(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
26. September 2013 (26.09.2013)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2013/138833 A1

(51) Internationale Patentklassifikation:
G06F 11/00 (2006.01) *G06F 11/07* (2006.01)

(21) Internationales Aktenzeichen: PCT/AT2013/050068

(22) Internationales Anmeldedatum:
19. März 2013 (19.03.2013)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
A 342/2012 20. März 2012 (20.03.2012) AT

(71) Anmelder: **FTS COMPUTERTECHNIK GMBH** [AT/AT]; Schönbrunner Straße 7, A-1040 Wien (AT).

(72) Erfinder: **POLEDNA, Stefan**; Dr. Techmann-Gasse 29, A-3400 Klosterneuburg (AT).

(74) Anwälte: **MATSCHNIG, F.** et al.; PATENTANWALTSKANZLEI MATSCHNIG & FORSTHUBER OG, 52, Siebensterngasse 54, A-1071 Wien (AT).

(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, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, 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, 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, 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, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

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

(54) **Title**: METHOD AND APPARATUS FOR FORMING SOFTWARE FAULT CONTAINMENT UNITS (SWFCUS) IN A DISTRIBUTED REAL-TIME SYSTEM

(54) **Bezeichnung** : VERFAHREN UND APPARAT ZUR BILDUNG VON SOFTWARE FAULT-CONTAINMENT UNITS (SWFCUS) IN EINEM VERTEILTEN ECHTZEITSYSTEM

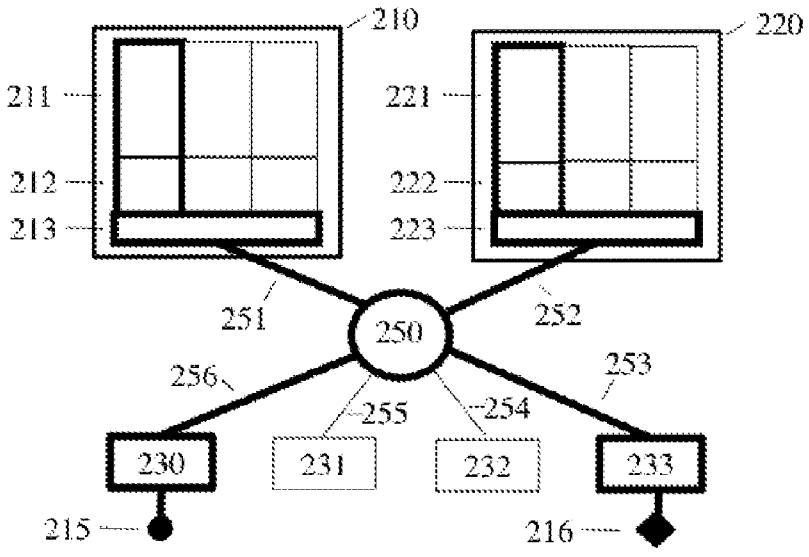

FIG. 2

(57) **Abstract**: The invention relates to a method for limiting the effects of software errors in a distributed real-time system in which a plurality of distributed application systems are executed simultaneously, wherein each application system forms an encapsulated software fault containment unit (SWFCU), wherein an SWFCU comprises the software of a distributed application system, said software being executed on one or more virtual computer nodes and one or more dedicated computer nodes, and exchanging messages via one or more encapsulated virtual communication systems, wherein a communication system consists of communication controllers, switching units and physical connections, and wherein the direct effects of a software error of an SWFCU remain limited to the SWFCU.

(57) **Zusammenfassung**:
[Fortsetzung auf der nächsten Seite]

WO 2013/138833 A1

Die Erfindung betrifft ein Verfahren zur Eingrenzung der Auswirkungen von Softwarefehlern in einem verteilten Echtzeitsystem, in dem mehrere verteilte Anwendungssysteme gleichzeitig exekutiert werden, wobei jedes Anwendungssystem eine abgekapselte Software-Fault-Containment-Unit (SWFCU) bildet, wobei eine SWFCU die Software eines verteilten Anwendungssystems umfasst, die auf einem oder mehreren virtuellen Rechnerknoten und einem oder mehreren dedizierten Rechnerknoten exekutiert wird, und die über einen oder mehrere abgekapselte virtuelle Kommunikationssysteme, wobei ein Kommunikationssystem aus Kommunikationskontrollern, Vermittlungseinheiten und physikalischen Verbindungen besteht, Nachrichten austauschen, und wobei die unmittelbaren Auswirkungen eines Softwarefehler einer SWFCU auf die SWFCU beschränkt bleiben.

VERFAHREN UND APPARAT ZUR BILDUNG VON SOFTWARE FAULT-CONTAINMENT UNITS (SWFCUS) IN EINEM VERTEILTEN ECHTZEITSYSTEM

Die Erfindung betrifft ein Verfahren zur Eingrenzung der Auswirkungen von Softwarefehlern in einem verteilten Echtzeitsystem, in dem mehrere verteilte Anwendungssysteme gleichzeitig exekutiert werden.

Weiters betrifft die Erfindung einen Kommunikationskontroller für einen physikalischen Rechnerknoten zum Durchführen eines solchen Verfahrens.

Außerdem betrifft die Erfindung einen Kommunikationskontroller für einen Personal Computer zum Durchführen eines solchen Verfahrens.

Die vorliegende Erfindung liegt im Bereich der Computertechnik. Sie beschreibt ein innovatives Verfahren und die unterstützende Hardware, wie in einem verteilten Echtzeitcomputersystem Software Fault Containment Units (SWFCU) gebildet werden können, um die Folgen von auftretenden Softwarefehlern auf klar abgegrenzte Bereiche einzugrenzen.

In vielen Echtzeitanwendungen müssen Aufgaben von unterschiedlicher Kritikalität durchgeführt werden. In einer *federated* Computer Architektur wird jede dieser Aufgaben auf einem verteilten Hardwaresystem mit dedizierten Rechnerknoten und einem eigenen Kommunikationssystemen gelöst, um zu verhindern, dass Fehler von einem System einer unteren Kritikalitätsklasse ein System einer höheren Kritikalitätsklasse beeinflussen können. Dieser Lösungsansatz führt zu einer Vielzahl von Rechnern, einem hohen Verkabelungsaufwand für die Kommunikation und damit zu hohen Kosten.

Die aufgrund der höheren Integrationsdichte zunehmende Leistungssteigerung der Rechnerhardware ermöglicht es – aus der Sicht der Performanz –, viele *Anwendungssysteme* unterschiedlicher Kritikalität auf einem einzigen leistungsfähigen verteilten Computersystem zu integrieren. Dies ist jedoch nur machbar, wenn durch die Systemarchitektur und die *zertifizierte Systemsoftware* die Anwendungssoftware eines verteilten *Anwendungssystems* so abgekapselt werden kann, dass gewährleistet ist, dass ein beliebiger Softwarefehler in einem

Anwendungssystem die Funktionalität eines anderen Anwendungssystems weder im Zeitbereich noch im Wertebereich beeinflussen kann.

Es ist eine Aufgabe der Erfindung, ein neues Verfahren offenzulegen, wie eine räumliche und zeitliche Abkapselung eines verteilten Anwendungssystems innerhalb eines verteilten Computersystems realisiert werden kann, sodass auf einem einzigen verteilten Computersystem mehrere verteilte Anwendungssysteme von unterschiedlicher Kritikalität integriert werden können.

Diese Aufgabe wird mit einem eingangs erwähnten Verfahren dadurch gelöst, dass erfindungsgemäß jedes Anwendungssystem eine abgekapselte Software-Fault-Containment-Unit (SWFCU) bildet, wobei eine SWFCU die Software eines verteilten Anwendungssystems umfasst, die auf einem oder mehreren *virtuellen Rechnerknoten* und einem oder mehreren dedizierten Rechnerknoten exekutiert wird, und die über einen oder mehrere *abgekapselte virtuelle Kommunikationssysteme,* wobei ein Kommunikationssystem aus Kommunikationskontrollern, Vermittlungseinheiten und physikalischen Verbindungen besteht, Nachrichten austauschen, und wobei die unmittelbaren Auswirkungen eines Softwarefehler einer SWFCU auf die SWFCU beschränkt bleiben.

Wenn mehrere Anwendungssysteme auf einer verteilten Computerarchitektur realisiert werden, so ist es zweckmäßig, zwischen folgenden Arten von Rechnerknoten zu unterscheiden: Ein *physikalischer Rechnerknoten* ist ein Computer mit CPU, Speicher und Kommunikationsinterface, z.B. ein Personal Computer. Ein *shared Rechnerknoten* ist ein physikalischer Rechnerknoten, auf dem mehrere Anwendungssysteme realisiert sind, z.B. ein Personal Computer, auf dem mittels eines Hypervisors oder eines entsprechenden partitionierten Betriebssystems, wie z.B. vom ARINC 653 Standard definiert [6], mehrere virtuelle Maschinen installiert sind. Der Hypervisor kapselt die virtuellen Maschinen räumlich und zeitlich voneinander ab. Ein *virtueller Rechnerknoten* ist eine der virtuellen Maschinen eines shared Rechnerknotens einschließlich des dazugehörigen Kommunikationskontrollers, der die Nachrichten der virtuellen Maschinen abkapselt. Ein *dedizierter Rechnerknoten* ist ein physikalischer Rechnerknoten (einschließlich des Kommunikationskontrollers), auf dem nur ein einziges Anwendungssystem realisiert ist.

Ein *physikalisches Kommunikationssystem* ermöglicht den Nachrichtentransport zwischen den Kommunikationskontrollern der physikalischen Rechnerknoten. Ein physikalisches Kommunikationssystem besteht aus den in den Rechnern installierten Kommunikationskontrollern, den physikalischen Leitungen und den Vermittlungseinheiten. Auf einem physikalischen Kommunikationssystem können mittels Zeitsteuerung eine Anzahl von *Partitions*, d.s. *virtuelle Kommunikationssysteme,* eingerichtet werden. Eine Partition ist aktiv, wenn sie Nachrichten versendet. Wenn innerhalb eines gegebenen Zeitintervalls mehrere Partitions aktiv sind, so regelt das physikalische Kommunikationssystem welche Nachrichten welcher Partitions auf den physikalischen Leitungen zu welchen Zeitpunkten versendet werden.

Eine Partition ist *abgekapselt*, wenn die zeitlichen Garantien in Bezug auf das Kommunikationsverhalten einer Partition von dem Verhalten der anderen gleichzeitig aktiven Partitions nicht beeinflusst werden kann. Abgekapselte Partitions sind vorhanden, wenn das physikalisches Kommunikationssystem als zeitgesteuertes Kommunikationssystem realisiert ist. Da in einem zeitgesteuerten Kommunikationssystem die periodischen Zeitschlitze zur Übertragung der Daten und damit die Bandbreiten *a priori* den einzelnen Teilnehmern zugeordnet werden, ist eine wechselseitige zeitliche Beeinflussung der auf einem physikalischen Kommunikationssystem eingerichteten Partitions ausgeschlossen.

Nachrichten werden vordefinierten so genannten *virtual links* zugeordnet, wobei *virtual link* <*identifier*> den Namen des *virtual links* angibt. Virtual links haben genau einen vordefinierten Sender und eine vordefinierte Gruppe an Empfängern. Nachrichten können entweder time-triggered, rate-constrained, oder nach dem best-effort Prinzip übertragen werden. *Time-triggered* bedeutet, dass die Nachrichten zu vordefinierten Zeitpunkten anhand einer synchronisierten Zeitbasis versendet werden. *Rate-constrained* bedeutet, dass zwischen zwei Nachrichten eines virtual links ein vordefinierter Mindestabstand eingehalten wird. *Best-effort* bedeutet, dass die Übertragung von Nachrichten nicht garantiert wird [4].

In einer Partition können Nachrichten von einem oder mehreren virtual links gesendet werden. Entsprechend der Art der Kommunikation der Nachrichten sprechen wir von *time-triggered Partition*, *rate-constrained Partition*, oder *best-effort Partition*. Außerdem sind Partitions möglich, die Nachrichten nach unterschiedlichen Prinzipien verschicken; solche Partitions werden *mixed Partitions* genannt. Im folgenden wird ein identifizierter Kommunikationskanal im Kommunikationssystem wie folgt benannt: *virtual link* <*identifier*>, wobei

<*identifier*> den Namen des *virtual links* angibt. In einer Partition können mehrere *virtual links* gleichzeitig aktiv sein.

Ein physikalisches Kommunikationssystem, das als zeitgesteuertes Kommunikationssystem realisiert ist und in dem eine oder mehrere rate-constrained Partitions und/oder best-effort Partitions und/oder mixed Partitions aktiv sind, weist nicht jeder einzelnen Nachricht der rate-constrained/best-effort /mixed Partition einen Zeitschlitz zu, sondern nur einen Zeitschlitz für die Summe aller Nachrichten der entsprechenden Partition. Damit wird gewährleistet dass sich Nachrichten unterschiedlicher Partitions zeitlich nicht beeinflussen können.

Im Bereich der Computerzuverlässigkeit hat der Begriff einer *Fault-Containment Unit (FCU)* eine zentrale Bedeutung [4, S. 136]. Unter einer FCU wird eine abgekapselte Gesamtheit von Subsystemen verstanden, wobei die unmittelbaren Auswirkungen einer Fehlerursache in einem Subsystem der Gesamtheit auf die spezifizierte Gesamtheit eingegrenzt sind. Ein Anwendungssystem bildet eine solche Gesamtheit, die aus folgenden Subsystemen bestehen kann: (i) der Software die auf einem oder mehreren virtuelle Rechnerknoten abläuft, (ii) der Software die auf einem oder mehreren dedizierten Rechnerknoten abläuft und (iii) ein oder mehrere abgekapselte virtuelle Kommunikationssysteme, die den Nachrichtentransport zwischen den virtuellen und dedizierten Rechnerknoten des Anwendungssystems vornehmen. Wir bezeichnen eine abgekapselte Gesamtheit der Software eines verteilten Anwendungssystems, die auf einem oder mehreren *virtuellen Rechnerknoten* und einem oder mehreren dedizierten Rechnerknoten exekutiert wird, und wo die unmittelbaren Auswirkungen eines Softwarefehlers dieser Gesamtheit abgekapselt sind eine *Software Fault-Containment Unit (SWFCU)*. Die unmittelbaren Folgen eines Fehler einer SWFCU sind somit auf diese SWFCU eingegrenzt und können eine andere im verteilten Echtzeitsystem realisierte SWFCU weder im Wertebereich noch im Zeitbereich beeinflussen. Wenn in einem integrierten verteilten Echtzeitsystem jedes Anwendungssystem eine eigene verteilte SWFCU bildet, so kann die wechselseitige Beeinflussung der Anwendungssysteme durch Softwarefehler in den Anwendungssystemen ausgeschlossen werden.

Die vorliegende Erfindung legt ein innovatives Verfahren offen, wie in einem verteilten Echtzeitsystem verteilte *Software-Fault-Containment Units* (SWFCUs) gebildet werden können. Es wird vorgeschlagen, dass jedes der auf einem verteilten Echtzeitsystem realisierten Anwendungssysteme eine eigene SWFCU bildet. Somit wird gewährleistet, dass ein Soft-

warefehler in einer SWFCU die richtige Funktion der anderen SWFCUs nicht beeinflussen kann.

Weitere vorteilhafte Ausgestaltungen des erfindungsgemäßen Verfahrens sind in den Unteransprüchen beschrieben. Beispielsweise ist es von Vorteil, wenn ein *virtueller Rechnerknoten* aus einer auf einem Computer durch einen Hypervisor verwalteten *Virtual Machine (VM)* und einer der VM exklusiv zugeordneten abgekapselten Partition eines Kommunikationskontrollers besteht.

Weiters kann es von Vorteil sein, wenn der Kommunikationskontroller die im Speicherbereich räumlich abgekapselten Ausgangsdaten in eine zugeordnete zeitlich abgekapselte Nachricht umsetzt und den Inhalt einer eintreffenden zeitlich abgekapselten Nachricht in einen der Nachricht zugeordneten räumlich abgekapselten Speicherbereich legt.

Außerdem kann vorgesehen sein, dass *virtual link Identifier* genutzt werden, um die Zuordnung zwischen zeitlich abgekapselten Nachrichten und zugeordneten abgekapselten Partitions eines Kommunikationskontrollers herzustellen.

Zweckmäßig ist es, wenn in einem zeitgesteuerten Kommunikationssystem ein Zeitschlitz für die Summe aller Nachrichten (time-triggered, rate constrainted, best effort) einer *mixed Partition* vorgesehen wird.

Weiters ist es vorteilhaft, wenn unterschiedliche SWFCUs ausschließlich über Nachrichten kommunizieren.

Dabei ist es zweckmäßig, wenn die Vermittlungseinheit eine Multicast Kommunikation unterstützt, so dass die Nachrichten, die zwischen den SWFCUs ausgetauscht werden, von einer unabhängigen Monitorkomponente beobachtet werden können.

Die oben erwähnte Aufgabe wird auch mit einem Kommunikationskontroller für einen physikalischen Rechnerknoten zum Durchführen eines oben beschriebenen Verfahrens realisiert, wobei der Kommunikationskontroller die im Speicherbereich einer virtuellen Maschine räumlich abgekapselten Ausgangsdaten in eine zugeordnete zeitlich abgekapselte

Nachricht umsetzt und die in einer zeitgesteuerten Nachricht eintreffenden Daten in einen zugeordneten räumlich abgekapselten Speicherbereich einer virtuellen Maschine ablegt.

Ebenso wird die oben erwähnte Aufgabe mit einem Kommunikationskontroller für einen Personal Computer zum Durchführen eines oben beschriebenen Verfahrens realisiert, wobei der Kommunikationskontroller den PCI Schnittstellenstandard unterstützt und die in einer zeitgesteuerten Nachricht eintreffenden Daten in einem zugeordneten räumlich abgekapselten Speicherbereich einer virtuellen Maschine abgelegt werden.

Die oben erwähnte Aufgabe wird auch mit einem Kommunikationskontroller für einen Personal Computer zum Durchführen eines oben beschriebenen Verfahrens realisiert, wobei alternativ oder als Fortbildung des oben beschriebenen Kommunikationskontrollers der Kommunikationskontroller den TTEthernet Standard unterstützt.

Die vorliegende Erfindung wird an Hand der folgenden Zeichnungen an einem Beispiel erklärt. Dabei zeigt

Fig. 1 einen physikalischen Rechnerknoten auf dem drei virtuelle Rechnerknoten realisiert sind, und

Fig. 2 ein SWFCU bestehend aus zwei virtuellen Rechnerknoten, einem virtuellen Kommunikationssystem und zwei dedizierten Rechnerknoten.

Das folgende konkrete Beispiel behandelt eine der vielen möglichen Realisierungen des erfindungsgemäßen Verfahrens.

In Fig. 1 ist ein physikalischer Rechnerknoten dargestellt, auf dem drei virtuelle Maschinen **101**, **102**, **103** realisiert sind. Ein dedizierter Speicherbereich **111** der virtuellen Maschine **101** kann sowohl von der virtuellen Maschine **101** wie auch von dem Kommunikationskontroller **120** angesprochen werden. Dieser dedizierte Speicherbereich **111** ist der Endpunkt eines virtuellen Kommunikationskanals, der auf dem physikalischen Kommunikationskanal **130** realisiert ist. Auf dem physikalischen Kommunikationskanal **130** können durch Zeitsteuerung mehrere zeitlich abgekapselte virtuelle Kommunikationskanäle eingerichtet werden. Der Kommunikationskontroller **120** bildet die räumlich abgekapselten Daten, die im Speicherbereich **111** liegen in eine zeitlich zugeordnete abgekapselte Nachricht ab (und umge-

kehrt). Der Kommunikationskontroller **120** stellt die drei abgekapselten Partitionen **111**, **112**, **113** zur Verfügung, wobei je eine Partition einer der drei durch einen Hypervisor verwalteten *Virtual Machines (VM)* **101**, **102**, **103** exklusiv zugeordnet ist.

Die Speicherbereiche **111**, **112**, **113**, die den virtuellen Maschinen **101**, **102**, **103** zugeordnet sind, bilden die Endpunkte dieser virtuellen Kommunikationssysteme. Vor Systemstart werden mittels einer zertifizierten Systemsoftware (ZSW) die Parameter der virtuellen Maschinen **101**, **102**, **103** und des physikalischen Kommunikationskontrollers **120** so gesetzt, dass die Software einer virtuellen Maschine keine Zugriffsrechte auf die Speicherbereiche der anderen virtuellen Maschine erhält, und dass zeitgesteuerten Nachrichten, die auf dem physikalischen Kommunikationskanal **130** transportiert werden, den entsprechenden Speicherbereichen **111**, **112**, **113** der virtuellen Maschinen **101**, **102**, **103** zugeordnet werden. Die Methodik des Aufbaus von virtuellen Maschinen durch Hypervisor wurde bereits in [1] offengelegt. In der Zwischenzeit gibt es Methoden die es ermöglichen, die Korrektheit der Software eines Hypervisors formal nachzuweisen [2]. Die Schnittstelle des Kommunikationskontrollers **120** zur CPU und/oder Speichers des physikalischen Rechnerknoten kann entsprechend dem PCI Standard [3] ausgelegt sein. Die Schnittstelle des Kommunikationskontrollers **120** zum zeitgesteuerten Kommunikationssystem **130** kann entsprechend dem TTEthernet Standard [5] ausgelegt sein.

Fig. 2 zeigt ein verteiltes Echtzeitsystem bestehend aus zwei physikalischen Knotenrechnern **210**, **220**, einer Vermittlungseinheit **250** und vier dedizierten Knotenrechner **230**, **231**, **232**, **233**. In diesem Echtzeitsystem gibt es mehrere Software Fault-Containment Units (SWFCUs). Die stark umrandeten Teile von Fig. 1 bilden eine dieser SWFCUs. Diese ausgewählte SWFCU umfasst die virtuelle Maschine **211**, den Kommunikationskontroller **213** und den dazwischen liegenden gemeinsamen Speicher **212**, den Kommunikationskanal **251** zur Vermittlungseinheit **250**, die virtuellen Maschine **221**, den Kommunikationskontroller **223** und den dazwischen liegenden gemeinsamen Speicher **222**, den Kommunikationskanal **252** zur Vermittlungseinheit **250**, sowie den dedizierten Rechnerknoten **230** mit dem Sensor **215** und den dedizierten Rechnerknoten **233** mit dem Aktuator **216** einschließlich die entsprechenden Verbindungen **256** und **253** zur Vermittlungseinheit **250**. Die beiden Hypervisor in den physikalischen Rechnerknoten **210** und **220**, die Kommunikationskontroller **213** und **223** sowie das Kommunikationsprotokoll in der Vermittlungseinheit **250** verhindern, dass ein Softwarefehler außerhalb dieser SWFCU die Funktionsweise dieser SWFCU beeinflussen

kann. In der Vermittlungseinheit **250** kann das TTEthernet Protokoll [5] zur Abkapselung der Kommunikation dieser SWFCU eingesetzt werden. Dieses Protokoll unterstützt eine deterministische zeitgesteuerte Kommunikation, sowie eine *rate-constrained* Kommunikation und eine *best effort* ereignisgesteuerte Kommunikation. Alternativ kann auch ein anderes Protokoll, das die Kommunikationskanäle zeitlich abkapselt, in der Vermittlungseinheit **250** eingesetzt werden.

Die Kommunikation zwischen unterschiedlichen SWFCUs die auf einem verteilten Echtzeitsystem realisiert sind, soll über Nachrichten erfolgen, wobei es von Vorteil ist, wenn diese Nachrichten von einem unabhängigen Monitor beobachtet werden können. Dies lässt sich erreichen, wenn die Vermittlungseinheit **250** eine Multicast Kommunikation unterstützt.

Zitierte Literatur:

[1] US Pat. 4,949,254. Shorter. *Method to manage concurrent execution of a distributed application program by a host computer and a large plurality of intelligent work stations on an SNA network.* Granted August 14, 1990

[2] Klein, G. et al..(2009). *Formal Verification of an OS Kernel.* Proc. Of the ACM SIGOPS 22nd Symposium on Operating System Principles. ACM Press.

[3] *Peripheral Component Interconnect (PCI) Standard,* Wikipedia. Accessed March 3, 2012.

[4] Kopetz, H. Real-Time Systems, *Design Principles for Distributed Embedded Applications.* Springer Verlag. 2011.

[5] SAE Standard von TTEthernet. URL: http://standards.sae.org/as6802

[6] ARINC 653P1-3 Avionics Application Software Standard Interface, Part 1, Required Services: https://www.arinc.com/cf/store/catalog_detail.cfm?item_id=1487, 653P2-1 Avionics Application Software Standard Interface, Part 2 - Extended Services: https://www.arinc.com/cf/store/catalog_detail.cfm?item_id=1072

PATENTANSPRÜCHE

1. Verfahren zur Eingrenzung der Auswirkungen von Softwarefehlern in einem verteilten Echtzeitsystem, in dem mehrere verteilte Anwendungssysteme gleichzeitig exekutiert werden, **dadurch gekennzeichnet, dass** jedes Anwendungssystem eine abgekapselte Software-Fault-Containment-Unit (SWFCU) bildet, wobei eine SWFCU die Software eines verteilten Anwendungssystems umfasst, die auf einem oder mehreren *virtuellen Rechnerknoten* und einem oder mehreren dedizierten Rechnerknoten exekutiert wird, und die über einen oder mehrere *abgekapselte virtuelle Kommunikationssysteme,* wobei ein Kommunikationssystem aus Kommunikationskontrollern, Vermittlungseinheiten und physikalischen Verbindungen besteht, Nachrichten austauschen, und wobei die unmittelbaren Auswirkungen eines Softwarefehler einer SWFCU auf die SWFCU beschränkt bleiben.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** ein *virtueller Rechnerknoten* aus einer auf einem Computer durch einen Hypervisor verwalteten *Virtual Machine (VM)* und einer der VM exklusiv zugeordneten abgekapselten Partition eines Kommunikationskontrollers besteht.

3. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet, dass** der Kommunikationskontroller **(120)** die im Speicherbereich **(111)** räumlich abgekapselten Ausgangsdaten in eine zugeordnete zeitlich abgekapselte Nachricht umsetzt und den Inhalt einer eintreffenden zeitlich abgekapselten Nachricht in einen der Nachricht zugeordneten räumlich abgekapselten Speicherbereich legt.

4. Verfahren nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet, dass** *virtual link Identifier* genutzt werden, um die Zuordnung zwischen zeitlich abgekapselten Nachrichten und zugeordneten abgekapselten Partitions eines Kommunikationskontrollers herzustellen.

5. Verfahren nach einem der Ansprüche 1 bis 4, **dadurch gekennzeichnet, dass** in einem zeitgesteuerten Kommunikationssystem ein Zeitschlitz für die Summe aller Nachrichten (time-triggered, rate constrainted, best effort) einer *mixed Partition* vorgesehen wird.

6. Verfahren nach einem der Ansprüche 1 bis 5, **dadurch gekennzeichnet, dass** unterschiedliche SWFCUs ausschließlich über Nachrichten kommunizieren.

7. Verfahren nach Anspruch 6, **dadurch gekennzeichnet, dass** die Vermittlungseinheit **(250)** eine Multicast Kommunikation unterstützt, so dass die Nachrichten, die zwischen den SWFCUs ausgetauscht werden, von einer unabhängigen Monitorkomponente beobachtet werden können.

8. Kommunikationskontroller für einen physikalischen Rechnerknoten der einen oder mehrere der in den Ansprüchen 1 bis 7 angeführten Verfahrensschritte realisiert, **dadurch gekennzeichnet, dass** der Kommunikationskontroller die im Speicherbereich einer virtuellen Maschine räumlich abgekapselten Ausgangsdaten in eine zugeordnete zeitlich abgekapselte Nachricht umsetzt und die in einer zeitgesteuerten Nachricht eintreffenden Daten in einen zugeordneten räumlich abgekapselten Speicherbereich einer virtuellen Maschine ablegt.

9. Kommunikationskontroller für einen Personal Computer der einen oder mehrere der in den Ansprüchen 1 bis 7 angeführten Verfahrensschritte realisiert, **dadurch gekennzeichnet, dass** der Kommunikationskontroller den PCI Schnittstellenstandard unterstützt und die in einer zeitgesteuerten Nachricht eintreffenden Daten in einem zugeordneten räumlich abgekapselten Speicherbereich einer virtuellen Maschine abgelegt werden.

10. Kommunikationskontroller für einen Personal Computer der einen oder mehrere der in den Ansprüchen 1 bis 7 angeführten Verfahrensschritte realisiert, **dadurch gekennzeichnet, dass** der Kommunikationskontroller den TTEthernet Standard unterstützt.

11. Echtzeitsystem mit einem Kommunikationskontroller nach einem der Ansprüche 8 bis 10.

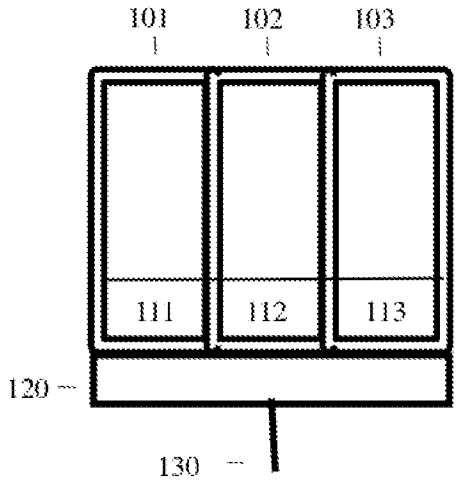
101
102
103
111
112
113
120
130

FIG. 1

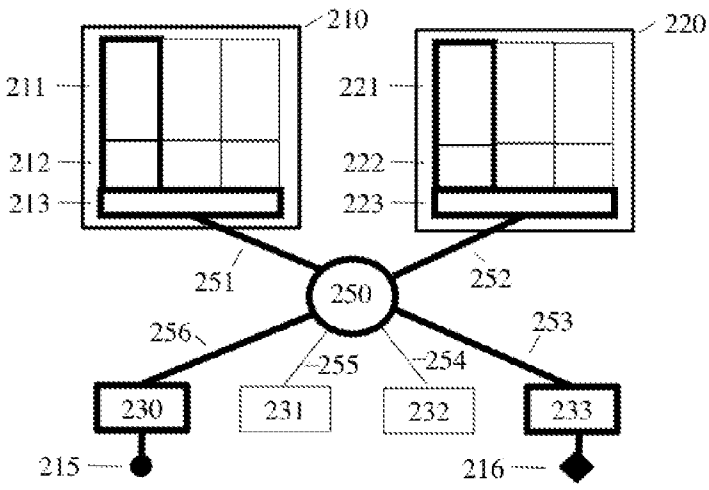
210
220
211
221
212
222
213
223
251
252
250
256
253
255
254
230
231
232
233
215
216

FIG. 2

INTERNATIONAL SEARCH REPORT

International application No
PCT/AT2013/050068

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F11/00 G06F11/07
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, INSPEC, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	L M Pinho: "An architecture for reliable distributed computer-controlled systems", ARCHITECTURE AND DESIGN OF DISTRIBUTED EMBEDDED SYSTEMS. IFIP WG10.3/WG10.4/WG10.5 INTERNATIONAL WORKSHOP ON DISTRIBUTED AND PARALLEL EMBEDDED SYSTEMS (DIPES 2000) KLUWER ACADEMIC PUBLISHERS NORWELL, MA, USA, 1 January 2001 (2001-01-01), pages 43-52, XP055064701, Retrieved from the Internet: URL:http://www.cister.isep.ipp.pt/activities/REFLECT/article1.pdf [retrieved on 2013-05-30] the whole document ----- -/--	1-11

[X] 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
30 May 2013	06/06/2013

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	Kielhöfer, Patrick

INTERNATIONAL SEARCH REPORT

International application No
PCT/AT2013/050068

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	GOVIL K ET AL: "CELLULAR DISCO: RESOURCE MANAGEMENT USING VIRTUAL CLUSTERS ON SHARED-MEMORY MULTIPROCESSORS", OPERATING SYSTEMS REVIEW, ACM, NEW YORK, NY, US, vol. 33, no. 5, 1 December 1999 (1999-12-01), pages 154-169, XP000919655, ISSN: 0163-5980, DOI: 10.1145/319344.319162 Section 2; figure 1	1-11
A	KOPETZ H: "Fault Containment and Error Detection in TTP/C and FlexRay", INTERNET CITATION, 28 August 2002 (2002-08-28), XP002386705, Retrieved from the Internet: URL:http://www.ttech.com/technology/docs/history/HK_2002-08-Fault_Containment/Error_Detection.pdf [retrieved on 2006-06-21] the whole document	1-11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AT2013/050068

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☒ Claims Nos.: **1, 3, 8 (all in part)**
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

see PCT/ISA/210

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

Continuation of Box II.2

Claims 1, 3, 8 (all in part)

It is not clear which technical features are used in the claims 1, 3, and 8 for solving the problems defined there or implementing the functional features (see separate sheet, point VIII for more detailed information).

The applicant is advised that claims relating to inventions in respect of which no international search report has been established cannot normally be the subject of an international preliminary examination (PCT Rule 66.1(e)). In its capacity as International Preliminary Examining Authority the EPO generally will not carry out a preliminary examination for subject matter that has not been searched. This also applies in cases where the claims were amended after receipt of the international search report (PCT Article 19) or where the applicant submits new claims in the course of the procedure under PCT Chapter II. However, after entry into the regional phase before the EPO an additional search may be carried out in the course of the examination (cf. EPO Guidelines, C-VI, 7.2) if the deficiencies that led to the declaration under PCT Article 17(2) have been corrected.

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/AT2013/050068

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. G06F11/00 G06F11/07
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, INSPEC, WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	L M Pinho: "An architecture for reliable distributed computer-controlled systems", ARCHITECTURE AND DESIGN OF DISTRIBUTED EMBEDDED SYSTEMS. IFIP WG10.3/WG10.4/WG10.5 INTERNATIONAL WORKSHOP ON DISTRIBUTED AND PARALLEL EMBEDDED SYSTEMS (DIPES 2000) KLUWER ACADEMIC PUBLISHERS NORWELL, MA, USA, 1. Januar 2001 (2001-01-01), Seiten 43-52, XP055064701, Gefunden im Internet: URL:http://www.cister.isep.ipp.pt/activities/REFLECT/article1.pdf [gefunden am 2013-05-30] das ganze Dokument ----- -/--	1-11

[X] 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
30. Mai 2013	06/06/2013

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	Kielhöfer, Patrick

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/AT2013/050068

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	GOVIL K ET AL: "CELLULAR DISCO: RESOURCE MANAGEMENT USING VIRTUAL CLUSTERS ON SHARED-MEMORY MULTIPROCESSORS", OPERATING SYSTEMS REVIEW, ACM, NEW YORK, NY, US, Bd. 33, Nr. 5, 1. Dezember 1999 (1999-12-01), Seiten 154-169, XP000919655, ISSN: 0163-5980, DOI: 10.1145/319344.319162 Section 2; Abbildung 1 -----	1-11
A	KOPETZ H: "Fault Containment and Error Detection in TTP/C and FlexRay", INTERNET CITATION, 28. August 2002 (2002-08-28), XP002386705, Gefunden im Internet: URL:http://www.ttech.com/technology/docs/history/HK_2002-08-Fault_Containment/Error_Detection.pdf [gefunden am 2006-06-21] das ganze Dokument -----	1-11

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/AT2013/050068

Feld Nr. II Bemerkungen zu den Ansprüchen, die sich als nicht recherchierbar erwiesen haben (Fortsetzung von Punkt 2 auf Blatt 1)

Gemäß Artikel 17(2)a) wurde aus folgenden Gründen für bestimmte Ansprüche kein internationaler Recherchenbericht erstellt:

1. ☐ Ansprüche Nr.
weil sie sich auf Gegenstände beziehen, zu deren Recherche diese Behörde nicht verpflichtet ist, nämlich

2. ☒ Ansprüche Nr. 1, 3, 8(alle teilweise)
weil sie sich auf Teile der internationalen Anmeldung beziehen, die den vorgeschriebenen Anforderungen so wenig entsprechen, dass eine sinnvolle internationale Recherche nicht durchgeführt werden kann, nämlich

siehe BEIBLATT PCT/ISA/210

3. ☐ Ansprüche Nr.
weil es sich dabei um abhängige Ansprüche handelt, die nicht entsprechend Satz 2 und 3 der Regel 6.4 a) abgefasst sind.

Feld Nr. III Bemerkungen bei mangelnder Einheitlichkeit der Erfindung (Fortsetzung von Punkt 3 auf Blatt 1)

Diese Internationale Recherchenbehörde hat festgestellt, dass diese internationale Anmeldung mehrere Erfindungen enthält:

1. ☐ Da der Anmelder alle erforderlichen zusätzlichen Recherchengebühren rechtzeitig entrichtet hat, erstreckt sich dieser internationale Recherchenbericht auf alle recherchierbaren Ansprüche.

2. ☐ Da für alle recherchierbaren Ansprüche die Recherche ohne einen Arbeitsaufwand durchgeführt werden konnte, der zusätzliche Recherchengebühr gerechtfertigt hätte, hat die Behörde nicht zur Zahlung solcher Gebühren aufgefordert.

3. ☐ Da der Anmelder nur einige der erforderlichen zusätzlichen Recherchengebühren rechtzeitig entrichtet hat, erstreckt sich dieser internationale Recherchenbericht nur auf die Ansprüche, für die Gebühren entrichtet worden sind, nämlich auf die Ansprüche Nr.

4. ☐ Der Anmelder hat die erforderlichen zusätzlichen Recherchengebühren nicht rechtzeitig entrichtet. Dieser internationale Recherchenbericht beschränkt sich daher auf die in den Ansprüchen zuerst erwähnte Erfindung; diese ist in folgenden Ansprüchen erfasst:

Bemerkungen hinsichtlich eines Widerspruchs

☐ Der Anmelder hat die zusätzlichen Recherchengebühren unter Widerspruch entrichtet und die gegebenenfalls erforderliche Widerspruchsgebühr gezahlt.

☐ Die zusätzlichen Recherchengebühren wurden vom Anmelder unter Widerspruch gezahlt, jedoch wurde die entsprechende Widerspruchsgebühr nicht innerhalb der in der Aufforderung angegebenen Frist entrichtet.

☐ Die Zahlung der zusätzlichen Recherchengebühren erfolgte ohne Widerspruch.

WEITERE ANGABEN **PCT/ISA/** 210

Fortsetzung von Feld II.2

Ansprüche Nr.: 1, 3, 8(alle teilweise)

Es ist nicht klar, welche technischen Merkmale in den Ansprüchen 1, 3 und 8 verwendet werden, um die dort definierten Aufgaben zu lösen, bzw. die funktionalen Merkmale zu realisieren. Siehe Separates Blatt Punkt VIII für eine genauere Ausführung.

Der Anmelder wird darauf hingewiesen, dass Patentansprüche auf Erfindungen, für die kein internationaler Recherchenbericht erstellt wurde, normalerweise nicht Gegenstand einer internationalen vorläufigen Prüfung sein können (Regel 66.1(e) PCT).In seiner Eigenschaft als mit der internationalen vorläufigen Prüfung beauftragte Behörde wird das EPA also in der Regel keine vorläufige Prüfung für Gegenstände durchführen, zu denen keine Recherche vorliegt.Dies gilt auch für den Fall, dass die Patentansprüche nach Erhalt des internationalen Recherchenberichtes geändert wurden (Art. 19 PCT), oder für den Fall, dass der Anmelder im Zuge des Verfahrens gemäss Kapitel II PCT neue Patentansprüche vorlegt.Nach Eintritt in die regionale Phase vor dem EPA kann jedoch im Zuge der Prüfung eine weitere Recherche durchgeführt werden (Vgl. EPA-Richtlinien C-IV, 7.2), sollten die Mängel behoben sein, die zu der Erklärung gemäss Art. 17 (2) PCT geführt haben.