau bestimmbaren Zeitpunkten auf externe Ereignisse. Im erfindungsgemäßen Verfahren werden vorbestimmte Zeitschlitze innerhalb eines Taktzyklus ausschließlich zum Testen des technischen Systems verwendet. Die restlichen Zeitschlitze des Taktzyklus dienen zur Durchführung der Kernfunktionen des technischen Systems.

Zur Durchführung der Tests ist in einem oder mehreren Rechnerknoten des technischen Systems jeweils eine Testsonde integriert, wobei durch eine jeweilige Testsonde beim Testen des technischen Systems ein internes Testprogramm ausgeführt wird, das in der jeweiligen Testsonde hinterlegt ist, und wobei die Testsonde mittels des internen Testprogramms auf eine System-Datenbank zugreift, die Daten in der Form von Zustandsdaten des technischen Systems enthält und in dem Rech-

nerknoten hinterlegt ist, in dem die jeweilige Testsonde integriert ist.

Der Begriff der Zustandsdaten des technischen Systems ist weit zu verstehen und kann verschiedenste Daten über den Betriebszustand des technischen Systems umfassen. Unter Zustandsdaten fallen neben den Daten zum Systemzustand auch Signaldaten von einzelnen Sensoren und/oder Aktoren. Insbesondere ist zu beachten, dass mittels der Zustandsdaten seltene oder kritische Betriebszustände des technischen Systems im Testbetrieb durch Manipulation der System-Datenbank über die Testsonde gezielt eingestellt und hierdurch simuliert werden können.

Unter Rechnerknoten des technischen Systems sind separate Einheiten mit Software und Hardware zu verstehen. Bei mehreren Rechnerknoten sind diese in geeigneter Weise über eine Kommunikationsinfrastruktur, wie z.B. Ethernet, miteinander vernetzt. Beispiele von Rechnerknoten sind separate Rechner bzw. Sensoren und/oder Aktoren im technischen System. In einer besonders bevorzugten Ausführungsform sind die Rechnerknoten zur Erfüllung von Sicherheitsanforderungen zumindest zum Teil redundant ausgeführt. Redundanz bedeutet, dass ein Rechnerknoten aus mindestens 2 Kanälen zur Prüfung der Datenintegrität des Rechnerknotens besteht und/oder dass ein Rechnerknoten die Aufgabe eines anderen Rechnerknotens übernehmen kann, sobald der andere Rechnerknoten ausfällt, etwa bei Verletzung der Datenintegrität.

Das erfindungsgemäße Verfahren ermöglicht durch Testsonden mit lokalen Testprogrammen in Rechnerknoten des technischen Systems eine schnelle, zuverlässige und taktgenaue Durchführung von Tests. Das Ergebnis der Tests kann auf den Testsonden gespeichert werden bzw. über eine Schnittstelle daraus gelesen werden. Die gelesenen Ergebnisse können einem Benutzer über eine Benutzerschnittstelle ausgegeben werden. Der Benutzer erhält hierdurch Informationen über das Verhalten des technischen Systems bei Durchführung des Tests. Zum Bei-

spiel erhält der Benutzer über die Benutzerschnittstelle die Rückmeldung, ob ein Test, der Fehler in das technische System injiziert, zu einem sicherheitskritischen Zustand des technischen Systems führt.

Die System-Datenbank, auf welche die jeweilige Testsonde zugreift, umfasst vorzugsweise Zustandsdaten des Rechnerknotens, in dem die jeweilige Testsonde integriert ist. Bei mehreren Rechnerknoten umfassen die Zustandsdaten bevorzugt auch Zustandsdaten zu weiteren Rechnerknoten des technischen Systems. Vorzugsweise umfasst die System-Datenbank ferner Zustandsdaten zu der jeweiligen Testsonde selbst. Hierdurch können Tests des gesamten technischen Systems und insbesondere auch der Testsonde selbst durchgeführt werden.

In einer besonders bevorzugten Variante werden durch eine jeweilige Testsonde zumindest manchmal in einem vorbestimmten Zeitschlitz mittels des internen Testprogramms mehrere Operationen durchgeführt. Diese Operationen umfassen das Lesen von Daten aus der System-Datenbank, die Auswertung der gelesenen Daten sowie eine Veränderung der Daten in der System-Datenbank. Hierdurch wird mittels des internen Testprogramms eine schnelle Ausführung entsprechender Tests mit lokaler Auswertung der Daten ermöglicht. Diese Variante trägt zur taktgenauen Ausführung der Tests bei.

In einer weiteren bevorzugten Ausführungsform erfolgt der Zugriff einer jeweiligen Testsonde auf die System-Datenbank basierend auf Befehlen folgender Befehlstypen:

- einen Befehlstyp zum Lesen von Daten aus der System-Datenbank;
- einen Befehlstyp zum Ändern von Daten in der System-Datenbank.

In der detaillierten Beschreibung werden diese Befehlstypen beispielhaft als „monitor“ und „manipulate“ bezeichnet.

In einer besonders bevorzugten Variante führt die jeweilige Testsonde mittels des internen Testprogramms ferner Befehle von einem Befehlstyp aus, der überprüft, ob vorbestimmte Aussagen (im Folgenden auch als Test-Aussagen bezeichnet) über in der System-Datenbank hinterlegte Zustände des technischen Systems erfüllt sind. Dieser Befehlstyp wird in der speziellen Beschreibung beispielhaft als „assert" bezeichnet.

Vorzugsweise führt eine jeweilige Testsonde mittels des internen Testprogramms ferner Befehle von Befehlstypen aus, mit denen der Betrieb des Rechnerknotens, in dem die jeweilige Testsonde integriert ist, angehalten wird und/oder mit denen der Betrieb des Rechnerknotens, in dem die jeweilige Testsonde integriert ist, fortgesetzt wird. Der Betrieb kann temporär angehalten werden. Dabei bleibt jedoch (ausschließlich) die Testsonde im Betrieb. Hierzu wird in der speziellen Beschreibung beispielhaft der Befehl „stop" verwendet. Ebenso kann der Betrieb des Rechnerknotens dauerhaft angehalten und damit beendet werden. Dieser Befehl ist in der speziellen Beschreibung beispielhaft mit „exit" bezeichnet. Demgegenüber ist der Befehl des Fortsetzens des Betriebs des technischen Systems in der speziellen Beschreibung beispielhaft mit „continue" bezeichnet.

In einer weiteren bevorzugten Ausführungsform werden für zumindest einen Teil der Befehle der Befehlstypen und insbesondere alle Befehle der Befehlstypen vorbestimmte Bedingungen spezifiziert, wobei bei Erfüllung der vorbestimmten Bedingungen der entsprechende Befehl ausgelöst wird. Die vorbestimmten Bedingungen können z.B. in den entsprechenden Befehlen hinterlegt sein bzw. in separaten Registern gespeichert sein.

In einer weiteren bevorzugten Variante sind die vorbestimmten Bedingungen über relationale Ausdrücke und boolesche Ausdrücke spezifizierbar. Vorzugsweise sind auch die oben genannten vorbestimmten Test-Aussagen über relationale Ausdrücke und boolesche Ausdrücke spezifizierbar. Mit dieser Ausführungsform können auch komplexe Bedingungen bzw. Aussagen für die

entsprechenden Befehle formuliert werden. Relationale Ausdrücke setzen zwei Bestandteile in einer Bedingung bzw. Aussage in Beziehung zueinander. Beispiele von relationalen Ausdrücken finden sich in der speziellen Beschreibung. Die Testsonde kann einzelne und zusammengesetzte relationale und boolesche Ausdrücke im Takt des Systems unter Test auswerten. Das ermöglicht taktgenaue Testaussagen.

In einer weiteren Ausführungsform sind für jeden Befehlstyp ein oder mehrere Befehlsregister vorgesehen, in denen die jeweiligen im aktuellen Zeitschlitz auszuführenden Befehle des entsprechenden Befehlstyps enthalten sind.

In einer weiteren bevorzugten Variante des erfindungsgemäßen Verfahrens sind für zumindest einen Teil der Testsonden jeweils neben der System-Datenbank eine oder mehrere weitere Datenbanken (im Folgenden auch als Test-Datenbanken bezeichnet) mit Daten in der Form von Zustandsdaten des technischen Systems vorgesehen, wobei die weitere oder weiteren Test-Datenbank in dem Rechnerknoten hinterlegt sind, in dem die jeweilige Testsonde integriert ist, und wobei die jeweilige Testsonde mittels des internen Testprogramms auf die weitere oder weiteren Test-Datenbanken zugreift. Über eine weitere Test-Datenbank kann beispielsweise vorbereitend zur Ausführung eines Tests durch Veränderung der Daten in dieser Test-Datenbank ein Betriebsszenario aufgebaut werden, das dann zu einem späteren Zeitpunkt im Rahmen des Tests verwendet wird. Die Vorbereitung von Tests über Test-Datenbanken kommt insbesondere dann zum Einsatz, wenn umfangreiche Manipulationen in den Zustandsdaten erforderlich sind (zu umfangreich, um sie einzeln in Echtzeit in einem Zeitschlitz durchzuführen). Die Verwendung mehrerer, Testsonden-spezifischer Datenbanken (d.h. der System-Datenbank und zumindest einer Test-Datenbank) hat den Vorteil, dass hierdurch das Zeitverhalten der Tests verbessert wird. Nach Testvorbereitung und nach Auslösen eines Tests kann dieser Test innerhalb eines Taktes große Datenmengen aus einer oder mehreren Test-Datenbanken in die System-Datenbank übertragen.

In einer bevorzugten Variante kann die jeweilige Testsonde mittels des internen Testprogramms von der System-Datenbank auf zumindest eine weitere Test-Datenbank und/oder umgekehrt umschalten und/oder Daten von zumindest einer weiteren Test-Datenbank in die System-Datenbank und/oder Daten von der System-Datenbank in zumindest eine weitere Test-Datenbank übertragen.

Gegebenenfalls können die eingespielten Daten auch dauerhaft in der entsprechenden Datenbank gespeichert werden, in der sie eingespielt wurden. Dies wird in der speziellen Beschreibung beispielhaft mit dem Befehl „save" erreicht.

In einer weiteren Ausgestaltung des erfindungsgemäßen Verfahrens ist an das technische System ferner eine externe Testkomponente mit einem darauf laufenden externen Testprogramm angeschlossen. Der Begriff „extern" ist derart zu verstehen, dass die externe Testkomponente keine Kernfunktionen des technischen Systems außerhalb des Testbetriebs durchführt. Die externe Testkomponente kommuniziert mit zumindest einem Teil der Testsonden und steuert den zumindest einen Teil der Testsonden mittels des externen Testprogramms. Auf diese Weise können verteilte Tests über mehrere Testsonden hinweg realisiert werden. Vorzugsweise kommuniziert die externe Testkomponente mit den entsprechenden Testsonden über eine separate Kommunikationsinfrastruktur, die von der Kommunikationsinfrastruktur des technischen Systems unabhängig ist.

Das erfindungsgemäße Verfahren kann für unterschiedlichste zeitgesteuerte technische Systeme zum Einsatz kommen. Bevorzugt wird das Verfahren eingesetzt in einem System zur Prozessautomatisierung und/oder zur Anlagensteuerung und/oder zur Gebäudesteuerung und/oder in einer Anlage zur Steuerung und Verteilung von Energie und/oder in einem Verkehrsmittel (Kraftfahrzeug, Zug, Flugzeug, Raumfahrzeug) und/oder in einem System zur Verkehrsfluss-Steuerung.

Neben dem oben beschriebenen Verfahren betrifft die Erfindung ferner ein technisches System, in dessen Betrieb basierend auf einem vorgegebenen Takt zyklisch vorbestimmte Zeitschlitze reserviert werden, welche ausschließlich zum Testen des technischen Systems nutzbar sind, und in einem oder mehreren Rechnerknoten des technischen Systems jeweils eine Testsonde integriert ist. Das technische System ist derart ausgestaltet, dass durch eine jeweilige Testsonde beim Testen des technischen Systems ein internes Testprogramm ausgeführt wird, das in der jeweiligen Testsonde hinterlegt ist, wobei die Testsonde mittels des internen Testprogramms auf eine System-Datenbank zugreift, die Daten in der Form von Zustandsdaten des technischen Systems enthält und in dem Rechnerknoten hinterlegt ist, in dem die jeweilige Testsonde integriert ist.

Das erfindungsgemäße technische System ist vorzugsweise derart ausgestaltet, dass eine oder mehrere bevorzugte Varianten des erfindungsgemäßen Verfahrens mit dem technischen System ausgeführt werden können.

Ausführungsbeispiele der Erfindung werden nachfolgend anhand der beigefügten Figuren detailliert beschrieben.

Es zeigen:

Fig. 1 eine schematische Darstellung einer Ausführungsform eines technischen Systems mit darin integrierten Testsonden gemäß einer Ausführungsform der Erfindung; und

Fig. 2 eine Detaildarstellung eines Rechnerknotens des technischen Systems aus Fig. 1 zur Erläuterung der Funktion der darin integrierten Testsonde.

Fig. 1 zeigt eine schematische Darstellung einer Plattform, die in einem technischen System in der Form eines Elektrofahrzeugs integriert ist und welche die Ausführung einer Va-

riante des erfindungsgemäßen Verfahrens ermöglicht. Die Plattform umfasst einen Zentralrechner R, über den verschiedene Funktionen des Elektrofahrzeugs elektrisch bzw. elektronisch gesteuert werden, wie z.B. solche Funktionen, welche herkömmlich über mechanische Kopplung realisiert sind, wie z.B. eine Lenkfunktion in dem Elektrofahrzeug.

In Fig. 1 ist der Zentralrechner R durch ein gestricheltes Rechteck angedeutet. Der Zentralrechner enthält redundant ausgelegte Rechner R1 und R2. Ferner ist eine Vielzahl von Sensoren und Aktoren vorgesehen, wobei im Folgenden ohne Beschränkung der Allgemeinheit nur auf die gezeigten Sensor- und Aktoreinheiten SA1, SA2, SA3 und SA4 Bezug genommen wird, welche jeweiligen Rädern W1 bis W4 des Fahrzeugs zugeordnet sind. Je nach Ausgestaltung können diese Einheiten unterschiedliche Funktionen am Rad durchführen. Zum Beispiel können sie die Radgeschwindigkeiten messen und über eine entsprechende Aktorik Bremsvorgänge am Rad auslösen. Die Rechner R1 und R2 sowie die Sensor- und Aktoreinheiten SA1 bis SA4 stellen Ausführungsformen von Rechnerknoten im Sinne der Patentansprüche dar. Die Rechnerknoten umfassen zur Steuerung des technischen Systems Software und Hardware und können untereinander kommunizieren, wie über die durchgezogenen Linien in Fig. 1 angedeutet ist. Die Kommunikation zwischen den Rechnerknoten kann z.B. basierend auf Ethernet ablaufen. Die Rechnerknoten umfassen jeweils zumindest eine Testsonde T. Dabei ist für jede der Sensor- und Aktoreinheiten SA1 bis SA4 eine einzelne Testsonde T vorgesehen. Demgegenüber sind in den einzelnen Rechnern R1 und R2 jeweils zwei Testsonden T integriert. Die einzelnen Rechner umfassen dabei jeweils zwei Kanäle C1 und C2, die sich gegenseitig überwachen. Für jeden der Kanäle existiert eine Testsonde T.

Die in Fig. 1 gezeigte Plattform ist zeitgesteuert, was bedeutet, dass zyklisch vorbestimmte Zeitschlitze vorgesehen sind, in denen die Plattform jeweils bestimmte Funktionen in einzelnen Rechnerknoten durchführen kann und damit auch auf vorbestimmte Ereignisse reagieren kann. Dabei sind in einem

Systemtakt eine oder mehrere vorbestimmte Zeitschlitze ausschließlich zur Durchführung von Tests mittels der dargestellten Testsonden T reserviert. Die restlichen Zeitschlitze eines Systemtakts werden zur Durchführung anderer Funktionen über die Plattform genutzt. Durch die speziell für Tests vorgesehenen Zeitschlitze und durch die Integration der Testsonden in die Plattform sind die durchgeführten Tests nichtintrusiv.

Das erfindungsgemäße Verfahren zeichnet sich durch eine lokale Steuerung der einzelnen Testsonden T in den Rechnerknoten aus. Dies wird anhand von Fig. 2 verdeutlicht. Diese Figur zeigt im Detail beispielhaft den Kanal C1 des Rechners R1. Der Rechner R1 stellt dabei einen Master-Rechner dar, der im Normalbetrieb entsprechende Funktionen des Elektrofahrzeugs durchführt. Parallel hierzu läuft der sog. Slave-Rechner R2, der bei Ausfall des Rechners R1 dessen Funktionen übernimmt. Die Testsonde T, die in der Form von Software und Hardware realisiert ist, wird gemäß Fig. 2 über ein internes, in der Testsonde T hinterlegtes Programm ITP gesteuert. Es sind dabei mehrere interne Testprogramme in der Testsonde T installiert, welche jedoch nicht gleichzeitig ausgeführt werden. Mit anderen Worten steuert immer nur ein internes Testprogramm die Testsonde eines Rechnerknotens. Hierzu wird das interne Testprogramm in den dargestellten Programmspeicher PS geladen.

Im Rahmen der Ausführung des Programms ITP wird die Testsonde T dazu veranlasst, Daten mit einer System-Datenbank S-DB auszutauschen, wie durch die Pfeile P angedeutet ist. Die System-Datenbank S-DB enthält Zustandsdaten über das technische System, und zwar nicht nur über den Rechnerknoten R1 selbst, sondern auch über die anderen Rechnerknoten, die mit dem Rechnerknoten R1 kommunizieren können. In der System-Datenbank S-DB ist somit der Zustand des technischen Systems, gesehen von dem Rechnerknoten R1, abgebildet. Die Zustandsdaten in der System-Datenbank S-DB können verschieden ausgestaltet sein und betreffen insbesondere Informationen im Hinblick da-

rauf, ob bzw. welche anderen Rechnerknoten des technischen Systems im Betrieb sind bzw. defekt oder ausgefallen sind. Dabei ist zu beachten, dass im Rahmen des Tests die Einträge der System-Datenbank manipuliert werden können und hierdurch reale, insbesondere seltene bzw. kritische Szenarien und Fehlerfälle simuliert werden können. Mit anderen Worten können Daten in der System-Datenbank S-DB einem Testziel entsprechend von den tatsächlichen Zuständen und von empfangen und gesendeten Signalen abweichen.

In der Ausführungsform der Fig. 2 sind ferner mehrere der oben erläuterten Test-Datenbaken, welche zur Vorbereitung von Tests eingesetzt werden, in dem Rechnerknoten R1 hinterlegt. Die Test-Datenbanken sind mit dem Bezugszeichen T-DB bezeichnet. Ferner ist die Wechselwirkung der Test-Datenbanken T-DB mit der Testsonde T durch die Pfeile P' angedeutet. Darüber hinaus umfasst die Testsonde T ein Befehlsspeicher BR, welcher für Teststeuerbefehle genutzt wird und zumindest zwei Befehlsregister umfasst, welche die Befehle enthalten, die die Testsonde im aktuellen Test ausführen soll, wie weiter unten näher erläutert wird.

Wie sich aus den obigen Ausführungen ergibt, werden zum Test des technischen Systems lokale Testsonden T in den einzelnen Rechnerknoten des Systems verwendet. Diese Testsonden werden eigenständig über interne Testprogramme gesteuert, welche auf lokale Datenbanken zur Abbildung des Zustands des technischen Systems zugreifen. Auf diese Weise können Tests taktgenau durchgeführt werden, da interne Testprogramme die Testsonde im Takt des Systems steuern und daher Daten nicht über lange Strecken von bzw. zu einem externen Testsystem übermittelt werden müssen. Nichtsdestotrotz kann zusätzlich auch eine externe Steuerung der Testsonden unter Verwendung eines externen Testsystems durchgeführt werden, wie weiter unten noch näher beschrieben wird.

Im Folgenden werden im Detail weitere Aspekte und bevorzugte Varianten der Erfindung erläutert. Die Erfindung bewahrt die

Eigenschaften und Vorteile von an sich bekannten, in technischen Systemen integrierten Messsonden. Dabei werden die Messsonden jedoch substantiell um neuartige Fähigkeiten erweitert und demzufolge als Testsonden bezeichnet. Ein besonders bevorzugter Anwendungsfall der Erfindung sind verteilte Software-intensive Echtzeitsysteme. Die Plattform der Fig. 1 stellt ein solches System dar. Die Systeme führen Funktionen zeitgesteuert durch und verhalten sich somit inhärent deterministisch. Darüber hinaus sind die Systeme vorzugsweise redundant ausgelegt, d.h. sie umfassen nicht nur einen Rechnerknoten, sondern mehrere Rechnerknoten, so dass funktionstüchtige Rechnerknoten funktionsuntüchtige Rechnerknoten im Produktivbetrieb ersetzen können.

Im erfindungsgemäßen Verfahren interagiert eine jeweilige Testsonde T mit einer System-Datenbank S-DB. Diese Datenbank entkoppelt die Rechnerknoten des getesteten technischen Systems. Die Rechnerknoten im technischen System tauschen dabei ausschließlich über die System-Datenbank Daten aus. Die System-Datenbank hält die Daten für mindestens einen Systemtakt. Die Daten in der System-Datenbank beschreiben den Datenfluss zwischen verschiedenen Rechnerknoten und innerhalb eines Rechnerknotens.

Jeder Rechnerknoten im getesteten System enthält zumindest eine Testsonde T. Aus Sicht des getesteten Systems verhält sich die Testsonde T wie jede andere Komponente im technischen System. Insbesondere führt das getestete System Funktionen der Testsonde zeitgesteuert aus, ebenso wie sie die Funktionen anderer Komponenten zeitgesteuert ausführt. Die zeitgesteuerte Ausführung der Funktionen wird dabei durch die Zuweisung entsprechender Zeitschlitze erreicht, wie weiter oben beschrieben wurde.

Die Testsonde führt mittels des internen Testprogramms Teststeuerbefehle aus. In der hier beschriebenen Ausführungsform kann eine Testsonde die Einträge in der System-Datenbank zu allen Rechnerknoten lesen, diese Einträge überschreiben sowie

prüfen. Im Folgenden wird der Lesebefehl als „monitor", der Schreibfehl als „manipulate" und der Prüfbefehl als „assert" bezeichnet. Der Prüfbefehl überprüft eine Test-Aussage in Bezug auf Zustandsdaten in der System-Datenbank (Wert "true" bei Erfüllung der Test-Aussage und Wert "false" bei Nichterfüllung der Test-Aussage). Im Rahmen des Tests kann durch den Befehl „assert" z.B. erreicht werden, dass hierüber das Fehlschlagen eines Tests festgestellt wird, wenn die entsprechende Aussage erfüllt ist. Die Testsonde kann auch ihre eigenen Daten in der System-Datenbank lesen, schreiben und prüfen.

Die Teststeuerbefehle werden in dem Befehlsspeicher BR (Fig. 2) der Testsonde gespeichert. Der Befehlsspeicher besteht aus mindestens einem Befehlsregister für jede Befehlsart, d.h. aus einem Register für den Befehl „monitor", für den Befehl „manipulate" und den Befehl „assert". Ggf. kann der Befehlsspeicher auch mehrere gleichartige Befehlsregister zur Spezifikation mehrerer Befehle der gleichen Befehlsart umfassen. Ein Teststeuerbefehl in einem Befehlsregister wird solange durch die Testsonde durchgeführt, bis ein neuer Teststeuerbefehl einen Teststeuerbefehl der gleichen Befehlsart ersetzt oder bis ein Teststeuerbefehl ein Befehlsregister der angegebenen Befehlsart löscht. Dies kann z.B. durch Befehle in der Form „clear monitor", „clear manipulate" und „clear assert" erreicht werden.

In der Ausführungsform der Fig. 2 enthält ein Rechnerknoten neben der System-Datenbank S-DB weitere Test-Datenbanken T-DB. Über die Teststeuerbefehle „load" und „save" können Daten zwischen der Test-Datenbank und der System-Datenbank übertragen werden. Mit dem Teststeuerbefehl „switch" kann zwischen der Test-Datenbank und der System-Datenbank innerhalb genau eines Takts umgeschaltet werden. Die Test-Datenbank enthält die gleiche Art von Daten wie die System-Datenbank. Eine Test-Datenbank kann beispielsweise dazu benutzt werden, dass parallel zur Durchführung eines Tests durch Manipulation von Daten in dieser Test-Datenbank ein bestimmtes Betriebsszenario erzeugt wird, welches dann in die System-Datenbank über-

tragen wird, woraufhin durch den Test das erzeugte Betriebsszenario getestet wird.

Vorzugsweise kann eine Testsonde den zugeordneten Rechnerknoten mit dem Teststeuerbefehl „stop" anhalten. Ebenso kann sie den angehaltenen Rechnerknoten mit dem Teststeuerbefehl „continue" fortsetzen. Darüber hinaus besteht ferner die Möglichkeit, einen angehaltenen oder laufenden Knoten nicht nur temporär anzuhalten, sondern dessen Betrieb zu beenden. Hierfür wird der Teststeuerbefehl „exit" benutzt.

Teststeuerbefehle besitzen einen Mechanismus zum Auslösen, wenn entsprechende Bedingungen erfüllt sind (sog. „guarding condition" oder „condition trigger"). Die Teststeuerbefehle werden taktgenau ausgelöst, wenn Daten in der System-Datenbank diese Bedingungen erfüllen, z.B. wenn Signaldaten bestimmte Grenzen erreichen oder Zustandsvariablen bestimmte Zustände anzeigen.

Je nach Ausgestaltung der Erfindung sind die Bedingungen, die Teststeuerbefehle auslösen, entweder Teil eines Teststeuerbefehls oder sie stehen in Steuerregistern. Dabei kann jedem Befehlsregister der entsprechenden Befehlsart („monitor", „manipulate", „assert") ein Steuerregister zugeordnet sein („control monitor", „control manipulate", „control assert").

Bedingungen, die Teststeuerbefehle auslösen, können sowohl boolesche Ausdrücke (and, or, not) als auch relationale Ausdrücke enthalten. Beispiele von relationalen Ausdrücken sind „gleich" (abgekürzt durch „="), „ungleich" (abgekürzt durch „!="), „kleiner" (abgekürzt durch „<"), „größer" (abgekürzt durch „>"), „größer gleich" (abgekürzt durch „≥") sowie „kleiner gleich" (abgekürzt durch „≤"). Die Operanden in den Bedingungen können somit boolesche und relationale Ausdrücke umfassen. Ferner beinhalten die Bedingungen Werte der System-Datenbank und ggf. Konstanten. Die Zahl der Operanden zur Beschreibung einer Bedingung ist nur beschränkt durch die Länge der Befehlsregister bzw. Steuerregister.

Das getestete technische System verhält sich im Testbetrieb und in dem Produktivbetrieb gleich. Systemressourcen, welche die Testsonden während des Testbetriebs nutzen, werden während des Produktivbetriebs nicht von anderen Aufgaben verwendet. Dies wird durch die oben beschriebene Zuweisung von Zeitschlitzen erreicht. Die Testsonden sind von Beginn an in das getestete System integriert. Sie werden nicht nachträglich zum Testen eingebaut.

Die internen Testprozeduren, welche durch die oben beschriebenen internen Testprogramme durchgeführt werden, steuern die Testsonden. Die internen Testprozeduren sind Folgen der oben beschriebenen Teststeuerbefehle. Wie bereits oben erwähnt, besteht ggf. auch die Möglichkeit, dass eine externe Teststeuerung vorgesehen ist. Diese läuft auf einem Knoten außerhalb des getesteten Systems. Auch die externe Teststeuerung verwendet Testprozeduren, mit denen die Testsonden der einzelnen Rechnerknoten zusätzlich gesteuert werden. Über externe Testprozeduren können verteilte Tests über mehrere Rechnerknoten des getesteten technischen Systems realisiert werden. Die Testsonden kommunizieren mit den externen Testprozeduren vorzugsweise über eine separate Kommunikationsinfrastruktur, die unabhängig von der Kommunikationsinfrastruktur des getesteten technischen Systems ist.

Im Unterschied zu externen Testprozeduren, die mehrere Testsonden in unterschiedlichen Rechnerknoten steuern können, steuern interne Testprozeduren genau eine Testsonde. Tests können über mehrere Zyklen hinweg auf einem Rechnerknoten des getesteten technischen Systems taktgenau durchgeführt werden. Die internen Testprozeduren realisieren in diesem Sinne sog. Built-in-Tests, die auf einem Rechnerknoten des getesteten technischen Systems autonom laufen. Während eines Tests, der mehrere Rechnerknoten des getesteten technischen Systems abdeckt, können interne Testprozeduren eine bestimmte Zeit lang und autonom Testbefehle taktgenau ausführen, und zwar ohne Verzögerungen, die ansonsten durch die Kommunikation mit ei-

ner externen Testprozedur entstehen. Insbesondere können mit internen Testprozeduren innerhalb eines Zeitschlitzes Daten aus der System-Datenbank ausgelesen werden, anschließend ausgewertet werden und basierend darauf Manipulationen von Daten in der System-Datenbank durchgeführt werden.

Interne und externe Testprozeduren arbeiten zeitgesteuert im Takt des getesteten technischen Systems. Diese Testprozeduren senden Teststeuerbefehle an die entsprechenden Testsonden. Eine Testsonde übergibt in einem Systemtakt gelesene Daten und Ergebnisse lokaler Prüfungen an die Testprozedur. Die maximale Größe der von einer Testsonde empfangenen und gesendeten Datenpakete ist limitiert und daher deterministisch, aber vorzugsweise konfigurierbar.

Die Längen von Teststeuerbefehlen („monitor", „manipulate", „assert", „load", „save") und damit auch die Größe von Befehlsregistern sind vorzugsweise konfigurierbar. Befehlsregister sind genauso groß wie die Datenpakete, die eine Testsonde empfängt und versendet.

Basierend auf den im Vorangegangenen beschriebenen Varianten der Erfindung können taktgenaue Tests zeitgesteuerter technischer Systeme durchgeführt werden. Insbesondere eignet sich die Erfindung zum Test von Software-intensiven zeitgesteuerten Systemen, die sicherheitsrelevante Funktionen in Echtzeit ausführen. Diese Systeme können verteilt und redundant ausgelegt sein, jedoch auch monolithisch (d.h. das System enthält nur einen Rechnerknoten mit entsprechender Testsonde). Sollen Tests an mehreren Rechnerknoten eines verteilten technischen Systems gleichzeitig angreifen, dann können die Tests auf Basis der Testsonden Zustände der Rechnerknoten, Testschritte (Simulation, Beobachtung und Prüfung) und Testergebnisse taktgenau abstimmen und korrigieren. Dies funktioniert auch unter Echtzeitbedingungen, für selten auftretende und ansonsten schwer nachzustellende Situationen und Fehler, frei von ungewünschten und unbeherrschbaren Zeiteffekten und zerstö-

rungsfrei, also nicht-intrusiv. Die Tests liefern auch in diesen Situationen eindeutige und zuverlässige Resultate.

In dem erfindungsgemäßen Verfahren können Fehlerhypothesen eines sicherheitskritischen Systems als deterministische Tests formuliert werden. Hierdurch wird eine Zertifizierung von sicherheitskritischen Systemen gegen Anforderungen aus Sicherheitsstandards (z.B. IEC 61508, EN 50128 und ISO 26262) vereinfacht.

Über die Testsonden können seltene Situationen in der System-Datenbank des technischen Systems taktgenau eingestellt werden (Teststeuerbefehl „manipulate") und die tatsächliche Reaktion des getesteten Systems gegen die erwartete Reaktion automatisch ermittelt und geprüft werden (Befehle „monitor", „assert"). Dazu muss das getestete technische System nicht nachträglich geändert werden, was das Zeitverhalten des getesteten technischen Systems unzulässig verändert würde. Im Besonderen sind die Testsonden von Beginn an, d.h. während des Entwicklungs- und Testbetriebs, in das technische System eingebaut, so dass deren Auswirkungen auf das Systemverhalten bei der Entwicklung berücksichtigt werden. Ferner werden die in das getestete System eingebauten Testsonden wie gewöhnliche Komponenten behandelt. Während des Produktivbetriebs werden die Testsonden nicht anderweitig verwendet. Im Falle von externen Tests wird eine von dem getesteten technischen System unabhängige Kommunikationsinfrastruktur verwendet.

Zeitliche Verzögerungen werden dadurch vermieden, dass die Testsonden und damit auch interne und externe Tests in Takt des Systems laufen, wenn notwendig auch autonom und über mehrere Zyklen hinweg. Testsonden vermeiden zeitliche Verzögerungen auch dadurch, dass sie komplexere Situationen in der System-Datenbank selbstständig bewerten können und mit Hilfe des Mechanismus zum Auslösen von Teststeuerbefehlen darauf reagieren können. Mit booleschen und relationalen Ausdrücken können entsprechende Bedingungen zum Auslösen von Teststeuer-

befehlen beschrieben werden. Ein Beispiel einer Bedingung in Prefix-Notation lautet wie folgt:

and == Node.State Degraded not availableSensor

Der gleiche Ausdruck lautet in Infix-Notation mit Klammern wie folgt:

((Node.State == Degraded) and (not availableSensor)))

Diese Bedingung bedeutet, dass bei einem vorbestimmten schlechten Zustand eines Rechnerknotens („Degraded") und bei mangelnder Verfügbarkeit eines Sensors („not availableSensor") die Bedingung erfüllt ist. Mit dieser Bedingung kann z.B. der Befehl „assert" ausgelöst werden. Hierzu kann die Bedingung in dem oben beschriebenen Steuerregister hinterlegt sein. Ebenso kann diese Bedingung eine Aussage des Befehls „assert" darstellen, die durch diesen Befehl auf Gültigkeit überprüft wird. Zum Beispiel kann ein Test derart ausgestaltet sein, dass im Falle, dass die genannte Bedingung in der System-Datenbank erfüllt ist, die Testsonde einen Fehler ausgibt.

Die interne Testprozedur der Testsonden kann in einer Variante ferner Daten aus einer Test-Datenbank in die System-Datenbank übertragen (Befehl „load"). Ferner können Daten aus der System-Datenbank in die Test-Datenbank übertragen werden (Befehl „save"). Ebenso kann ggf. zwischen der System-Datenbank und der Test-Datenbank gewechselt werden (Befehl „switch"). Im Produktivbetrieb des technischen Systems kann ferner an der Testsonde eine Blackbox angeschlossen werden, die bestimmte Daten in einem bestimmten Zeitfenster aufzeichnet. Dies kann über einen Kommunikationsanschluss an der Testsonde realisiert werden.

Im Testbetrieb kann ein Systemingenieur eine oder mehrere Rechnerknoten des getesteten technischen Systems mit Hilfe der Testsonden anhalten, analysieren, ggf. verändern und

fortsetzen. Zum Beispiel kann folgende Sequenz von Teststeuerbefehlen (angegeben in erweiterter Backus-Naur Form EBNF) durchgeführt werden:

…stop {monitor | manipulate | load | save | switch} continue…

Die Steuerbefehle in geschweiften Klammern stellen dabei Alternativen von Teststeuerbefehlen dar, die in den jeweiligen Zyklen des Systemtakts durchgeführt werden. Diese Steuerbefehle werden aufgrund des vorangestellten Befehls „stop" im angehaltenen Zustand eines entsprechenden Knotens durchgeführt. Der Betrieb des Knotens wird anschließend durch den Befehl „continue" wieder fortgesetzt.

Die erfindungsgemäßen Testsonden ermöglichen die Realisierung von effizienten Testsuiten aus mehreren Tests. Im Testbetrieb können Testsonden laufende Rechnerknoten sofort beenden, wenn das Testergebnis feststeht (Befehl „exit"). Mit Hilfe der Testsonden kann das getestete System (alle Rechnerknoten) neu gestartet und der nächste Test ausgeführt werden. Alternativ kann eine Testsonde zwischen zwei aufeinander folgenden Tests einen definierten Systemzustand aus einer Test-Datenbank innerhalb eines Takts in die System-Datenbank übertragen (Befehle „load" oder „switch").

Ein Systemingenieur kann interne Testprozeduren ausführen lassen, wenn diese zum getesteten System gelinkt sind. Tests können Ausgaben an eine externe Teststeuerung zur Darstellung, Auswertung oder Aufzeichnung senden. Interne Testprozeduren können auch innerhalb eines Takts auf Verhaltensänderungen des getesteten Systems reagieren, indem die Tests in einem Takt nach Empfang und Auswertung der Daten aus der System-Datenbank auswertungsspezifische Teststeuerbefehle im gleichen Takt der Testsonde übergeben.

Eine Testsonde kann ggf. in einem Takt von mehreren Befehlen derselben Befehlsart gesteuert werden. In diesem Fall sind mehrere Befehlsregister für die entsprechende Befehlsart in

dem entsprechenden Befehlsspeicher vorgesehen. Zum Beispiel kann eine Testsonde zwei Befehlsregister zum Ändern von Speicherzellen in der System-Datenbank besitzen. Bezeichnet man diese Befehlsregister als „manipulate1" und „manipulate2", so kann die Testprozedur eine Testsonde so steuern, dass sie über „manipulate1" Simulationsdaten einspielt, um eine seltene Situation von Zuständen des technischen Systems herzustellen. Im gleichen Takt injiziert die Testsonde mit „manipulate2" ein Fehler. Damit soll das Verhalten eines Rechnerknotens des getesteten Systems auf einen außergewöhnlichen Fehler in einer seltenen Situation taktgenau und deterministisch getestet werden. Hierzu wird wiederum der Befehl „assert" genutzt.

Zwischen den Testsonden und dem getesteten technischen System gibt es keine unbeabsichtigten Wechselwirkungen. Die Testsonden sind nach Plan in das getestete technische System eingebaut und verwenden für die Kommunikation mit externen Testsystemen eine separate Infrastruktur.

Eine Testsonde kann zusammen mit anderen Bestandteilen des entsprechenden Rechnerknotens den gleichen Prozessor nutzen. Alternativ kann die Testsonde einen separaten Prozessor nutzen. Dieser separate Prozessor umfasst einen Befehlsspeicher für Teststeuerbefehle, Speicherbereiche für eine System-Datenbank und ggf. für eine oder mehrere Test-Datenbanken, Speicherbereiche für die internen Testprozeduren sowie einen I/O-Controller, über den die Testsonde Datenpakete mit einer externen Teststeuerung austauscht.

Eine Testsonde mit separatem Prozessor erlaubt die Parallelisierung von Testprogrammen. Es können somit im Rahmen eines Tests die Daten schneller und ggf. auch mehr Daten verarbeitet werden. Der für einen Test sichtbare Bereich in der System-Datenbank wird erweitert. Der Einfluss der Testsonden wird reduziert auf die Synchronisation, die für die deterministischen Tests notwendig ist, um Daten zwischen den Testsonden und dem getesteten System kontrolliert auszutauschen.

Testsonden, ggf. ein externes Testsystem sowie das getestete technische System sind getrennt und erfüllen damit eine Forderung aus Sicherheitsstandards, nämlich die Segregation von kritischen Komponenten. Die Testsonde ist eine sicherheitskritische Komponente aufgrund ihrer Fähigkeiten und möglichen Auswirkungen auf die funktionale Sicherheit des technischen Systems.

Das erfindungsgemäße Verfahren kann in beliebigen zeitgesteuerten technischen Systemen vorteilhaft eingesetzt werden. Bevorzugte Anwendungsfälle wurden bereits im Vorangegangenen genannt. Speziell kann das Verfahren Verwendung finden in der Industrieautomatisierung, in Zugsteuersystemen, Elektrofahrzeug-Steuerungen sowie Prozesssteuerungen, wie z.B. die Steuerung von Walzstraßen.

Bei der Verwendung in industriellen Automatisierungsanlagen kann das erfindungsgemäße Verfahren die Testbarkeit entsprechender Steuereinheiten verbessern. In Bezug auf Zugsteuersysteme kommt das erfindungsgemäße Verfahren vorzugsweise in solchen Zugsteuerungen zum Einsatz, die redundante Rechnerknoten enthalten, welche im sog. Warm- oder Hot-Stand-by betrieben werden, so dass sie beim Ausfall eines Rechnerknotens schnell zugeschaltet werden können. Dabei kann mittels der Testsonden z.B. überprüft werden, ob das Kommunikationssystem des Zugs zuverlässig nach der Norm EN 50159 arbeitet. Mit Testsonden lassen sich z.B. Mechanismen einfach prüfen, die Kommunikationssysteme zur Sicherung der Datenintegrität implementieren, z.B. Prüfsummen. Dabei werden einkommende Nachrichten, wie erhalten, in der System-Datenbank gespeichert. In einem Test kann die Testsonde Nachrichtenteile, die zu verschiedenen Protokollen einer Protokollhierarchie gehören, gezielt fälschen und den Umgang der Rechnerknoten mit den gefälschten Daten prüfen.

Vorzugsweise kommt das erfindungsgemäße Verfahren auch in verteilten Steuer- und Regelungssystemen zum Einsatz. Gerade

in derartigen Systemen sind punktgenaues (Ort) und taktgenaues (Zeit) Lesen und Schreiben von Daten sowie Testen von Dateneigenschaften notwendig. Testsonden ermöglichen punktgenaue und taktgenaue Tests, die frei sind von unbeabsichtigten Seiteneffekten auf das verteilte Steuer- und Regelungssystem unter Test.

Ein weiterer Anwendungsfall der Erfindung ist die Integration von Testsonden in einem Elektrofahrzeug, wie weiter oben beispielhaft anhand von Fig. 1 erläutert wurde. Der Standard ISO 26262 für sicherheitsrelevante elektrische/elektronische Systeme in Kraftfahrzeugen fordert dabei ausdrücklich Tests mit Fehlerinjektion. Dabei können die Testsonden der Erfindung Fehler injizieren und Reaktionen auf injizierte Fehler prüfen, und zwar ohne Seiteneffekte, zerstörungsfrei und im Takt des Systems.

Für alle oben beschriebenen Anwendungen ermöglichen die erfindungsgemäßen Testsonden nicht-intrusive Test von Fehlerhypothesen, was die Zertifizierung nach Sicherheitsstandards (z.B. nach Standards der IEC 61508 Familie) erleichtert. Gleichzeitig können die mit den Testsonden durchgeführten Tests bereits den Entwicklungsprozess des technischen Systems kontinuierlich begleiten. Das technische System kann somit schneller und mit geringeren Kosten hergestellt werden. Ferner können auch bereits ausgelieferte Systeme mit Hilfe der Testsonden getestet werden. Die Tests verzahnen Systementwicklung, Systemwartung und Sicherheitsnachweis.

Da die Testsonden durch die Verwendung interner Testprogramme programmierbar sind, können sie ggf. auch für andere Zwecke eingesetzt werden, z.B. als sog. Watchdogs. In einem Elektrofahrzeug lassen sich mit programmierbaren Testsonden auf einfache Weise z.B. Fahrtenschreiber, Fahrerinformationssysteme und automatische Notrufsysteme realisieren.

Patentansprüche

1. Verfahren zum rechnergestützten Testen eines technischen Systems, bei dem basierend auf einem vorgegebenen Takt zyklisch vorbestimmte Zeitschlitze reserviert werden, welche ausschließlich zum Testen des technischen Systems nutzbar sind, und in einer oder mehreren Rechnerknoten (R1, R2, …, SA4) des technischen Systems jeweils eine Testsonde (T) integriert ist, wobei durch eine jeweilige Testsonde (T) beim Testen des technischen Systems ein internes Testprogramm (ITP) ausgeführt wird, das in der jeweiligen Testsonde (T) hinterlegt ist, und die jeweilige Testsonde (T) mittels des internen Testprogramms (ITP) auf eine System-Datenbank (S-DB) zugreift, die Daten in der Form von Zustandsdaten des technischen Systems umfasst und in dem Rechnerknoten (R1, R2, …, SA4) enthalten ist, in dem die jeweilige Testsonde (T) integriert ist.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass ein technisches System aus mehreren Rechnerknoten (R1, R2, …, SA4) mit darin integrierten Testsonden (T) getestet wird, wobei die mehreren Rechnerknoten (R1, R2, …, SA4) untereinander kommunizieren können und vorzugsweise zumindest zum Teil redundant im technischen System ausgeführt sind.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass die System-Datenbank (S-DB) Zustandsdaten des Rechnerknotens (R1, R2, …, SA4) umfasst, in dem die jeweilige Testsonde (T) integriert ist, und vorzugsweise ferner Zustandsdaten zu weiteren Rechnerknoten (R1, R2, …, SA4) des technischen Systems und/oder zu der jeweiligen Testsonde (T) umfasst.

4. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass eine jeweilige Testsonde (T) zumindest manchmal in einem vorbestimmten Zeitschlitz mittels des internen Testprogramms (ITP) Daten aus der System-Datenbank (S-

DB) liest, die ausgelesenen Daten auswertet und Daten in der System-Datenbank (S-DB) verändert.

5. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der Zugriff einer jeweiligen Testsonde (T) auf die System-Datenbank (S-DB) basierend auf Befehlen der folgenden Befehlstypen erfolgt:

- einen Befehlstyp zum Lesen von Daten aus der System-Datenbank (S-DB);
- einen Befehlstyp zum Ändern von Daten in der System-Datenbank (S-DB).

6. Verfahren nach Anspruch 5, dadurch gekennzeichnet, dass die jeweilige Testsonde (T) mittels des internen Testprogramms (ITP) ferner Befehle von einem Befehlstyp ausführt, der überprüft, ob vorbestimmte Aussagen über in der System-Datenbank (S-DB) hinterlegte Zustände des technischen Systems erfüllt sind.

7. Verfahren nach Anspruch 5 oder 6, dadurch gekennzeichnet, dass eine jeweilige Testsonde (T) mittels des internen Testprogramms (TP) ferner Befehle von Befehlstypen ausführt, mit denen der Betrieb des Rechnerknotens (R1, R2, …, SA4), in dem die jeweilige Testsonde (T) integriert ist, angehalten wird und/oder mit denen der Betrieb des Rechnerknotens (R1, R2, …, SA4), in dem die jeweilige Testsonde (T) integriert ist, fortgesetzt wird.

8. Verfahren nach einem der Ansprüche 5 bis 7, dadurch gekennzeichnet, dass für zumindest einen Teil der Befehle der Befehlstypen vorbestimmte Bedingungen spezifiziert werden, wobei bei Erfüllung der vorbestimmten Bedingungen der entsprechende Befehl ausgelöst wird, wobei die vorbestimmten Bedingungen vorzugsweise den Befehlen zugeordnet sind und/oder in separaten Registern hinterlegt sind.

9. Verfahren nach Anspruch 8, dadurch gekennzeichnet, dass die vorbestimmten Bedingungen über relationale Ausdrücke und

boolesche Ausdrücke spezifizierbar sind, wobei vorzugsweise ferner auch die vorbestimmten Aussagen über relationale Ausdrücke und boolesche Ausdrücke spezifizierbar sind.

10. Verfahren nach einem der Ansprüche 5 bis 9, dadurch gekennzeichnet, dass für jeden Befehlstyp ein oder mehrere Befehlsregister vorgesehen sind, in denen die jeweiligen im aktuellen Zeitschlitz auszuführenden Befehle des entsprechenden Befehlstyps enthalten sind.

11. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass für zumindest einen Teil der Testsonden (T) jeweils eine oder mehrere weitere Datenbanken (T-DB) mit Daten in der Form von Zustandsdaten des technischen Systems vorgesehen ist, wobei die weitere oder weiteren Datenbanken (T-DB) in dem Rechnerknoten (R1, R2, …, SA4) enthalten sind, in dem die jeweilige Testsonde (T) integriert ist, und wobei die jeweilige Testsonde (T) mittels des internen Testprogramms (ITP) auf die weitere oder weiteren Datenbanken (T-DB) zugreift.

12. Verfahren nach Anspruch 11, dadurch gekennzeichnet, dass die jeweilige Testsonde (T) mittels des internen Testprogramms (ITP) den Zugriff von der System-Datenbank (S-DB) auf zumindest eine weitere Datenbank (T-DB) und/oder umgekehrt umschalten kann und/oder Daten von zumindest einer weiteren Datenbank (T-DB) in die System-Datenbank (S-DB) und/oder Daten von der System-Datenbank (S-DB) in zumindest eine weitere Datenbank übertragen kann.

13. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass an das technische System ferner eine externe Testkomponente mit einem darauf laufenden externen Testprogramm angeschlossen ist, wobei die externe Testkomponente mit zumindest einem Teil der Testsonden (T) kommuniziert und dabei den zumindest einen Teil der Testsonden (T) mittels des externen Testprogramms steuert.

14. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass ein technisches System in der Form eines Systems zur Prozessautomatisierung und/oder Anlagensteuerung und/oder Gebäudesteuerung und/oder einer Anlage zur Steuerung und Verteilung von Energie und/oder eines Verkehrsmittels, insbesondere eines Kraftfahrzeugs oder Zugs oder Flugzeugs oder Raumfahrzeugs, und/oder eines Systems zur Verkehrsfluss-Steuerung getestet wird.

15. Technisches System, in dessen Betrieb basierend auf einem vorgegebenen Takt zyklisch vorbestimmte Zeitschlitze reserviert werden, welche ausschließlich zum Testen des technischen Systems nutzbar sind, und in einem oder mehreren Rechnerknoten (R1, R2, …, SA4) des technischen Systems jeweils eine Testsonde (T) integriert ist, wobei das technische System derart ausgestaltet ist, dass durch eine jeweilige Testsonde (T) beim Testen des technischen Systems ein internes Testprogramm (ITP) ausgeführt wird, das in der jeweiligen Testsonde hinterlegt ist, und die jeweilige Testsonde (T) mittels des internen Testprogramms (ITP) auf eine System-Datenbank (S-DB) zugreift, die Daten in der Form von Zustandsdaten des technischen Systems enthält und in dem Rechnerknoten (R1, R2, …, SA4) hinterlegt ist, in dem die jeweilige Testsonde (T) integriert ist.

16. Technisches System nach Anspruch 15, dadurch gekennzeichnet, dass das technische System zur Durchführung eines Verfahrens nach einem der Ansprüche 2 bis 14 eingerichtet ist.

FIG 1

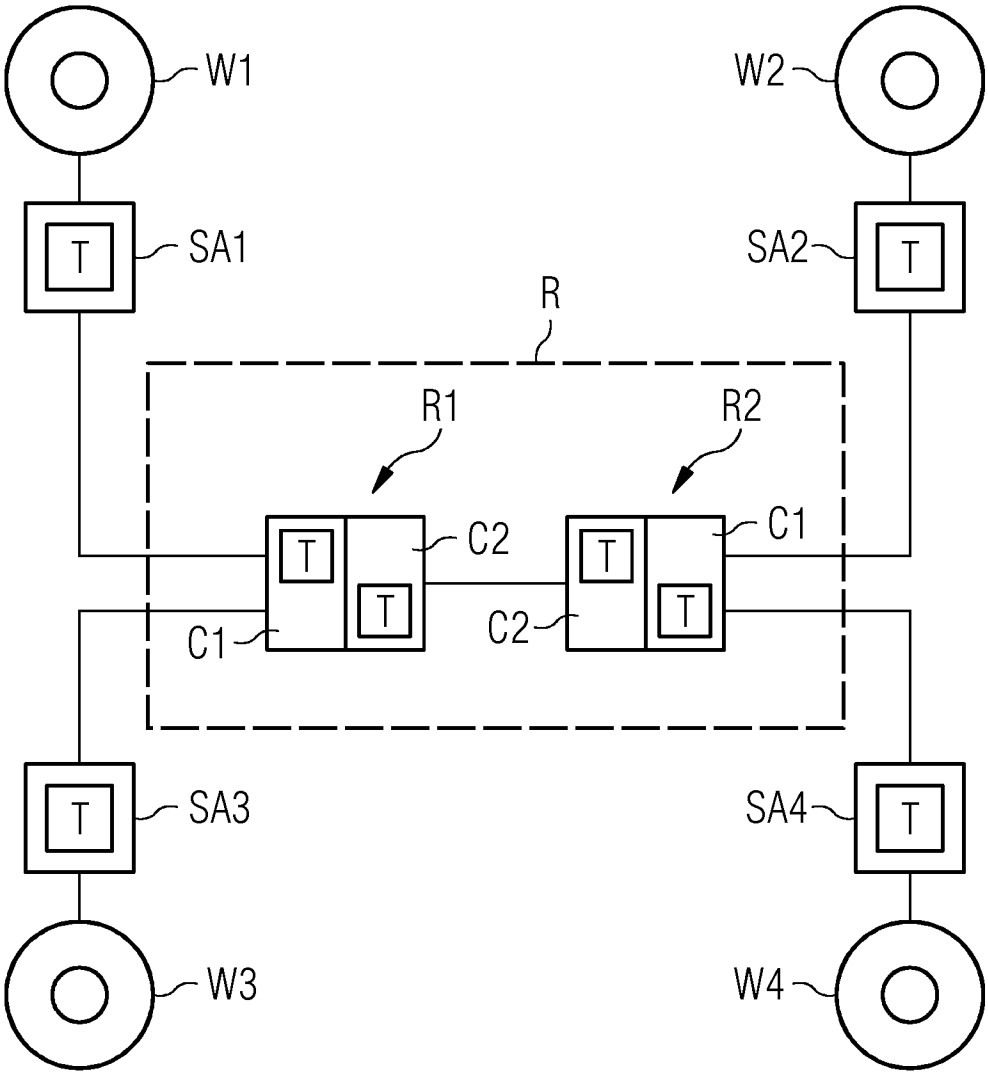
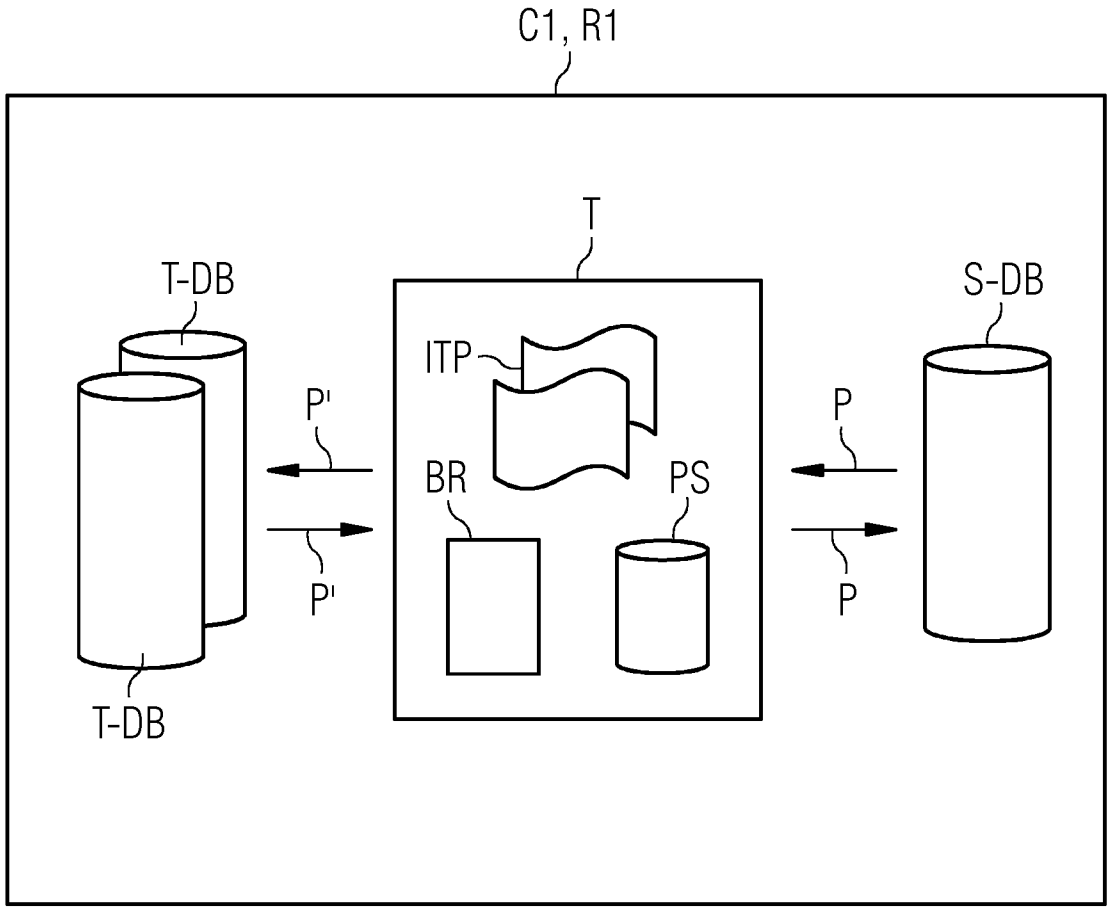


FIG 2



INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2015/059816

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F11/27
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 1 178 321 A2 (SIEMENS AG [DE]) 6 February 2002 (2002-02-06) paragraph [0009] - paragraph [0013] paragraph [0017] paragraph [0026] - paragraph [0027] paragraph [0034] - paragraph [0036] paragraph [0050] - paragraph [0053]; figure 1 -----	1-16
Y	US 5 638 383 A (WOTZAK WILLIAM J [US] ET AL) 10 June 1997 (1997-06-10) column 3, line 14 - column 4, line 27 column 4, line 61 - column 5, line 4 column 6, line 5 - line 27 column 7, line 17 - line 26; figures 1,4 -----	1-16

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 July 2015	03/08/2015

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Gorzewski, Michael

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2015/059816

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1178321 A2	06-02-2002	AT 284038 T	15-12-2004
		DE 10037992 A1	21-02-2002
		EP 1178321 A2	06-02-2002
		ES 2231354 T3	16-05-2005
US 5638383 A	10-06-1997	NONE	

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2015/059816

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. G06F11/27
ADD.

Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
G06F

Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	EP 1 178 321 A2 (SIEMENS AG [DE]) 6. Februar 2002 (2002-02-06) Absatz [0009] - Absatz [0013] Absatz [0017] Absatz [0026] - Absatz [0027] Absatz [0034] - Absatz [0036] Absatz [0050] - Absatz [0053]; Abbildung 1 -----	1-16
Y	US 5 638 383 A (WOTZAK WILLIAM J [US] ET AL) 10. Juni 1997 (1997-06-10) Spalte 3, Zeile 14 - Spalte 4, Zeile 27 Spalte 4, Zeile 61 - Spalte 5, Zeile 4 Spalte 6, Zeile 5 - Zeile 27 Spalte 7, Zeile 17 - Zeile 26; Abbildungen 1,4 -----	1-16

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen ☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" frühere Anmeldung oder Patent, die bzw. das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
27. Juli 2015	03/08/2015

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Gorzewski, Michael

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2015/059816

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 1178321 A2	06-02-2002	AT 284038 T	15-12-2004
		DE 10037992 A1	21-02-2002
		EP 1178321 A2	06-02-2002
		ES 2231354 T3	16-05-2005
US 5638383 A	10-06-1997	KEINE	