(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
5. Juli 2001 (05.07.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/47598 A1

(51) Internationale Patentklassifikation[7]: A61N 1/36, 1/372

(21) Internationales Aktenzeichen: PCT/EP00/06666

(22) Internationales Anmeldedatum: 13. Juli 2000 (13.07.2000)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
199 62 915.3 23. Dezember 1999 (23.12.1999) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **INTELLIGENT IMPLANTS GMBH** [DE/DE]; Niebuhrstrasse 1a, 53113 Bonn (DE).

(72) Erfinder; und

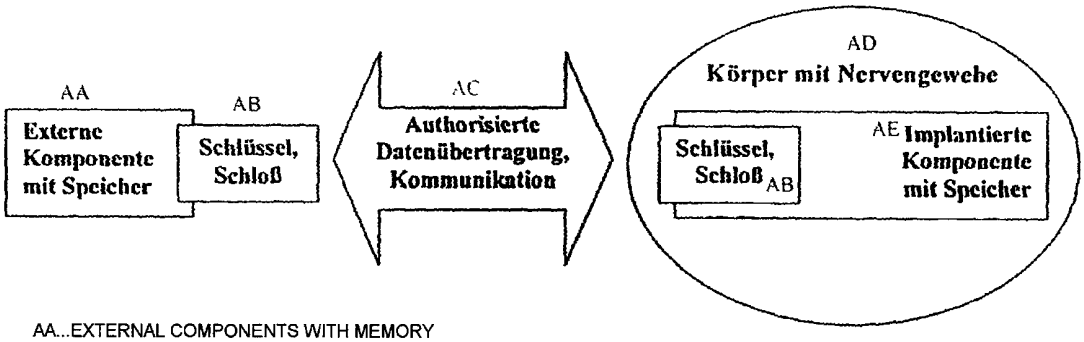
(75) Erfinder/Anmelder *(nur für US)*: **ECKMILLER, Rolf** [DE/DE]; Kaster Strasse 22, D-41460 Neuss (DE). **BECKER, Michael** [DE/DE]; Gregor-Mendel-Strasse 7, D-53115 Bonn (DE). **HÜNERMANN, Ralph** [DE/DE]; Schallstrasse 14, D-50931 Köln (DE). **ORTMANN, Valerij** [DE/DE]; Bahnhofstrasse 45a, D-53757 Sankt Augustin (DE).

(74) Anwalt: **LENZING, Andreas**; Münsterstrasse 248, D-40470 Düsseldorf (DE).

[Fortsetzung auf der nächsten Seite]

(54) Title: DEVICE FOR THE PROTECTED OPERATION OF NEUROPROSTHESES AND CORRESPONDING METHOD

(54) Bezeichnung: VORRICHTUNG FÜR DEN GESCHÜTZTEN BETRIEB VON NEUROPROTHESEN UND VERFAHREN HIERZU



AA...EXTERNAL COMPONENTS WITH MEMORY
AB...KEY, LOCK
AC...AUTHORISED DATA TRANSMISSION, COMMUNICATION
AD...BODY WITH NERVE TISSUE
AE...IMPLANTED COMPONENTS WITH MEMORY

(57) **Abstract:** The invention relates to a system for protecting the operation of neuroprostheses that are designated for treating functional disorders of the nervous system from unauthorised access to functional or operating data. This neuro-implant protection system (NIS) is characterised especially in that at least one neuroprosthesis component is implanted in such a way that it is in contact with a nerve tissue or is associated with a nerve tissue in such a way that they interact, in that the neuroprothesis is only operated during the period of a specific authorisation, or/and in that the system comprises an authorised data transmission between external components and implanted components or/and an authorised communication for monitoring or/and fixing the neuroprosthesis operating status, or/and the communication between the external and implanted components is encoded.

(57) **Zusammenfassung:** Die Erfindung betrifft ein System zum Schutz des Neuroprothesen-Betriebes vor nicht autorisiertem Zugriff auf Funktion bzw. Betriebsdaten, welches Neuroprothesen zur Behandlung von Funktionsstörungen des Nervensystems zugeordnet ist. Dieses Neuroimplantat-Schutzsystem (NIS) ist insbesondere dadurch gekennzeichnet, dass mindestens eine Neuroprothesen-Komponente in Kontakt bzw. Wirkungszusammenhang mit Nervengewebe implantiert ist, der Neuroprothesen-Betrieb nur im Zeitraum einer spezifischen Autorisierung erfolgt, oder/und eine autorisierte Datenübertragung zwischen externer und implantierter Komponente, oder/und eine autorisierte Kommunikation zur Überwachung, oder/und Festlegung des Neuroprothesen-Funktionszustandes umfasst, oder/und die Kommunikation zwischen externer und implantierter Komponente verschlüsselt ist.

WO 01/47598 A1

(81) **Bestimmungsstaaten** *(national)*: AU, BR, CA, CN, IL, JP, KR, MX, NZ, SG, US.

(84) **Bestimmungsstaaten** *(regional)*: europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht:

— *Mit internationalem Recherchenbericht.*

Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Vorrichtung für den geschützten Betrieb von Neuroprothesen und Verfahren hierzu

Die Erfindung betrifft ein Verfahren zum Betrieb einer Neuroprothese mit den Merkmalen des Oberbegriffs des Anspruchs 1 sowie eine Vorrichtung hierzu.

Unter Neuroprothesen sind im Zusammenhang mit der vorliegenden Patentanmeldung Vorrichtungen zum Einsatz in Kontakt oder Wirkungszusammenhang (unidirektionale oder bidirektionale Beeinflussung durch Ausschüttung von Wirkstoffen) mit dem zentralen Nervensystem innerhalb des Schädels, des Rückenmarks oder mit dem Rückenmark verbundener peripherer Nerven, sowie Sehprothesen oder Hörprothesen mit einer implantierten internen Komponente und einer nicht implantierten externen Komponente zu verstehen.

Es sind mehrere Neuroprothesen mit einer implantierten Komponente in Kontakt mit Nervengewebe u.a. zur Behandlung von Funktionsstörungen des Sehsystems, des Hörsystems, des intrakraniellen Nervensystems, des vegetativen Nervensystems, des Rückenmarks, oder des peripheren Nervensystems bekannt, bei denen eine Datenübertragung zwischen einer externen und einer internen, implantierten Komponente zum Zwecke des Betriebes, der Funktionsüberwachung, oder der Funktionsfestlegung vorgesehen ist, z.B. aus den WO 98/36793, WO 98/36795 und US 6,002,966 .

Es sind mehrere Systeme zur geschützten Datenübertragung zwischen voneinander entfernten Komponenten u.a. im Mobilfunk, der Satelliten-Kommunikation, oder bei lokalen Computernetzen oder dem Internet z.B. für Tele-Banking, PKW Diebstahlsicherung oder Tele-Chirurgie bekannt, z.B. aus den Druckschriften DE 2618401, US 5,646,456, US 5,734,330, US 5,940,515, US 5,930,362, US 5,963,621, US 5,940,799, DE 19630920 und EP 0946018

Es sind Implantate ohne Kontakt zu Nervengewebe bekannt, die u.a. zur Personenidentifikation oder zur Standortverfolgung von Tieren in Signal-Verbindung mit einer externen Komponente stehen, z.B. aus US4,399,821, US 4,909,250, US 5,855,609, WO 97/00708, EP 0896 828 A2 und WO 98/29160

Es sind Implantate als Herzschrittmacher bekannt, deren Betriebszustand über eine externe Komponente überprüft oder/und verändert werden kann, z.B. aus US 4,361,153, DE 2944542, US 5,871,451 und US 5,891,178

Es gibt Verschlüsselungs- und Entschlüsselungs-Vorrichtungen und -Verfahren zur Vermeidung des nicht

autorisierten Zugriffs auf digitale oder analoge Datenübertragungen u.a. in technischen oder medizintechnischen Anwendungsgebieten, z.B. aus US 4,766,516, US 5,365,225, US 5,696,825, US 5,987,440 und WO 98/10836

Die gegenwärtig konzipierten bzw. verfügbaren Neuroprothesen oder Neuroimplantate, wie z.B.: Cochlear Implant für Gehörlose, lernfähiges Retina Implant für Blinde mit Netzhautdegeneration haben keine Zugangskontrolle, die den Zugriff auf Daten und Betrieb von einer spezifischen Autorisierung abhängig macht. Deswegen können im Prinzip bei einem gegebenen Implantatträger die für ihn speziell eingestellten externen Komponenten ausgetauscht bzw. verwechselt werden und so zu erheblichen und ggf. schädlichen Funktionsstörungen im technischen oder/und biomedizinischen Bereich führen.

Ferner können schutzbedürftige personenbezogene Daten oder/und implantatbezogene Daten zum Schaden des Implantatträgers oder/und des Implantatherstellers/Betreibers unautorisiert abgerufen oder/und verändert werden.

Stattdessen wird gegenwärtig für den Neuroprothesen-Betrieb typisch eine Kommunikationsverbindung zwischen der fest mit dem Implantatträger verbundenen implantierten Komponente und einer prinzipiell austauschbaren externen Komponente aufgebaut ohne eine hinreichende Vorsorge zum Schutz vor dem unautorisierten Datenzugriff usw. getroffen zu haben. Daher ist das prinzipielle Risiko eines Missbrauchs bzw. eines nicht beabsichtigten Fehlbetriebes nennenswert.

Es ist deshalb die Aufgabe der vorliegenden Erfindung, diese Nachteile zu beseitigen und ein Neuroimplantat-Schutzsystem (NIS) zu offenbaren, dass den unautorisierten Zugriff verhindert.

Weil der Datentransfer bzw. der Betrieb der Neuroprothese nur nach einer Autorisierung mithilfe der implantierten Komponente erfolgen kann, werden diverse Formen eines denkbaren Betriebsmissbrauches verhindert.

Die bevorzugten Ausgestaltungsformen des Autorisierungsvorganges stützen sich auf wesentliche Funktionsmerkmale der implantierten Komponente, die im implantierten Zustand nicht ausgeforscht, kopiert oder simuliert werden können.

Da der Autorisierungsvorgang das Zusammenwirken der implantierten mit der externen Komponente zwingend voraussetzt, können geschützt gespeicherte Daten in der internen, der externen und gegebenenfalls einer weiteren internen Komponente nicht nur Daten für Zwecke der Neuroprothese, sondern auch z.B. wirtschaftlich oder juristisch wichtige personenbezogenen Daten einschließen.

Aufbau und Autorisierungssystem einer so ausgestalteten Neuroprothese verhindern den Nachbau der einzelnen Komponenten.

Das hier offenbarte Neuroimplantat-Schutzsystem (NIS) verschafft den so erweiterten bzw. zusätzlich ausgestatteten Neuroprothesen eine Reihe von wesentlichen Vorteilen gegenüber bisherigen Neuroprothesen ohne NIS. Damit wird die Betriebssicherheit und die Akzeptanz von Neuroprothesen u.a. in Bezug auf Datenschutz und Schutz vor Bedienungsfehlern wesentlich erhöht.

Erstmals wird hier ein System offenbart, dass Betriebsmissbrauch durch Kopplung der implantierten Komponente mit nicht speziell zugeordneten externen Komponenten verhindert. Damit wird erstmals sichergestellt, dass der Implantatträger vor Funktionsschäden aufgrund des falschen Komponenten-Einsatzes geschützt wird.

Durch diese Erfindung wird es für mit NIS ausgestattete Neuroprothesen erstmals möglich, den nicht autorisierten Zugang zu den Daten und Funktionsfestlegungen der implantierten Komponente zu verhindern.

Ferner wird es durch diese Erfindung erstmals möglich, den nicht autorisierten Zugang zur Datenübertragung zwischen externer und implantierter Komponente zu verhindern. Dadurch wird insbesondere der personenbezogene Datenschutz des Implantatträgers, der bei herkömmlichen Heilverfahren u.a. durch die Schweigepflicht des behandelnden Arztes geschützt wird, bezüglich des Neuroprothesen-Betriebes erstmals nachhaltig gesichert.

Zusätzlich kann durch die offenbarte Erfindung der nicht autorisierte Zugang zu wesentlichen Funktionseigenschaften der Neuroprothese verhindert werden. Damit wird der nicht autorisierte Nachbau (Reverse Engineering) von Komponenten der so ausgestatteten Neuroprothesen verhindert, da einerseits wesentliche Funktionseigenschaften für den nicht autorisierten Nachbau fehlen und da andererseits derartige nicht autorisierte Nachbaukomponenten nicht mit den übrigen Komponenten wegen fehlender Kompatibilität

und fehlender Autorisierung der Komponentenkommunikation betrieben werden können.

Im folgenden werden Ausführungsbeispiele von vorteilhaften Ausgestaltungen des Neuroimplantat-Schutzsystems (NIS) und der zugehörigen Verfahren anhand der Zeichnung dargestellt. Es zeigen:

Figur 1: ein Schema des Neuroimplantat-Schutzsystems (NIS) für eine Neuroprothese;

Figur 2: das Schema eines bei der Fertigung zugeordneten Paares von externer (Schlüssel) und interner (Schloss) Komponente

Figur 3: das Schema einer bevorzugten Realisierung der mikroelektronischen Festlegung der Schlüssel / Schlossfunktion in der implantierten internen Komponente bzw. in der externen Komponente

Figur 4: das Schema einer bevorzugten Ausführung eines ‚Dynamischen Labyrinthes' zur Repräsentation des zweiten Autorisierungssignals als Schloss in der internen Komponente; sowie

Figur 5: eine weitere bevorzugte Ausgestaltung für das Schema des Neuroimplantat-Schutzsystems (NIS).

Fig. 1 zeigt ein Schema des Neuroimplantat-Schutzsystems (NIS) für eine Neuroprothese. Sowohl die externe Komponente der Neuroprothese, als auch die implantierte, interne Komponente verfügen über einen Schlüssel oder / und ein Schloss für die Prüfung und Durchführung von autorisierten Datenübertragungen oder / und zu Abfragen oder / und Neufestlegungen des Funktionszustandes der einzelnen Komponenten.

Der Betrieb der Neuroprothese bzw. der autorisierte Zugriff auf intern oder extern gespeicherte Daten ist nur möglich, wenn ein von der externen Komponente bei der internen Komponente eintreffendes Autorisierungssignal nach einem Verfahren legitimiert worden ist, welches allein auf Merkmalen der internen Komponente basiert und nicht von einer externen Komponente aus analysiert, verändert, oder umgangen werden kann.

Fig.2 zeigt das Schema eines bei der Fertigung zugeordneten Paares von externer (Schlüssel) und interner (Schloss) Komponente ohne die Möglichkeit der Entdeckung des Schlüssels oder des Schlosses durch Analyse der externen Komponente. In einer hier skizzierten bevorzugten Ausgestaltung wird angenommen, dass aus einem größeren Frequenzbereich (Schall, elektromagnetische Wellen, Licht, Rauschgenerator, usw.) für das in dem Frequenz-Zeit-Diagramm als einfaches Beispiel skizzierte Autorisierungs-Signal die Frequenzen F1, F2, F3 sowie die Zeitfolge T1, T2, T3, T4 während der Paar-Fertigung ausgewählt wurden. Ferner wurde das skizzierte Frequenz-Zeit-Muster zur Autorisierung bzw. Identifikation für dieses Paar ausgewählt. Die zugehörigen Parameter- und Funktionsfestlegungen in der externen und in der internen Komponente erfolgten während bzw. nach der Fertigung zum Teil durch Festlegungen in der zugehörigen Mikroelektronik bzw. Mikromechanik und zum Teil durch Festlegungen in der Software.

Fig.3 zeigt das Schema einer bevorzugten Realisierung der mikroelektronischen Festlegung der Schlüssel / Schlossfunktion in der implantierten internen Komponente bzw. in der externen Komponente. Das ausgewählte Autorisierungssignal ist z.B. ein Signal-Muster, welches

durch Amplituden-, Frequenz-, Zeit- und Orts-Parameter (im Prinzip z.B. vergleichbar der Vokalisation eines Tieres) festgelegt ist. Zum Zweck der Autorisierung wird in einer bevorzugten Ausführung durch das Zusammenwirken von Speicher, Prozessor und FPGA o.ä. während oder nach der Fertigung eine Art Labyrinth erzeugt, welches das Schloß repräsentiert und welches nur vom einzig richtigen Autorisierungssignal als Schlüssel durchlaufen werden kann. Das richtige Durchlaufen des ‚Labyrinthes' erzeugt seinerseits in einer bevorzugten Ausführung ein zeitliches Signalmuster, welches in einer mikroelektronisch festgelegten Form auf eine logische Gatterstruktur geleitet und als "Ja=Autorisierung kann stattfinden" interpretiert wird. Weder die Struktur und Funktion des Labyrinthes, noch die längs des Labyrinthes angekoppelte Gatterfunktion oder Struktur, die vollständig der implantierten, internen Komponente zugeordnet sind, können durch Einwirkungen seitens der externen Komponente transparent gemacht, kopiert oder simuliert werden.

Fig. 4 zeigt das Schema einer bevorzugten Ausführung eines ‚Dynamischen Labyrinthes' zur Repräsentation des zweiten Autorisierungssignals als Schloss in der internen Komponente. Das ‚Dynamische Labyrinth' (zum kleinen Teil angedeutet unten in Fig. 4 durch eine Sequenz von Instruktionen bzw. digitalen Zuständen, von denen z.B. sechs als Koppelpunkte 1 bis 6 laufend beobachtet werden) kann vorzugsweise durch einen Algorithmus repräsentiert sein, der durch ein festgelegtes Zusammenwirken von programmierbarer Mikroelektronik (z.B. FPGA), Speicher oder/und Prozessor realisiert wird und der die einzelnen Elemente eines eintreffenden Signales jeweils logischen Funktionen und Informationsverarbeitungspfaden zuordnet,

so dass sich das Signal als Funktion der Zeit über dieses Labyrinth verteilt bzw. schrittweise in ihm fortschreitet. In einer bevorzugten Ausgestaltung ist vorgesehen, dass nur, wenn das von der externen Komponente empfangene Signal als Autorisierungssignal und somit als Schlüssel aufgrund der in programmierbare Hardware, Speicher und Prozessor der internen Komponente die Koppelpunkte 1 bis 6 zu den vorgegebenen Zeiten mit dem jeweils für die Autorisierung vereinbarten Wert erreicht und hier z.B. von einem Schaltnetz oder Schaltwerk (Oktagone mit Kreuz und Kreis als angedeutete logische Bausteine einschließlich Zeitverzögerungsglieder mit den angedeuteten Verbindungsleitungen) detektiert wird und die Ausgangssignale des Schaltnetzes wiederum von dem rechts angedeuteten UND-Gatter in einem engen Zeitfenster als logische Eins bewertet werden, die Autorisierung vollzogen wird. Die zugehörigen Zeitfestlegungen und logischen sowie Labyrinth-Festlegungen sind in dieser bevorzugten Ausgestaltung nicht explizit als Algorithmen verfügbar, sondern sind in die interne Komponente eingebettete Festlegungen, die nicht ausgeforscht werden können und wegen der Implantation nicht zugänglich sind. Erst wenn die Autorisierung erfolgt ist, können Neuroprothesen-Betrieb, Datenübertragung oder / und Zugriff auf geschützte Speicherbereiche der einzelnen Komponenten erfolgen. Die Autorisierung kann während des Betriebes erneuert werden, wobei in einer bevorzugten Ausgestaltung nicht das zur primären Autorisierung verwendete Autorisierungssignal wiederholt verwendet wird, sondern hierfür ein neues Signal verwendet wird.

Fig. 5. zeigt eine weitere bevorzugte Ausgestaltung für das Schema des Neuroimplantat-Schutzsystems (NIS). Ein

NIS besteht aus z.B. zwei implantierten Komponenten und geschützten Datenübertragungskanälen, zur Kommunikation zwischen implantierten Komponenten sowie zwischen internen Komponenten und z.B. zwei externen Komponenten und/oder einem PC sowie z.B. zur Übertragung biometrischer Daten vom Implantatträger an eine der externen Komponenten oder/und einen PC. Die Kommunikation findet verschlüsselt statt. Externe und interne Komponente beinhalten dazu notwendige Verschlüsselungshardware und/oder -Software auf der Basis eines Prozessors und/oder programmierbarer Hardware und/oder von Speichern. Der Betrieb erfolgt nur nach einer erfolgreicher Authentifizierung und Autorisierung aller Komponenten.

Eine vorteilhafte Ausgestaltung des Verfahrens zum geschützten Betrieb einer Neuroprothese (s. Fig. 1, Fig.2, Fig. 3, Fig. 4, Fig. 5) besteht darin, dass die externe Komponente ein verschlüsseltes Autorisierungssignal durch ein gängiges elektromagnetisches (z.B. als frequenzmodulierte Pulsgruppe), oder/und optoelektronisches Verfahren (z.B. als amplitudenmodulierte Pulsgruppe von einer Laser-Diode als Sender zu einem Photosensor als direkt unter der Haut oder innerhalb des Auges implantierter Empfänger), oder nach anderen physikalischen oder chemischen Prinzipien wie z.B. die Modulation von Schall einschließlich Körperschall mit technisch bekannten Sendern und Empfängern, oder die spezifische Applikation eines mechanischen Signals (z.B. die Erzeugung von Vibrationsmustern mit einem oder mehreren, örtlich verteilten sehr lokal wirkenden Vibratoren in Kommunikation mit entsprechenden technisch bekannten Vibrationssensoren) mit einer hierfür speziell

ausgestalteten und / oder positionierten Teilstruktur der implantierten, internen Komponente zum Zweck der für den Neuroimplantat-Betrieb oder/und für die Datenübertragung zwischen externer und interner Komponente erforderlichen Autorisierung austauscht.

Eine weitere vorteilhafte Ausgestaltung des Verfahrens zum geschützten Betrieb besteht darin, dass die interne, implantierte Komponente neben einem periodischen über einen nicht-periodischen Zeitgeber verfügt, der die Zeit nach einem festgelegten Code einteilt und zum Zwecke der Autorisierung eine Kopie dieses Zeitcode-Gebers in der externen Komponente benötigt. Zu diesem Zweck wird z.B. während der Fertigung bzw. Justierung eines Paares von externer und implantierter, interner Komponente in beiden Komponenten ein Algorithmus zur Erzeugung von zueinander identischen, nicht-periodischen Zeitreihen festgelegt. Ferner wird in dieser bevorzugten Ausgestaltung z.B. durch vereinbarte Synchronisiersignale der Gleichlauf beider nicht-periodischer Zeitgeber sichergestellt. Damit können u.a. nicht-autorisierte Zugangsversuche zu Daten oder Betrieb der Neuroprothese, die typischerweise auf periodischen Zeitgebern basieren, sehr schnell erkannt und abgewehrt werden.

Eine weitere vorteilhafte Ausgestaltung des Verfahrens zum geschützten Betrieb besteht darin, dass die interne Komponente, je nach Festlegung, im Falle der Ablehnung des Autorisierungsversuches entweder ein Ablehnungssignal geben, oder sich passiv verhalten und so seine Existenz und ggf. genaue Lokalisation geheim halten kann.

Eine weitere vorteilhafte Ausgestaltung des Verfahrens zum geschützten Betrieb besteht darin, dass je nach

Festlegung in der Neuroprothese das Akzeptieren einer Autorisierung sehr unterschiedlich umgesetzt werden kann durch: a) automatischer Betriebs- oder Datenübertragungsbeginn ohne separates Akzeptanz-Signal, b) Erzeugung eines von der internen Komponente gesendeten Signales, welches auch ohne Zugang zum entsprechenden Code von entsprechenden extern positionierten Sensoren detektiert werden kann und c) Verstellung einer passiven Eigenschaft der internen Komponente (z.B. das Einschalten eines internen Energieempfängers, Schwingkreises, oder von Absorptions- oder Reflexionsstrukturen), die zwar von der speziell autorisierten Komponente, die z.B. im autorisierten Code sendet, extern z.B. durch erhöhten Energieabfluss messbar ist, jedoch nicht von fremden externen Detektoren entdeckt werden kann.

Eine weitere vorteilhafte Ausgestaltung des Verfahrens zum geschützten Betrieb besteht darin, dass zur Vermeidung von Betriebsmissbrauch grundsätzlich eine interne Komponente nur genau einer externen Komponente zugeordnet ist und umgekehrt. Diese eindeutige Exklusiv-Zuordnung ist so realisiert, dass sie nicht durch in der Datenverarbeitung gängige Zugangskontrollmechanismen mit "Super user" Rechten z.B. des Implantat-Betreibers oder Herstellers oder durch Kenntnis eines Passwortes außer Kraft gesetzt werden kann, sondern dass z.B. der Austausch einer ursprünglich der internen Komponente zugeordneten speziellen externen Komponente nur durch die ausdrückliche Zustimmung des Implantat-Trägers nach Art der Zustimmung zu einem medizinischen Eingriff erfolgen kann. Zu diesem vorteilhaften Zweck kann ein funktionelles Echtzeit-Modell der speziellen externen Komponente nur während des autorisierten Betriebes hergestellt bzw. während der Paarfertigung oder initialen

Justierung eines Paares aus externer und interner Komponente ein Duplikat der externen Komponente hergestellt werden, das so gesichert verwahrt wird, dass nur der Implantatträger über den Zugang zu dieser "Kopie" als Modell bzw. Duplikat des für die Autorisierung und den Datenaustausch nötigen Moduls der externen Komponente verfügen kann.

Eine weitere vorteilhafte Ausgestaltung des Verfahrens zum geschützten Betrieb besteht darin, dass die Erlangung des autorisierten Zuganges zu Datenübertragung oder/und interner Komponente durch eine Funktionsanalyse der speziellen externen Komponente, oder dem ihr zugeordneten funktionellen Echtzeit-Modell außerhalb des autorisierten Betriebes nicht möglich ist. Diese vorteilhafte Eigenschaft wird u.a. dadurch realisiert, dass die in der externen Komponente während des Analysebetriebes erfassbaren Eigenschaften keinen hinreichenden Aufschluss über die zur erfolgreichen Autorisierung benötigte Codierung bzw. Verschlüsselung und Decodierung bzw. Entschlüsselung des Autorisierungssignals geben. Zu diesem Zweck wird die Autorisierung bevorzugt derart gestaltet, dass ein mehrdimensionales "Template Match", welches z.B. die Dimensionen: Zeit, Amplitude, Frequenz und Ort umfasst, und welches bei der paarweisen Fertigung von je einer internen und der zugehörigen externen Komponente in einem Zufallsprozess, oder mithilfe neuronaler Netze bzw. anderer Lernalgorithmen, oder unter Verwendung von nur dem Implantatträger eigenen Merkmalen wie z.B. : Iris des Auges, Fingerabdruck, Erbmaterial festgelegt wurde, ein unverwechselbares "Schlüssel-Schloss" Paar bildet. Dabei kann bei einer Funktions- und Strukturanalyse der externen Komponente weder der externe "Schlüssel", noch das zugehörige interne "Schloss" mit

vernünftigem Aufwand ermittelt werden. Die bei dem Bemühen um unautorisierten Zugang denkbaren Tests, ob eine gerade gewählte Schlüssel-Kombination vom in der internen Komponente repräsentierten Schloss akzeptiert wird, sind bezüglich der Kombinationsmöglichkeiten derart groß, dass sehr schnell die vorgegebene Zahl vergeblicher Autorisierungsversuche erreicht und so die interne Komponente auf Dauer sperren würde.

Eine weitere vorteilhafte Ausgestaltung des Verfahrens zum geschützten Betrieb besteht darin, dass zur Herstellung bzw. zur initialen Justierung oder Funktionsfestlegung eines eindeutigen Paares von externer und interner Komponente sowie ggf. eines sicher zu verwahrenden Duplikates der externen Komponente bezüglich der Codierungs-Elemente jeweils Paare der zugehörigen Speicher oder/und Prozessor oder/und FPGA Bausteine in ihrer Funktion durch identische Software oder/und Hardware-Festlegungen behandelt werden. Z.B. kann das entsprechende Paar von programmierbaren Mikroelektronik-Bausteinen (z.B. FPGA) unter Berücksichtigung seiner physikalischen und geometrischen Eigenschaften durch einen identischen Prozess programmiert bzw. durch maschinelle Fertigungsschritte hergestellt werden, wodurch z.B. der nicht-periodische Zeitgeber oder die Festlegung der nur für dieses Paar verwendeten Familie von Autorisierungssignalen eindeutig, vertraulich und geschützt, nämlich eingebettet in die Mikroelektronik festgelegt wird. Diese identischen Funktionsfestlegungen bewirken aufgrund der in der externen und der internen Komponente verschieden festgelegten Funktionsabläufe und zusätzlicher Funktionen jedoch nicht identische Gesamtfunktionen, sondern genau eindeutig zu einander passende, komplementäre Funktionen. Dabei kann es sich um

vom Hersteller wiederholbare oder nicht wiederholbare Funktionsfestlegungen handeln. Im Ergebnis entstehen so Paare, die nur miteinander, jedoch nicht mit anderen Komponenten kommunizieren bzw. Signale austauschen können.

Eine weitere vorteilhafte Ausgestaltung des Verfahrens zum geschützten Betrieb besteht darin, dass der Zugriff auf geschützte Daten oder Funktionszuständen sowohl in der internen Komponente, als auch in der externen Komponente von der erfolgreichen Autorisierung abhängig gemacht wird bzw. werden kann. Zu diesem Zweck wird in einer bevorzugten Ausführung ein in der internen Komponente legitimierter Autorisierungsversuch auch in der externen Komponente registriert und dort nicht nur zur Freischaltung der Datenübertragung, sondern auch zur Freischaltung des Zuganges zu in der externen Komponente geschützt verfügbaren Daten oder Funktionszuständen verwendet.

Eine weitere vorteilhafte Ausgestaltung des Verfahrens zum geschützten Betrieb besteht darin, dass das ausgewählte Autorisierungssignal z.B. ein Signal-Muster ist, welches durch Amplituden-, Frequenz-, Zeit- und Orts-Parameter festgelegt ist. Jede externe Komponente hat als Autorisierungssignal seine eindeutige Kennung als Autorisierungs-Schlüssel. Jede interne Komponente hat ihrerseits ein anderes Autorisierungssignal als Autorisierungs-Schloss. Kenntnis des Schlüssels oder des Schlosses allein erlaubt keinen Rückschluss auf das jeweils zur Autorisierung benötigte andere Signal. Nur, wenn in der internen Komponente das einzig richtige Autorisierungssignal als Schlüssel empfangen wird und unter Verwendung eines Speichers, oder/und eines

Prozessors oder/und eines FPGA erfolgreich mit dem dort als Schloss verfügbaren Autorisierungssignal verglichen wird, so dass Schlüssel und Schloss gemeinsam zur Autorisierungsentscheidung führen, können Datenübertragung oder/und Neuroprothesenbetrieb gestartet werden.

Zum obengenannten Zweck wird in einer bevorzugten Ausführung durch das eventuelle Zusammenwirken von Speicher, Prozessor und programmierbare Hardware (s. Fig. 3) während oder nach der Fertigung eine Art ‚Dynamisches Labyrinth' (Fig. 4) erzeugt, welches das Autorisierungssignal der internen Komponente das Schloss repräsentiert und welches nur vom einzig richtigen Autorisierungssignal als Schlüssel durchlaufen werden kann. Das richtige Durchlaufen des ‚Labyrinthes' erzeugt seinerseits in einer bevorzugten Ausführung ein zeitliches Signalmuster, welches in einer mikroelektronisch festgelegten Form auf eine logische Gatterstruktur geleitet und als „Ja = Autorisierung kann stattfinden" interpretiert wird. Weder die Struktur und Funktion des Labyrinthes, noch die längs des Labyrinthes angekoppelte Gatterfunktion oder Struktur, die vollständig der implantierten, internen Komponente zugeordnet sind, können durch Einwirkungen seitens der externen Komponente transparent gemacht, kopiert oder simuliert werden.

Eine weitere vorteilhafte Ausgestaltung des Verfahrens zum geschützten Betrieb besteht darin, dass das ‚Dynamische Labyrinth', vorzugsweise durch eine Sequenz von Instruktionen bzw. digitalen Zuständen, von denen einige als Koppelpunkte laufend beobachtet werden(s. Fig. 4) vorzugsweise durch einen Algorithmus repräsentiert

ist, der durch ein festgelegtes Zusammenwirken von programmierbarer Hardware, Speicher oder/und Prozessor realisiert wird. Dieser bevorzugte Labyrinth-Algorithmus ordnet die einzelnen Elemente eines eintreffenden Signals jeweils logischen Funktionen und Informationsverarbeitungspfaden zu so dass sich das Signal als Funktion der Zeit über dieses Labyrinth verteilt bzw. schrittweise in ihm fortschreitet.

In einer bevorzugten Ausgestaltung des Labyrinthes besteht das Labyrinth, welches als Algorithmus nach dem Stand der Technik z.B. in FPGA, Speicher und/oder Prozessor implementiert werden kann, funktionell aus einer Zahl von Pfaden mit Gabelungen, Richtungsfestlegungen und Toren, die sich als Funktion der Zeit ändern. Ein typischer Versuch eines Signals, das Labyrinth erfolgreich zu durchlaufen, umfasst die Gliederung des Signals in einzelne Signalelemente, die an unterschiedlichen Stellen im Labyrinth gestartet werden und deren Zeitverlauf genau zum Zeitverlauf des jeweiligen Labyrinth-Pfades passen muß. Nur wenn sich also die Signalelemente genau passend zum Labyrinthpfad z.B. bezüglich Geschwindigkeit und Bewegungsrichtung ändern, können an festgelegten Koppelpunkten die geforderten Prüfsignale zu den geforderten Zeiten auftreten. In dieser bevorzugten Ausführung gilt, dass nur, wenn das von der externen Komponente empfangene Signal als Autorisierungssignal und somit als Schlüssel aufgrund des speziell festgelegten Labyrinth-Durchlaufes die Koppelpunkte zu den vorgegebenen Zeiten mit dem jeweils für die Autorisierung vereinbarten Wert erreicht und hier z.B. von einem Schaltnetz oder Schaltwerk (vorzugsweise bestehend aus logischen Bausteinen bzw. Funktionen einschließlich Zeitverzögerungsglieder und

Verbindungsleitungen zu den einzelnen Koppelpunkten) detektiert wird und die Ausgangsignale der einzelnen Schaltnetzelemente (s. Fig. 4) wiederum von dem rechts angedeuteten UND-Gatter zeitlich koinzident bzw. in einem engen Zeitfenster als logische Eins bewertet werden, wird die Autorisierung vollzogen. Dabei wird die Koinzidenz der zu verschiedenen Zeiten an den Koppelpunkten detektierten Ereignisse durch Zeitverzögerungsglieder realisiert. Die zugehörigen Zeitfestlegungen und logischen Festlegungen des Schaltnetzes als Prüfsystem für die Zugehörigkeit von Schlüssel und Schloß sowie die das Schloß repräsentierenden Labyrinth-Festlegungen sind in die interne Komponente eingebettet und können daher nicht ausgeforscht werden und sind wegen der Implantation nicht zugänglich.

In einer bevorzugten Ausgestaltung des Verfahrens zum geschützten Betrieb wird der Vollzug der Autorisierung zur Verhinderung einer nicht autorisierten Vollzugsmeldung an die externe Komponente (Falschmeldung) nicht explizit an die externe Komponente gemeldet, sondern nur implizit durch die von der externen Komponente detektierbare Betriebsaufnahme der internen Komponente realisiert. Alternativ dazu wird der Vollzug jeweils durch ein nur einmal benutzbares und in der externen Komponente zwar richtig interpretierbares aber nicht explizit gespeichertes Signal von der internen an die externe Komponente gemeldet.

Eine weitere vorteilhafte Ausgestaltung des Verfahrens zum geschützten Betrieb besteht darin, dass die Autorisierung während des Betriebes verändert wird. Dies geschieht vorzugsweise dadurch, dass bereits bei der Festlegung von Autorisierungs-Schlüssel und Schloss im

Zusammenhang mit der Fertigung eines Paares von externer und interner Komponente, der Wechsel des Schlüssels oder/und des Schlosses z.B. nach jeder erfolgreichen Autorisierung in der externen bzw. der internen Komponente vorbereitet wird und entsprechend automatisch erfolgt.

Eine weitere vorteilhafte Ausgestaltung des Verfahrens zum geschützten Betrieb besteht darin, dass in einer implantierten Komponente gespeicherte personenbezogene Daten, die grundsätzlich der ärztlichen Schweigepflicht unterliegen, wie z.B. Art und intendierter Wirkmechanismus der Neuroprothese, Quantität, Art oder Zeitverlauf der therapeutischen oder / und diagnostischen Maßnahme mit einer hierfür gesonderten Zugangssicherung geschützt sind.

Eine weitere vorteilhafte Ausgestaltung des Verfahrens zum geschützten Betrieb besteht darin, dass im Falle einer Betriebsstörung oder eines anders gelagerten Notfalles die interne Komponente abgeschaltet bzw. funktionell stillgelegt, oder auf ein vorbereitetes Notfallprogramm umgeschaltet werden kann unter Verwendung eines hierfür separaten technischen Verfahrens und/oder mikroelektronischer Vorrichtung. Dieses Verfahren für den Zugriff auf Teilfunktionen der internen Komponente verwendet bevorzugt ein magnetostatisches Prinzip, also z.B. die Bewegung eines zur internen Komponente gehörigen Hebels mit ferromagnetischer Komponente, ein induktives Prinzip, also die induktive Einwirkung auf die interne Komponente, ein schalltechnisches Prinzip, also die Einwirkung auf einen Schaltmechanismus in der internen Komponente durch Schallsignale, ein mechanisches Prinzip, also z.B. die Anregung von mechanischen Druck-, Sog-,

Bewegungs-, oder Vibrationsdetektoren in der internen Komponente, bzw. die Anwendung anderer technisch bekannter physikalischer oder chemischer Prinzipien, um entsprechende Detektoren in der internen Komponente erreichen.

Eine weitere vorteilhafte Ausgestaltung des Verfahrens zum geschützten Betrieb besteht darin, dass die Aufhebung einer zuvor eingetretenen Sperre (siehe oben) mit Hilfe einer Authentifikation erfolgt, für die ein weiterer Schlüssel bei der Herstellung der Komponente in der Software und/oder der Hardware der Komponente implementiert wird, oder mit Hilfe eines im vorhergehenden Absatz genannten Verfahrens.

Eine weitere vorteilhafte Ausgestaltung des Verfahrens zum geschützten Betrieb besteht darin, dass die Verschlüsselung der zwischen externer und interner Komponente ausgetauschten Daten einschließlich des Autorisierungssignals in nicht zwingend periodischen Abständen wechselt. Es ist vorzugsweise vorgesehen, dass die Datenverschlüsselung und zugehörige Entschlüsselung vor Beginn der Autorisierung fest ist. Ferner ist vorzugsweise vorgesehen, dass sich die Datenverschlüsselung nach erfolgter Autorisierung in Abhängigkeit vom zuletzt verwendeten Autorisierungssignal in einer bei der Paarfertigung festgelegten Weise ändert.

Die Verschlüsselung der Datenübertragung erfolgt in dieser vorteilhaften Ausführung mit Hilfe eines Algorithmus zur Ver- und Entschlüsselung von Daten auf der Basis öffentlicher und privater Schlüssel. Jede externe und jede implantierte Komponente der Neuroprothese betreibt einen Schlüsselsatz bestehend aus

einem privaten Schlüssel, der nur innerhalb der jeweiligen Komponente bekannt ist, und aus einem öffentlichen Schlüssel, der zusätzlich innerhalb der übrigen Komponenten bekannt ist. Bei der Herstellung der Komponenten werden diese jeweils mit einem öffentlichen und einem privaten Initialschlüssel sowie mit den öffentlichen Initialschlüsseln der anderen Komponenten ausgestattet. Jede Komponente ersetzt in zufälligen Zeitabständen in der Größenordnung einiger Sekunden den eigenen Schlüsselsatz automatisch. Jede Komponente gibt den öffentlichen Schlüssel an die anderen Komponenten verschlüsselt weiter, sobald dieser geändert wurde. Zum Zweck der Verschlüsselung der Daten verfügt jede Komponente über elektronische Leitungen, einen Speicher und einen Prozessor, die gemeinsam die Implementierung des Verschlüsselungsalgorithmus darstellen. Die Verschlüsselung der Daten erfolgt derart, dass der Verschlüsselungsalgorithmus aus den Daten, dem privaten Schlüssel der sendenden Komponente und aus dem öffentlichen Schlüssel der Komponente, an die die Daten gesendet werden sollen, neue Daten generiert. Diese Daten werden gesendet und von der empfangenden Komponente mittels des öffentlichen Schlüssels der sendenden Komponente und des privaten Schlüssels der empfangenden Komponente entschlüsselt. Der Entschlüsselungsalgorithmus ist derart gestaltet, dass empfangene Daten, die mit anderen als den oben vorgesehenen Schlüsseln verschlüsselt wurden, von der empfangenden Komponente ignoriert werden.

Eine weitere vorteilhafte Ausgestaltung des Verfahrens zum geschützten Betrieb besteht darin, dass die verschlüsselte Kommunikation nach dem Prinzip eines Verschlüsselungssystems mit einem öffentlichen und einem

privaten Schüssel aufgebaut ist. Der Sender einer Nachricht (interne oder externe Komponente) verschlüsselt die Nachricht mit dem nur in der sendenden Komponente im bekannten privaten Schlüssel, der mikroelektronisch und/oder softwaretechnisch bei der Herstellung der Komponente eingestellt wird. Der Empfänger dieser Nachricht entschlüsselt diese anhand der Information, von welcher Komponente sie gesendet wurde und mit dem öffentlichen Schlüssel der sendenden Komponente, der mikroelektronisch und/oder softwaretechnisch bei der Herstellung der Komponente eingestellt wird. Es wird keine technische Vorrichtung zum Auslesen des eingestellten Schlüssels weder in der externen noch in der internen Komponente implementiert.

Eine weitere vorteilhafte Ausgestaltung des Verfahrens zum geschützten Betrieb besteht darin, dass eine Authentifikation zur Freischaltung der internen und der externen Komponenten verwendet wird. Dabei wird die Software und/oder Hardware der Komponenten mit Hilfe von Freischaltungsschlüsseln entschlüsselt bzw. initialisiert. Die Freischaltung ist nur dann möglich, wenn alle bei der Herstellung der Komponenten vordefinierten Komponenten vorhanden sind und miteinander kommunizieren. Es wird keine technische Vorrichtung zum unverschlüsselten Auslesen des eingestellten Freischaltungsschlüssels weder in der externen noch in der internen Komponente implementiert.

Eine weitere vorteilhafte Ausgestaltung des Verfahrens zum geschützten Betrieb besteht darin, dass um einen Nachbau der Software zu vermeiden, die Software-Komponenten der externen und/oder internen Komponenten bei der Herstellung in der verschlüsselten Form

gespeichert werden. Zur Inbetriebnahme einer internen und/oder externen Komponente wird zuerst ein Entschlüsselungsprogramm gestartet, das die Freischaltungsschlüssel von allen anderen internen und/oder externen Komponenten durch den verschlüsselten Kanal bezieht und das Hauptprogramm der Komponente entschlüsselt. Wenn zumindest ein Schlüssel falsch empfangen wird, wird das Hauptprogramm falsch entschlüsselt und wird dadurch funktionsunfähig.

Eine weitere vorteilhafte Ausgestaltung des Verfahrens zum geschützten Betrieb besteht darin, dass die Authentifikation in einer vorbestimmten Reihenfolge abläuft, z.B. zuerst werden die Freischaltungsschlüssel aus internen Komponenten über den verschlüsselten Kanal ausgelesen und damit wird die Software der externen Komponenten entschlüsselt und deren Hardwarekomponente initialisiert. Alternativ erfolgt dies nach einem stochastischem Prinzip.

Eine weitere vorteilhafte Ausgestaltung des Verfahrens zum geschützten Betrieb besteht darin, dass die Freischaltungsschlüssel anhand der biometrischen Merkmale (z.B. Iris, Fingerabdruck, Stimme, genetischer Abdruck, Gehirnwellen, bioelektrische Eigenschaften der Gewebe) des Implantatträgers erstellt werden. Damit wird ein nichtautorisierter Betrieb der Neuroprothese in der Abwesenheit des Implantatträgers verhindert.

Eine weitere vorteilhafte Ausgestaltung des Verfahrens zum geschützten Betrieb besteht darin, dass eine Autorisierung jeder Komponente nach der Authentifikation und permanent bzw. wiederholt während des Betriebs erfolgt, und zur Detektion möglicher Angriffe dient. Die

Autorisierung erfolgt mittels Autorisierungsschlüssel. Jede interne und externe Komponente beinhaltet einen eigenen Autorisierungsschlüssel, der entweder stochastisch und/oder anhand der Herstellerdaten und/oder biometrischen Daten des Implantatträgers erstellt wird und mikroelektronisch und/oder softwaretechnisch bei der Herstellung der Komponente eingestellt wird.

Eine weitere vorteilhafte Ausgestaltung des Verfahrens zum geschützten Betrieb besteht darin, dass zwischen zwei Arten des NIS-Betriebs unterschieden wird: Einstellungsbetrieb und autonomer Betrieb. Während des Einstellungsbetriebes findet eine Kommunikation zwischen dem Implantatträger und einem PC, oder zwischen dem Arzt und einem PC, oder zwischen einer anderen legitimierten Person und dem PC statt. Jeder Person wird ein unikales Passwort zugewiesen, das zusammen mit Autorisierungsschlüsseln der internen und/oder externen Komponenten die Berechtigungen zum Betrieb der Neuroprothese definieren. Die Passworte unterliegen der Geheimhaltungspflicht.

Eine weitere vorteilhafte Ausgestaltung des Verfahrens zum geschützten Betrieb besteht darin, dass der Einstellbetrieb der Neuroprothese nur nach einer Versetzung des Implantatträgers in einen für den autonomen Betrieb der Neuroprothese ungewöhnlichen psychischen und/oder physiologischen Zustand erfolgt, der mit vorhandenen elektromagnetischen bzw. elektrochemischen bzw. optischen bzw. thermischen bzw. mechanischen Sensoren identifiziert werden kann (z.B. Schlafzustand kann mittels Detektion von alpha- und beta-Wellen des Gehirns identifiziert werden, erhöhter pH-Wert kann mit einem pH-Sensor gemessen werden, erhöhte oder

erniedrigte Körpertemperatur z.B. mittels Temperaturmessung, erhöhte Durchblutung der Haut z.B. mittels optischer Sensoren).

Eine weitere vorteilhafte Ausgestaltung des Verfahrens zum geschützten Betrieb besteht darin, dass im autonomen Betrieb eine Autorisierung nach einem Zustandsmuster erfolgt. Das Zustandsmuster wird durch Autorisierungsschlüssel und/oder interne Signale und/oder Zustände der internen und /oder externen Komponenten definiert (z.B. bei einer Neuroprothese werden die Stimulationssignale und/oder Zustände der spatialen und/oder temporalen Filter zur Beschreibung des Zustandsmusters benutzt). Die internen Signale und Zustände identifizieren eindeutig den Implantatträger und kommen in keiner anderen Neuroprothese in der Kombination des Zustandsmusters vor.

Eine weitere vorteilhafte Ausgestaltung des Verfahrens zum geschützten Betrieb besteht darin, dass die interne Komponente oder/und die externe Komponente sowohl im Falle unerwünschter Funktionen, wie einer Fehlfunktion der Neuroprothese, eines versuchten Betriebsmissbrauchs oder /und eines für den autorisierten Betrieb nicht vorgesehenen Zugriffsversuchs auf Daten oder Funktion der Neuroprothese, als auch im Falle bestimmter autorisierter Funktionen, wie z.B. bei der Abfrage von personenbezogenen Daten aus einer internen Komponente, gesonderte Signale auslöst. Dieses Alarmsignal im einen Fall bzw. Statussignal im anderen Fall wird in einer bevorzugten Ausgestaltung allein dem Implantatträger zur Kenntnis gebracht, z.B. durch Auslösung einer über Mechanorezeptoren wahrnehmbaren Empfindung.

Patentansprüche

1. Verfahren zum Betrieb einer Neuroprothese im zentralen Nervensystem innerhalb des Schädels, des Rückenmarks oder mit dem Rückenmark verbundener peripherer Nerven, oder einer Sehprothese oder Hörprothese, wobei die Neuroprothese eine implantierte interne Komponente und eine nicht implantierte externe Komponente umfasst, wobei weiter eine drahtlose Datenübertragung zwischen der internen und der externen Komponente vorgesehen ist, **dadurch gekennzeichnet, dass** die Datenübertragung eines Teiles der Daten oder aller Daten nur dann erfolgt, wenn ein von der externen Komponente an die interne Komponente übermitteltes Autorisierungssignal geprüft und akzeptiert worden ist.

2. Verfahren zum Betrieb einer Neuroprothese im zentralen Nervensystem innerhalb des Schädels, des Rückenmarks sowie mit dem Rückenmark verbundener peripherer Nerven, oder einer Sehprothese oder Hörprothese, wobei die Neuroprothese eine implantierte interne und eine nicht implantierte externe Komponente umfasst, wobei weiter die interne Komponente in Kontakt oder Wirkungszusammenhang mit Nervengewebe steht und im Betrieb eine Funktion des Nervengewebes überwachen, beeinflussen oder ersetzen kann, **dadurch gekennzeichnet, dass** der Betrieb der internen Komponente nur dann erfolgt, wenn ein von der externen

Komponente an die interne Komponente übermitteltes Autorisierungssignal geprüft und akzeptiert worden ist.

3. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet, dass** das von der internen Komponente akzeptierte Autorisierungssignal genau einer externen Komponente oder genau zwei externen Komponenten zugeordnet ist.

4. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet, dass** das von der internen Komponente akzeptierte Autorisierungssignal Teil eines Datenstroms ist, der von der externen Komponente an die interne Komponente übermittelt wird.

5. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** die Überprüfung des Autorisierungssignals in der internen Komponente mittels eines programmierbaren Speichers erfolgt.

6. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** die Überprüfung des Autorisierungssignals in der internen Komponente mittels einer festen topologischen Halbleiterstruktur erfolgt.

7. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** für die Datenübertragung oder Funktion der internen Komponente mindestens zwei Betriebszustände möglich sind, die mittels unterschiedlicher Autorisierungssignale aktivierbar sind.

8. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** im Falle einer

Betriebsstörung mit einem zweiten Autorisierungsverfahren eine Abschaltung oder ein Notfallprogramm der internen Komponente vorgenommen werden kann, wobei das zweite Verfahren vorzugsweise nach einem anderen Funktionsprinzip (technischen Verfahren) arbeitet als das erste Verfahren.

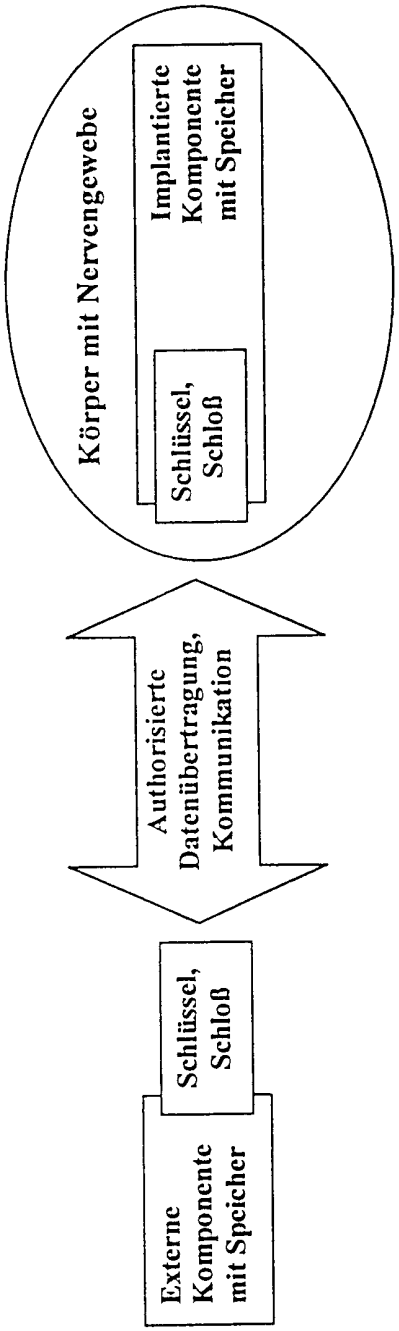
9. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** die interne Komponente im Betrieb mit einer weiteren implantierten Komponente Daten austauscht.

10. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** die Datenübertragung verschlüsselt erfolgt, wobei vorzugsweise die interne Komponente einen programmierbaren oder mittels einer festen toplogischen Halbleiterstruktur definierten Schlüssel enthält.

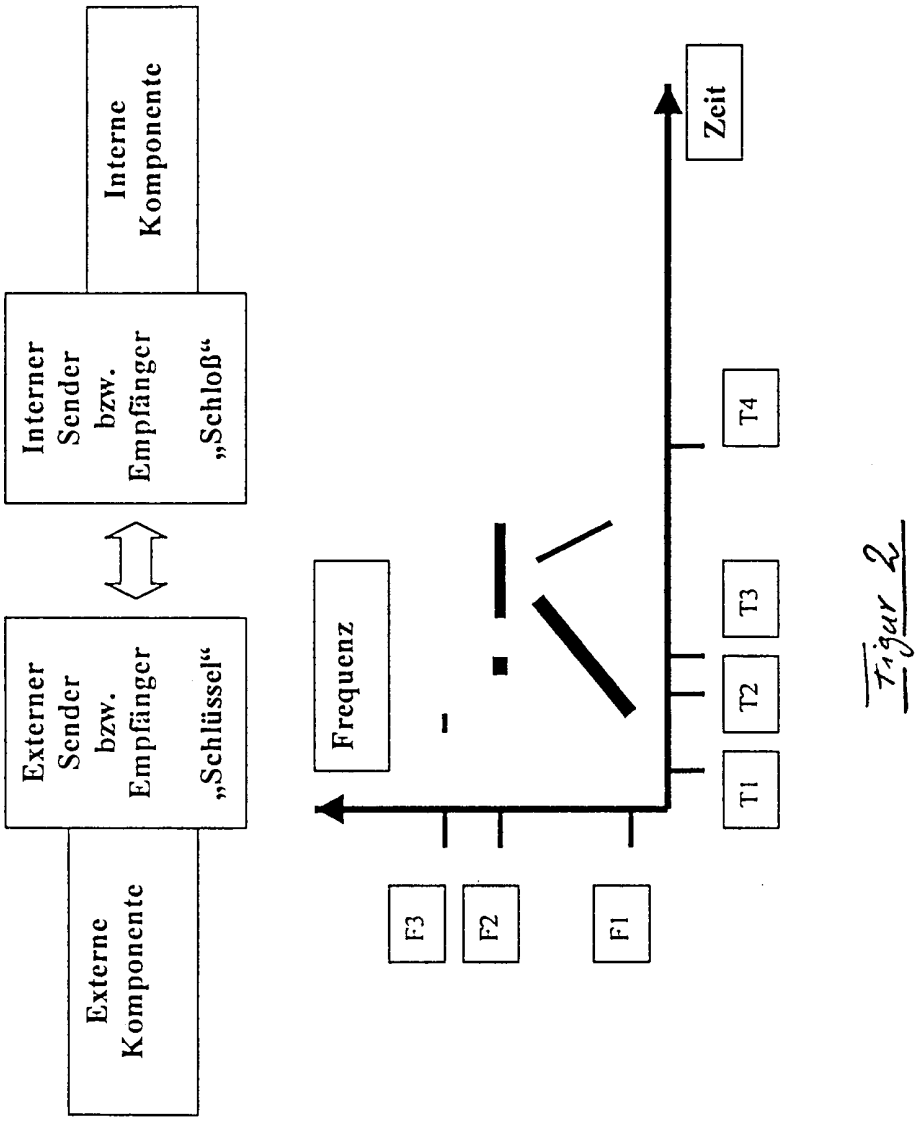
11. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** nach einer Anzahl von geprüften und nicht akzeptierten Autorisierungsversuchen die Annahme weiterer Autorisierungsversuche zeitweise oder permanent gesperrt wird und dass eine Aufhebung der Sperre nur mittels eines im normalen Betrieb nicht erforderlichen Autorisierungssignals erfolgen kann.

12. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** nach einer akzeptierten Autorisierung kein die Autorisierung anzeigendes Statussignal von der internen Komponente an die externe Komponente übermittelt wird.

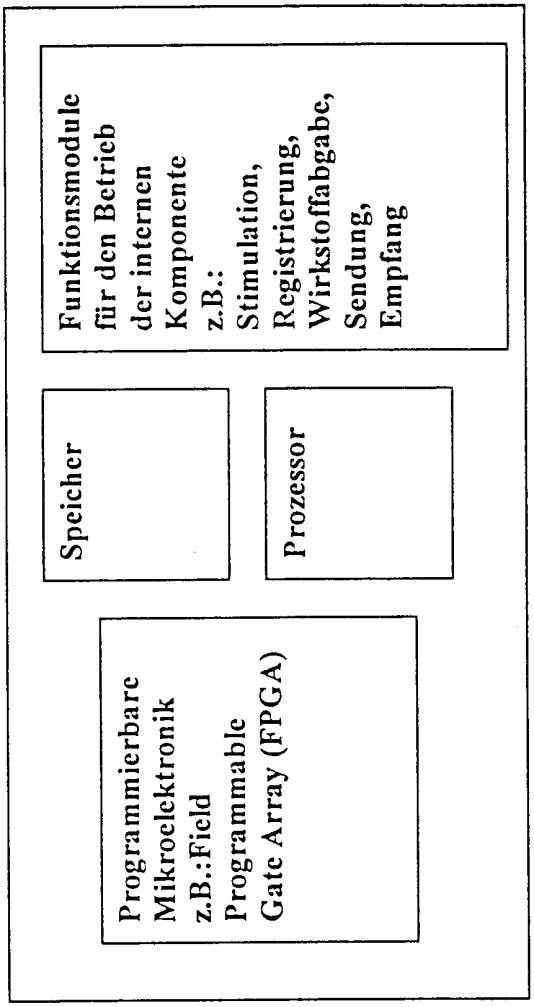
13. Vorrichtung zur Durchführung des Verfahrens nach einem der vorhergehenden Ansprüche 1 bis 12.


Körper mit Nervengewebe
Implantierte Komponente mit Speicher
Schlüssel, Schloß
Authorisierte Datenübertragung, Kommunikation
Externe Komponente mit Speicher
Schlüssel, Schloß

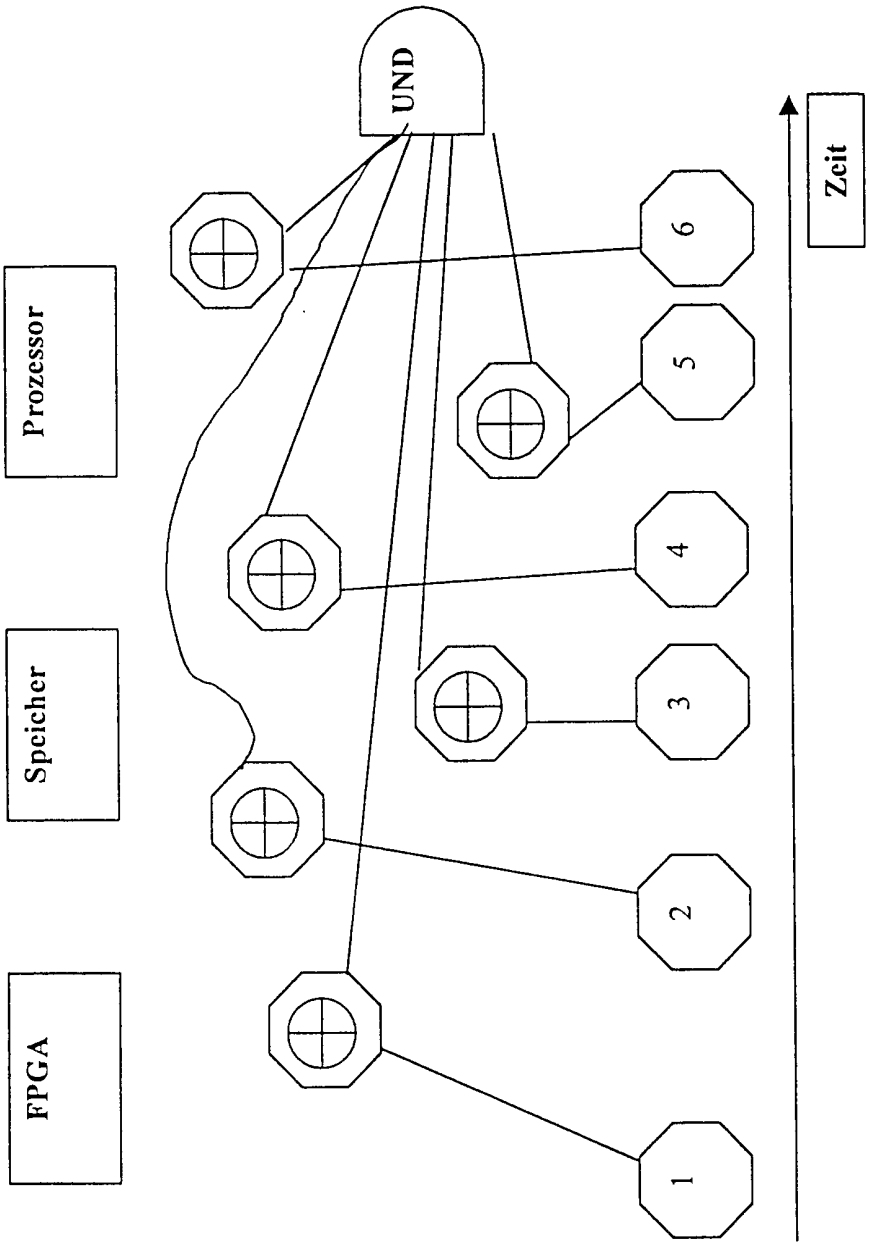
Figur 1


Interne Komponente
Interner Sender bzw. Empfänger „Schloß“
Externer Sender bzw. Empfänger „Schlüssel“
Externe Komponente
Frequenz
Zeit
F3
F2
F1
T1
T2
T3
T4

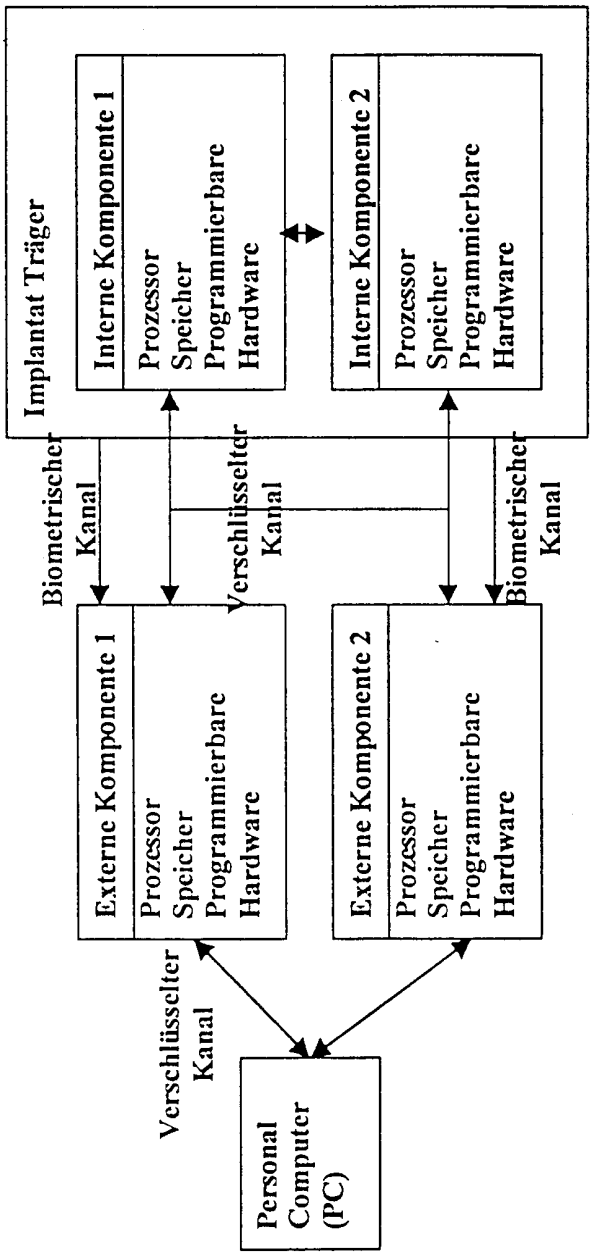
Figur 2


Programmierbare Mikroelektronik z.B.:Field Programmable Gate Array (FPGA)
Speicher
Prozessor
Funktionsmodule für den Betrieb der internen Komponente z.B.: Stimulation, Registrierung, Wirkstoffabgabe, Sendung, Empfang

Figur 3



Figur 4


Implantat Träger
Interne Komponente 1
Prozessor
Speicher
Programmierbare
Hardware
Interne Komponente 2
Prozessor
Speicher
Programmierbare
Hardware
Biometrischer Kanal
Verschlüsselter Kanal
Biometrischer Kanal
Externe Komponente 1
Prozessor
Speicher
Programmierbare
Hardware
Externe Komponente 2
Prozessor
Speicher
Programmierbare
Hardware
Verschlüsselter Kanal
Personal Computer (PC)

Figur 5

INTERNATIONAL SEARCH REPORT

Interr ıal Application No
PCT/EP 00/06666

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 A61N1/36 A61N1/372

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)
IPC 7 A61N

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 practical, 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.
X	WO 86 02567 A (ZION FOUNDATION) 9 May 1986 (1986-05-09) page 2, line 15 - line 27 page 5, line 28 -page 6, line 10 page 7, line 31 -page 8, line 8 page 9, line 16 - line 32 page 11, line 7 - line 16 page 14, line 14 - line 26 page 16, line 20 -page 17, line 25 figures --- -/--	1-4

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in 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 document 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
3 October 2000	11/10/2000

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, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Ferrigno, A

2

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Interr ıal Application No
PCT/EP 00/06666

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 954 758 A (PECKHAM PAUL HUNTER ET AL) 21 September 1999 (1999-09-21) column 2, line 8 - line 9 column 3, line 9 - line 17 column 5, line 49 -column 6, line 26 column 20, line 59 - line 67 figures	1,2
A		3-5,10, 13
X	US 5 169 384 A (BOSNIAK STEPHEN L ET AL) 8 December 1992 (1992-12-08) column 3, line 5 - line 26 column 11, line 3 - line 29	1,2
A	US 5 752 976 A (DUFFIN EDWIN G ET AL) 19 May 1998 (1998-05-19) cited in the application column 7, line 9 - line 14 column 9, line 21 - line 45 column 11, line 62 -column 12, line 26 figures	1,2

2

INTERNATIONAL SEARCH REPORT

/ormation on patent family members

Interr ıal Application No
PCT/EP 00/06666

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 8602567 A	09-05-1986	AU 5062385 A	15-05-1986
		EP 0202258 A	26-11-1986
		JP 62501192 T	14-05-1987
US 5954758 A	21-09-1999	US 6026328 A	15-02-2000
		US 5776171 A	07-07-1998
		US 5769875 A	23-06-1998
US 5169384 A	08-12-1992	NONE	
US 5752976 A	19-05-1998	AU 709767 B	09-09-1999
		AU 6176996 A	22-01-1997
		CA 2224520 A	09-01-1997
		EP 0939662 A	08-09-1999
		JP 11508165 T	21-07-1999
		WO 9700708 A	09-01-1997
		US 6083248 A	04-07-2000

INTERNATIONALER RECHERCHENBERICHT

Internales Aktenzeichen
PCT/EP 00/06666

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 A61N1/36 A61N1/372

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

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 A61N

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.
X	WO 86 02567 A (ZION FOUNDATION) 9. Mai 1986 (1986-05-09) Seite 2, Zeile 15 - Zeile 27 Seite 5, Zeile 28 -Seite 6, Zeile 10 Seite 7, Zeile 31 -Seite 8, Zeile 8 Seite 9, Zeile 16 - Zeile 32 Seite 11, Zeile 7 - Zeile 16 Seite 14, Zeile 14 - Zeile 26 Seite 16, Zeile 20 -Seite 17, Zeile 25 Abbildungen --- -/--	1-4

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] 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" älteres Dokument, 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 anderen 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
3. Oktober 2000	11/10/2000

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Ferrigno, A

2

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Interr nales Aktenzeichen
PCT/EP 00/06666

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 5 954 758 A (PECKHAM PAUL HUNTER ET AL) 21. September 1999 (1999-09-21) Spalte 2, Zeile 8 - Zeile 9 Spalte 3, Zeile 9 - Zeile 17 Spalte 5, Zeile 49 -Spalte 6, Zeile 26 Spalte 20, Zeile 59 - Zeile 67 Abbildungen	1,2
A		3-5,10, 13
X	US 5 169 384 A (BOSNIAK STEPHEN L ET AL) 8. Dezember 1992 (1992-12-08) Spalte 3, Zeile 5 - Zeile 26 Spalte 11, Zeile 3 - Zeile 29	1,2
A	US 5 752 976 A (DUFFIN EDWIN G ET AL) 19. Mai 1998 (1998-05-19) in der Anmeldung erwähnt Spalte 7, Zeile 9 - Zeile 14 Spalte 9, Zeile 21 - Zeile 45 Spalte 11, Zeile 62 -Spalte 12, Zeile 26 Abbildungen	1,2

2

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichur., , die zur selben Patentfamilie gehören

Interr ales Aktenzeichen
PCT/EP 00/06666

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 8602567 A	09-05-1986	AU 5062385 A	15-05-1986
		EP 0202258 A	26-11-1986
		JP 62501192 T	14-05-1987
US 5954758 A	21-09-1999	US 6026328 A	15-02-2000
		US 5776171 A	07-07-1998
		US 5769875 A	23-06-1998
US 5169384 A	08-12-1992	KEINE	
US 5752976 A	19-05-1998	AU 709767 B	09-09-1999
		AU 6176996 A	22-01-1997
		CA 2224520 A	09-01-1997
		EP 0939662 A	08-09-1999
		JP 11508165 T	21-07-1999
		WO 9700708 A	09-01-1997
		US 6083248 A	04-07-2000