



Europäisches Patentamt
European Patent Office
Office européen des brevets



(11) **EP 1 669 824 A1**

(12) **EUROPÄISCHE PATENTANMELDUNG**

(43) Veröffentlichungstag:
14.06.2006 Patentblatt 2006/24

(51) Int Cl.:
G05B 19/05 (2006.01)

(21) Anmeldenummer: **05110582.3**

(22) Anmeldetag: **10.11.2005**

(84) Benannte Vertragsstaaten:
**AT BE BG CH CY CZ DE DK EE ES FI FR GB GR
HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI
SK TR**
Benannte Erstreckungsstaaten:
AL BA HR MK YU

(71) Anmelder: **SIEMENS AKTIENGESELLSCHAFT
80333 München (DE)**

(72) Erfinder: **Temming, Rudolf
38154, Königslutter (DE)**

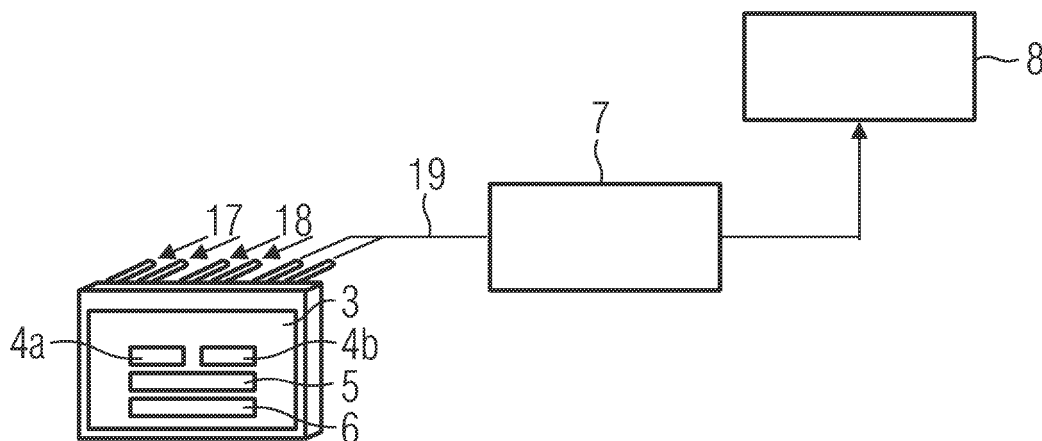
(30) Priorität: **08.12.2004 DE 102004059717**

(54) **Verfahren und Vorrichtung zur Vorgabe einer Betriebsartennummer**

(57) Die Erfindung betrifft ein Verfahren und eine Vorrichtung zur Vorgabe einer Betriebsartennummer (4a) für sicherheitsrelevante Prozesse, insbesondere Bahnbetriebsprozesse, wobei ein hohes Sicherheitsni-

veau bei minimalem Hardwareaufwand erreicht wird, indem die Betriebsartennummer (4a) und gegebenenfalls weitere Daten, als Datensatz mit einem Sicherungsanhang über eine serielle Schnittstelle in einen nichtflüchtigen Speicher eingelesen werden.

FIG 2



EP 1 669 824 A1

Beschreibung

[0001] Verfahren und Vorrichtung zur Vorgabe einer Betriebsartennummer

[0002] Die Erfindung betrifft ein Verfahren zur Vorgabe einer Betriebsartennummer gemäß dem Oberbegriff des Anspruchs 1 und eine diesbezügliche Vorrichtung gemäß dem Oberbegriff des Anspruchs 2.

[0003] Die nachfolgende Beschreibung bezieht sich im Wesentlichen auf sicherheitsrelevante Bahnbetriebsprozesse, ohne dass die Erfindung auf diese Anwendung beschränkt sein soll.

[0004] Sicherheitsrelevante Bahnbetriebsprozesse betreffen insbesondere die Ansteuerung von Feldelementen, beispielsweise Weichen und Signale. Dazu dienen Stellwerkselemente, über die unter anderem auch Betriebsartennummern, beispielsweise für Normalbetrieb oder Antriebsersatz, vorgegeben werden. Mit der Betriebsartennummer wird die Verarbeitungssoftware der Stellwerkselemente in bestimmter Weise initialisiert, d. h. zu einem bestimmten Verhalten gezwungen. Die Betriebsartennummer muss daher signaltechnisch sicher vorgegeben werden.

[0005] Bekannt sind Betriebsartenstecker, die durch Brücken im Stecker das Verhalten der Verarbeitungssoftware bestimmen. Nachteilig bei diesen Betriebsartensteckern ist vor allem deren erheblicher Hardwareaufwand.

[0006] Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren und eine Vorrichtung gattungsgemäßer Art anzugeben, die sich durch geringeren Hardwareaufwand auszeichnen, wobei die Betriebsartenwahl die Sicherheitsanforderungsstufe SIL4 nach CENELC erfüllt.

[0007] Die Aufgabe wird verfahrensgemäß mit den kennzeichnenden Merkmalen des Anspruches 1 und vorrichtungsgemäß mit den kennzeichnenden Merkmalen des Anspruches 2 gelöst. Durch das Einschreiben der Betriebsartennummer zusammen mit einem Sicherungsanhang in einen nichtflüchtigen Speicher ist eine sehr hohe Sicherheit bezüglich der Korrektheit der Betriebsartennummer und damit der entsprechenden Auswirkungen auf den sicherheitsrelevanten Prozess gegeben. Ein weiterer Vorteil gegenüber dem bekannten Betriebsartenstecker mit Brücken besteht darin, dass neben der Betriebsartennummer zusätzlich eine Teilnehmernummer und gegebenenfalls weitere Daten gespeichert werden können. Darüber hinaus ist bei geringem Volumen des Speichermoduls nur minimaler Hardwareaufwand erforderlich. Der Datensatz, bestehend aus Betriebsartennummer, Teilnehmernummer, gegebenenfalls weiteren Daten und Sicherungsanhang, lässt sich über eine serielle Schnittstelle sehr einfach in den nichtflüchtigen Speicher einlesen.

[0008] Vorzugsweise ist der Sicherungsanhang gemäß Anspruch 3 als MD4-Signatur (Message Digest) ausgebildet. Durch die kryptografische MD4-Funktion wird der Eingabedatensatz in einen kurzen Wert fester Länge, den Hashwert, umgewandelt. Bei diesem Algo-

rithmus verändern sich Variablen mittels nichtlinearer Transformationen anhand der Eingabedaten, d. h. des auf Datenintegrität zu prüfenden Datensatzes, und bilden dadurch einen eindeutigen Hashwert. Bei einer guten Hashfunktion gibt es kaum zwei Datensätze, die denselben Hashwert besitzen. Weiterhin beeinflussen geringe Änderungen des Eingabedatensatzes bei einer guten Hashfunktion den Hashwert sehr stark. Bei dem MD4-Algorithmus sind vier Variablen vorgesehen, die in drei Runden in die Berechnung des Hashwertes eingehen. Um noch größere Sicherheit hinsichtlich des Nachweises der Datenintegrität zu erreichen, kann auch eine höhere Version des MD-Algorithmus, beispielsweise MD5 eingesetzt werden. Es können auch andere Verfahren zur Sicherung genutzt werden, beispielsweise CRC16 oder CRC32. Der Sicherungsanhang wird über den gesamten Datensatz gebildet.

[0009] Als nichtflüchtiger Speicher wird gemäß Anspruch 4 vorzugsweise ein EEPROM (electrically erasable programmable read only memory) eingesetzt. Dieser Festwertspeicher zeichnet sich dadurch aus, dass der Programmiervorgang und auch der Löschvorgang sehr einfach mittels eines Computers oder eines Peripheriegerätes möglich sind.

[0010] Die serielle Schnittstelle zum Speicher ist gemäß Anspruch 5 als I2C-Schnittstelle ausgebildet. Der I2C-Bus ist ein sehr häufig eingesetzter 2-Draht-Bus und wurde speziell für die Kommunikation zwischen einzelnen Komponenten innerhalb eines Gerätes entwickelt. Der Datensatz mit der Betriebsartennummer kann über die I2C-Schnittstelle mit besonders geringem Aufwand eingelesen werden. Da üblicherweise mehrere Komponenten parallel an einem I2C-Bus hängen, ist es nötig, auch die Teilnehmeradresse zu speichern.

[0011] Der Speicher selbst ist gemäß Anspruch 6 in einem Betriebsartenstecker integriert. Der Betriebsartenstecker ist vorzugsweise äußerlich mit der Betriebsartennummer beschriftet und wird bedarfsweise in ein Frontplattenmodul eines Mikro-Controllers, der die Verarbeitungssoftware enthält, eingesetzt.

[0012] Nachfolgend wird die Erfindung anhand figürlicher Darstellungen näher erläutert.

[0013] Es zeigen:

Figur 1 Betriebsartenstecker im Zusammenwirken mit einem Frontplattenmodul und
Figur 2 eine Architekturspezifikation des Betriebsartensteckers.

[0014] Figur 1 zeigt beispielhaft zwei Betriebsartenstecker 1 und 2, wobei der erste Betriebsartenstecker 1 für Normalbetrieb und der zweite Betriebsartenstecker 2 für Antriebsersatz bei der Ansteuerung einer Weichenbaugruppe vorgesehen sind. Die Betriebsartenstecker 1 und 2 sind jeweils mit einem EEPROM 3 (Fig. 2) zur Speicherung der zugeordneten Betriebsartennummer 4a, einer Teilnehmernummer 4b, einer Teilnehmeradresse 5 und einer MD4-Signatur 6 ausgestattet (Figur 2).

Damit der Betriebsartenstecker 1 bzw. 2 in ein Frontplattenmodul 7, das mit einem Mikro-Controller 8 (Figur 2) verbunden ist, auf einfache Weise eingesteckt und abgezogen werden kann, ist ein Griff 9 an den Betriebsartenstecker 1 bzw. 2 angeformt. Der Betriebsartenstecker 1 bzw. 2 ist dabei derart gestaltet, dass ein kontaktsicheres Einstecken in eine Steckerbuchse 10 des Frontplattenmoduls 7 möglich ist, wobei der Betriebsartenstecker 1 bzw. 2 bündig mit der Oberfläche des Frontplattenmoduls 7 abschließt und sich nicht durch Erschütterungen lösen kann. Wird kein Betriebsartenstecker 1 bzw. 2 genutzt, kann auch eine Blindplatte ohne jede elektrische Funktionalität gesteckt werden. Mit dem Betriebsartenstecker 1 bzw. 2 wird der Verarbeitungssoftware in dem Mikro-Controller 8 mitgeteilt, wie sie sich zu verhalten hat. Der Betriebsartenstecker 1 bzw. 2 ist mit der Nummer der Betriebsart deutlich beschriftet. Diese Nummer wird blinkend in einem Diagnosedisplay 11 auf dem Frontplattenmodul 7 angezeigt. Der signaltechnisch sicher aufgebaute Mikro-Controller 8 liest zyklisch über das Frontplattenmodul 7 den Datensatz aus den Betriebsartenstecker 1 bzw. 2. Auf dem Frontplattenmodul 7 sind neben der Steckerbuchse 10 und dem Diagnosedisplay 11 verschiedene Schalter 12 und 13, eine Diagnosebuchse 14 sowie Statusanzeigen 15 und eine LED-Matrix 16 zur Prozessanzeige vorgesehen.

[0015] Figur 2 veranschaulicht den Datenfluss von dem Betriebsartenstecker 1 bzw. 2 über das Frontplattenmodul 7 zum Mikro-Controller 8. Der Datensatz für den Betriebsartenstecker 1 bzw. 2 wird über eine I2C-Schnittstelle 17 geladen. Dabei muss sichergestellt sein, dass die Daten des Betriebsartensteckers 1 bzw. 2 im gesteckten Zustand nicht verändert werden können. Weiterhin ist der Betriebsartenstecker 1 bzw. 2 mit einer Stromversorgung 18 und einem seriellen I2C-Bus 19 verbunden. Über den I2C-Bus 19 liest das Frontplattenmodul 7 den Datensatz und überprüft diesen zweikanalig anhand der MD4-Signatur auf Datenintegrität. Danach wird die Betriebsartennummer ohne MD4-Signatur an die Abbildspeicher des zweikanaligen Mikro-Controllers 8 weitergeleitet. Wird der Betriebsartenstecker 1 bzw. 2 gezogen oder hat die Betriebsartennummer sich geändert, wird auf dem Diagnosedisplay 11 des Frontplattenmoduls 7 ein Fehler angezeigt. Da die Betriebsartennummer 4 auf dem EEPROM 3 durch die MD4-Signatur 6 abgesichert ist, kann die Datenintegrität auf sehr hohem Sicherheitsniveau gemäß der Sicherheitsanforderungsstufe SIL 4 nach CENELEC überwacht werden.

[0016] Die Erfindung beschränkt sich nicht auf das vorstehend angegebene Ausführungsbeispiel. Vielmehr ist eine Anzahl von Varianten denkbar, welche auch bei grundsätzlich anders gearteter Ausführung von den Merkmalen der Erfindung Gebrauch machen.

(4a) für sicherheitsrelevante Prozesse, insbesondere Bahnbetriebsprozesse, **dadurch gekennzeichnet, dass** die Betriebsartennummer (4a) und gegebenenfalls weitere Daten als Datensatz mit einem Sicherungsanhang über eine serielle Schnittstelle in einen nichtflüchtigen Speicher eingelesen werden.

2. Vorrichtung zur Durchführung des Verfahrens nach Anspruch 1, **dadurch gekennzeichnet, dass** ein nichtflüchtiger Speicher mit einer seriellen Schnittstelle vorgesehen ist, wobei die Betriebsartennummer (4a) und gegebenenfalls weitere Daten, als Datensatz mit einem Sicherungsanhang über die Schnittstelle in den Speicher einlesbar sind.
3. Vorrichtung nach Anspruch 2, **dadurch gekennzeichnet, dass** der Sicherungsanhang als MD4-Signatur (6) über den gesamten Datensatz ausgebildet ist.
4. Vorrichtung nach Anspruch 2, oder 3, **dadurch gekennzeichnet, dass** der Speicher als EEPROM (3) ausgebildet ist.
5. Vorrichtung nach einem der Ansprüche 2 bis 4, **dadurch gekennzeichnet, dass** die Schnittstelle als I2C-Schnittstelle (17) ausgebildet ist.
6. Vorrichtung nach einem der Ansprüche 2 bis 5, **dadurch gekennzeichnet, dass** der Speicher in einem Betriebsartenstecker (1, 2) integriert ist.

Patentansprüche

1. Verfahren zur Vorgabe einer Betriebsartennummer

FIG 1

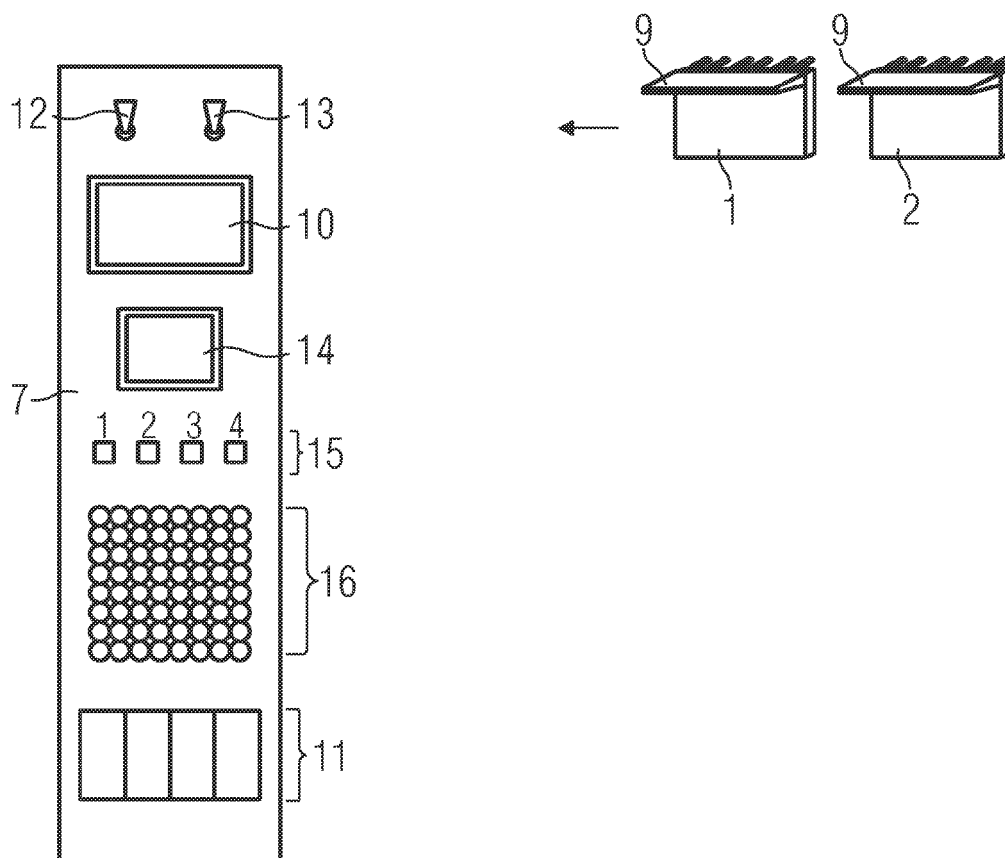
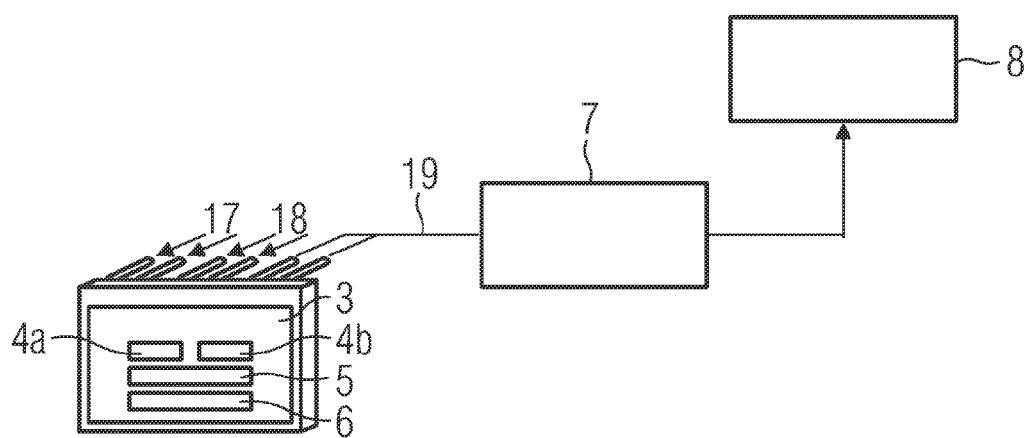


FIG 2





Europäisches
Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 05 11 0582

EINSCHLÄGIGE DOKUMENTE			
Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (IPC)
X	US 5 659 705 A (MCNUTT ET AL) 19. August 1997 (1997-08-19) * Abbildung 3 * * Zusammenfassung * * Spalte 3, Zeile 13 - Zeile 22 * * Spalte 10, Zeile 24 - Zeile 39 * -----	1-6	G05B19/05
A	DE 41 14 921 A1 (AHLBORN MESS- UND REGELUNGSTECHNIK, 8150 HOLZKIRCHEN, DE) 12. November 1992 (1992-11-12) * Spalte 1, Zeile 28 - Zeile 45; Abbildung 5 * * Spalte 4, Zeile 50 - Zeile 69 * -----	1-6	
A	DE 100 40 866 A1 (ALCATEL, PARIS) 7. März 2002 (2002-03-07) * Absätze [0001], [0021] * -----	3	
A	LENNARTZ K: "SIGNALTECHNISCH SICHERE DATENUEBERTRAGUNG IM RAHMEN VON CIRNET" 1. April 1993 (1993-04-01), SIGNAL + DRAHT, TELZLAFF VERLAG GMBH. DARMSTADT, DE, PAGE(S) 96-101, XP000380305 ISSN: 0037-4997 * Absatz [03.4] * -----	3	RECHERCHIERTE SACHGEBIETE (IPC) G05B
A	RIVEST R L ED - MENEZES A J ET AL INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH: "THE MD4 MESSAGE DIGEST ALGORITHM" 30. Dezember 1991 (1991-12-30), ADVANCES IN CRYPTOLOGY - PROCEEDINGS OF CRYPTO. SANTA BARBARA, AUG. 11, PAGE(S) 303-311 , XP000260021 * Zusammenfassung * * Seite 304, Absatz 3 * ----- -/-	3	
Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt			
Recherchenort München		Abschlußdatum der Recherche 6. April 2006	Prüfer Jünger, B
KATEGORIE DER GENANNTEN DOKUMENTE X : von besonderer Bedeutung allein betrachtet Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie A : technologischer Hintergrund O : mündliche Offenbarung P : Zwischenliteratur		T : der Erfindung zugrunde liegende Theorien oder Grundsätze E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist D : in der Anmeldung angeführtes Dokument L : aus anderen Gründen angeführtes Dokument ----- & : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument	

2

EPO FORM 1503 03/82 (P04C03)



EINSCHLÄGIGE DOKUMENTE			
Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (IPC)
A	"ST24C04, ST25C04, ST24W04, ST25W04, 4kBit Serial I2C Bus EEPROM with user defined Block Write Protection" Februar 1999 (1999-02), ANNOUNCEMENT ST MICROELECTRONICS, PAGE(S) 1-16 , XP002206612 * das ganze Dokument *	4,5	
A	US 5 485 590 A (HYATT ET AL) 16. Januar 1996 (1996-01-16) * Zusammenfassung *	1-6	
			RECHERCHIERTE SACHGEBIETE (IPC)
Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt			
Recherchenort München		Abschlußdatum der Recherche 6. April 2006	Prüfer Jünger, B
KATEGORIE DER GENANNTEN DOKUMENTE X : von besonderer Bedeutung allein betrachtet Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie A : technologischer Hintergrund O : mündliche Offenbarung P : Zwischenliteratur		T : der Erfindung zugrunde liegende Theorien oder Grundsätze E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist D : in der Anmeldung angeführtes Dokument L : aus anderen Gründen angeführtes Dokument & : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument	

 2
EPO FORM 1503 03.82 (P04C03)

**ANHANG ZUM EUROPÄISCHEN RECHERCHENBERICHT
ÜBER DIE EUROPÄISCHE PATENTANMELDUNG NR.**

EP 05 11 0582

In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten europäischen Recherchenbericht angeführten Patentdokumente angegeben.
Die Angaben über die Familienmitglieder entsprechen dem Stand der Datei des Europäischen Patentamts am
Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

06-04-2006

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 5659705 A	19-08-1997	CN 1171852 A	28-01-1998
		DE 69510230 D1	15-07-1999
		DE 69510230 T2	04-11-1999
		EP 0800671 A1	15-10-1997
		ES 2136299 T3	16-11-1999
		WO 9621178 A1	11-07-1996

DE 4114921 A1	12-11-1992	KEINE	

DE 10040866 A1	07-03-2002	AT 295040 T	15-05-2005
		EP 1193949 A2	03-04-2002
		ES 2239113 T3	16-09-2005

US 5485590 A	16-01-1996	CA 2031951 A1	09-07-1991
		DE 4100198 A1	11-07-1991
		FR 2657441 A1	26-07-1991
		JP 2840463 B2	24-12-1998
		JP 4153705 A	27-05-1992

EPO FORM P0461

Für nähere Einzelheiten zu diesem Anhang : siehe Amtsblatt des Europäischen Patentamts, Nr.12/82