(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 702 827 A1

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
20.09.2006 Patentblatt 2006/38

(51) Int Cl.:
B61L 21/04 *(2006.01)*

(21) Anmeldenummer: **06111067.2**

(22) Anmeldetag: **14.03.2006**

(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

(30) Priorität: **16.03.2005 DE 102005013194**

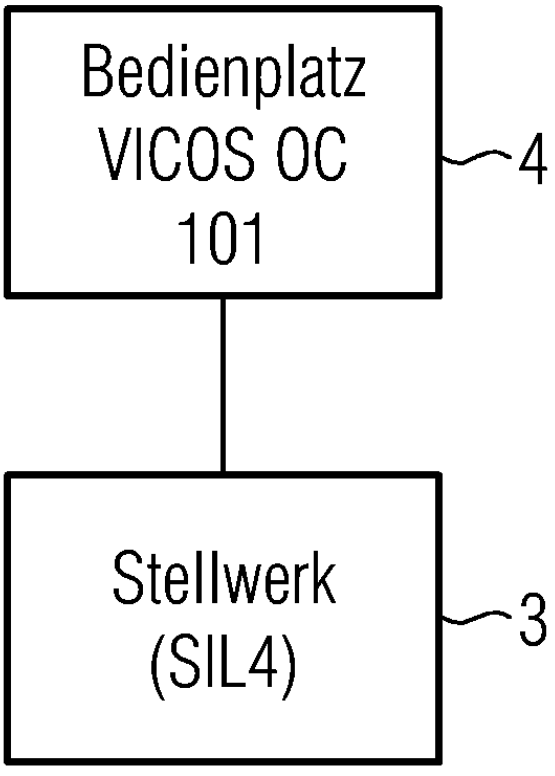
(71) Anmelder: **SIEMENS AKTIENGESELLSCHAFT**
80333 München (DE)

(72) Erfinder: **Grabe, Wolfgang**
38154 Königslutter (DE)

(54) Bedienplatzsystem

(57) Die Erfindung betrifft ein Bedienplatzsystem mit signaltechnisch sicherer Kommandoausgabe gemäß Sicherheitslevel CENELEC SIL4 und signaltechnisch nicht sicherer Kommandoanzeige für die Bedienung und Überwachung eines SIL4-Stellwerks (3). Ein derartiges Bedienplatzsystem mit nur einem Kanal ist möglich, wenn der Kanal mit einem Rechner (4) eines mehrere identische Rechner (1,2) aufweisenden, mehrkanaligen SIL4-Bedienplatzes sowohl hinsichtlich Hardware als auch hinsichtlich Software übereinstimmt.

FIG 2



EP 1 702 827 A1

Beschreibung

[0001] Die Erfindung betrifft ein Bedienplatzsystem gemäß dem Oberbegriff des Patentanspruchs. Bedienplatzsysteme in der Eisenbahnsignaltechnik müssen Sicherheitsanforderungen genügen, die in der CENELEC-Norm in Form von Sicherheitsstufen SIL0 - signaltechnisch nicht sicher - bis SIL4 - signaltechnisch hochgradig sicher - definiert sind. Besteht für die Kommandoausgabe eine Sicherheitsanforderung nach SIL4 und für die Kommandoanzeige keine Sicherheitsanforderung, d. h. SILO, werden bisher Bedienplatzsysteme eingesetzt, die insgesamt dem Sicherheitslevel SIL4 entsprechen. Das bedeutet nach der Normvorgabe, dass das Bedienplatzsystem zweikanalig auszuführen ist. Damit ist zwangsläufig ein hoher Hardware- und Softwareaufwand verbunden.

[0002] Der Erfindung liegt die Aufgabe zugrunde, ein Bedienplatzsystem der gattungsgemäßen Art anzugeben, das weniger aufwendig ist, insbesondere hinsichtlich Kommunikationsschaltungen, Projektierung und Installation.

[0003] Erfindungsgemäß wird die Aufgabe mit den kennzeichnenden Merkmalen des Patentanspruchs gelöst. Durch die Reduzierung auf nur einen Kanal ergibt sich ohne Sicherheitseinbuße eine erhebliche Einsparung. Durch den Wegfall des zweiten Kanals entfallen Kommunikationsschaltungen inklusive der zugehörigen Software. Projektierung und Installation werden bei verringertem Platzbedarf vereinfacht. Zusätzlich erhöht sich die Verfügbarkeit des Bedienplatzsystems um Faktor zwei. Statt mindestens zwei PCs wird nur noch ein PC zur Ausbildung des einzigen Kanals eingesetzt. Dieser PC muss identisch sein mit einem von mehreren PCs eines mehrkanaligen SIL4-Bedienplatzsystems sowohl hinsichtlich Hardware als auch hinsichtlich Software. Auf diese Weise gilt die SIL4-Zertifizierung unter den unten genannten Voraussetzungen auch für das Bedienplatzsystem gemäß der geforderten Sicherheit, nämlich Kommandoausgabe gemäß SIL4 und Kommandoanzeige signaltechnisch nicht sicher. Diese "gemischte" Sicherheitsanforderung ergibt sich aus der Überlegung, dass nicht eine falsche Anzeige bei korrekter Kommandoausgabe gefährlich ist, sondern ein verfälschtes Kommando, das trotzdem in der gewünschten Weise, d. h. als korrekt angezeigt wird. Folglich kann es sinnvoll sein, ein Bedienplatzsystem zu konzipieren, das nur bezüglich der Kommandoausgabe dem Sicherheitslevel SIL4 entspricht. Damit für diese Anforderung ein einkanaliges System eingesetzt werden kann, muss der entsprechende PC für die Kommandoausgabe SIL4-tauglich sein. Dazu müssen gemäß der Normvorgabe folgende vier Voraussetzungen erfüllt sein:

1. Die tolerierbare Gefährdungsrate pro Stunden und pro Funktion für SIL4 gemäß CENELEC EN 50129, Tabelle A-1 muss im Bereich von 10^{-9} und 10^{-8} liegen.
2. Die Software muss gemäß den Vorgaben von CENELEC EN 50128 entwickelt worden sein.
3. Die Projektierung, Projektierungsprüfung, Installation und Wartung müssen den Anforderungen von SIL4 gerecht werden.
4. Die Nutzung des Bedienplatzes muss den Anforderungen nach SIL4 entsprechen.

[0004] Der Nachweis dieser Anforderungen wird nachfolgend am Beispiel des VICOS-Systems näher erläutert. Es zeigen:

Figur 1 das Prinzip eines bekannten Bedienplatzsystems und
Figur 2 das beanspruchte Bedienplatzsystem.

[0005] Das bekannte Bedienplatzsystem, das die Anforderungen nach CENELEC SIL4 erfüllt, ist bisher als zweikanaliges System mit zwei VICOS OC 111-Rechnern 1 und 2 ausgebildet. Die beiden Rechner 1 und 2 dienen zur Ansteuerung und Überwachung eines Stellwerks 3, das ebenfalls der Sicherheitsstufe SIL4 entspricht.

[0006] Bei der in Figur 2 dargestellten beanspruchten Lösung ist nur noch ein VICOS OC 101- Rechner 4 vorgesehen. Dieser Bedienplatz ist für signaltechnisch sichere Ausgabe nach SIL4 und nicht signaltechnisch sicherer Anzeige ausgelegt. Bei der Verwendung des VICOS OC 101-Rechners 4 ist bisher davon ausgegangen worden, dass nur Sicherheitsanforderungen bis CENELEC SIL2 erfüllt werden können. Die nachfolgende Betrachtung bezüglich der oben genannten vier Voraussetzungen für die SIL4-Eignung führen jedoch überraschenderweise zu dem Ergebnis, dass die einkanalige Konfigurierung nach Figur 2 bezüglich der Kommandoausgabe den Sicherheitsanforderungen nach SIL4 genügt.

1. Für den zweikanaligen Bedienplatz OC 111 existiert eine Gefährdungsanalyse, wobei für die zwei Ausfälle alte Bedienfolge und Verfälschung von Bedienfolgen für die Kommandorichtung eine Gefährdungsrate von $1{,}9 \times 10^{-10}$ resultiert. Die Bedienplätze VICOS OC 111 und VICOS OC 101 unterscheiden sich darin, dass bei VICOS OS 111 für die Kommandofreigabe-Verfahren zwei hardwaremäßig unabhängige Rechner 1 und 2 und bei VICOS OC 101 nur ein Rechner 4 eingesetzt werden. Um die Gefährdungsrate, die sich für die Kommandorichtung beim Bedienplatz VICOS OC 101 ergibt, zu berechnen, muss zunächst betrachtet werden, welche Aufgabe der zweite Rechner 1 bzw. 2 im VICOS OC 111-System übernimmt.

Regelbedienungen, also nicht freigabepflichtige Bedienungen, werden bei VICOS OC 111 auch nur einkanalig ausgeführt. Bei freigabepflichtigen Bedienungen liefert der Referenz-Rechner 1 bzw. 2 die Checksumme seiner Anzeige zum Vergleich mit der Checksumme des Bedien-Rechners 2 bzw. 1 an das Stellwerk 3. Dort können Fehler in der Anzeige aufgedeckt werden.

Im vorliegenden Fall soll die Anzeige nicht SIL4 entsprechen. Gefährlich ist nicht, dass eine falsche Anzeige erscheint, gefährlich ist, dass das Kommando verfälscht wird und dann trotzdem die gewünschte Anzeige erscheint. Wird ein Ausfall des Bedienplatzes angenommen, infolge dessen immer Kommandos verfälscht würden, liegt die Wahrscheinlichkeit, dass die gewünschte Anzeige erscheint, bei $< 10^{-2}$. Da die Anzeige zwei voneinander unabhängige Verfahren, nämlich Elementausleuchtung und Telegrammtext, umfasst, ergibt sich eine Wahrscheinlichkeit von $< 10^{-4}$. Die Hardwarefehler, die zu einem Ausfall und damit letztlich zur Gefährdung führen können, betreffen die PC-Komponenten, die an dieser Funktion beteiligt sind. Unter Berücksichtigung dieser Komponenten, nämlich CPU, Hauptspeicher, Graphikkarte und Monitor, und den anfangs betrachteten Ausfällen "alte Bedienfolge" und "Verfälschung von Bedienfolgen" beträgt die Gesamtgefährdung $1{,}0 \times 10^{-9}$. Dieser Wert ist ausrechend für SIL4.

2. Für den OC 101-Rechner 4 wird die gleiche Software wie für den OC 111-Rechner 1 bzw. 2 eingesetzt. Damit ist diese Anforderung nach SIL4 gegeben.

3. Sofern alle vorgeschriebenen Maßnahmen für den OC 101-Rechner 4 durchgeführt werden, wird SIL4 erreicht.

4. Der Betrieb des Bedienplatzes OC 111 ist entsprechend SIL4 zugelassen. Es ist sicherzustellen, dass alle Maßnahmen, die für die Kommandoausgabe beim Bedienplatz OC 111 vorgesehen sind, auch beim Bedienplatz OC 101 projektiert werden.

[0007] Wenn die oben genannten Maßnahmen und Auflagen für den OC 101-Rechner 4 nachgewiesen werden, kann der OC 101-Rechner 4 folglich bei SIL4-Anforderungen bezüglich der Kommandoausgabe eingesetzt werden. Ein zweiter Kanal gemäß Figur 1 kann entfallen.

[0008] Die Erfindung beschränkt sich nicht auf das vorstehend genannte Ausführungsbeispiel. Vielmehr ist eine Anzahl von Varianten denkbar, welche auch bei grundsätzlich anders gearteter Ausführung von den Merkmalen der Erfindung Gebrauch machen.

Patentansprüche

1. Bedienplatzsystem mit signaltechnisch sicherer Kommandoausgabe gemäß Sicherheitslevel CENELEC SIL4 und signaltechnisch nicht sicherer Kommandoanzeige für die Bedienung und Überwachung eines SIL4-Stellwerks (3), **dadurch gekennzeichnet,**
dass das Bedienplatzsystem einkanalig ausgebildet ist, wobei der Kanal mit einem Rechner (4) eines mehrere identische Rechner (1,2) aufweisenden, mehrkanaligen SIL4-Bedienplatzsystems sowohl hinsichtlich Hardware als auch hinsichtlich Software übereinstimmt.

FIG 1
Stand der Technik

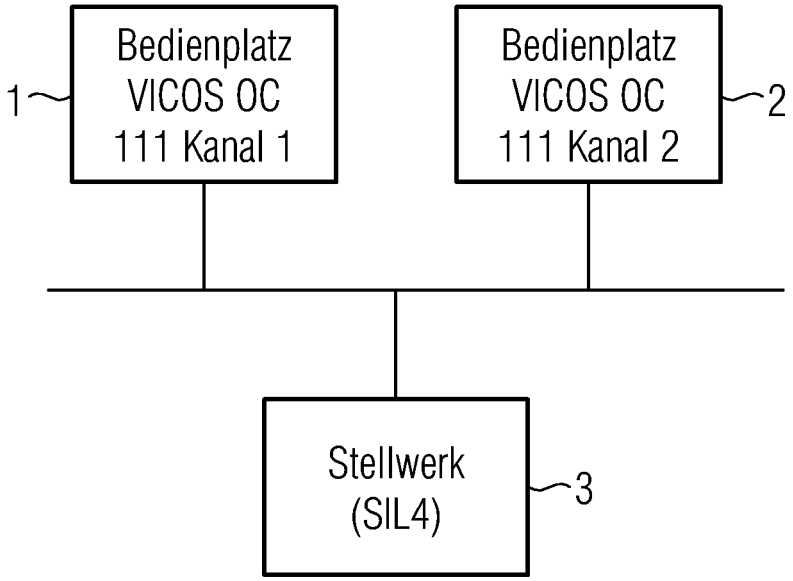
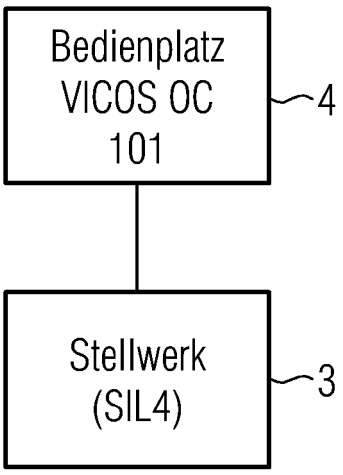


FIG 2



Europäisches Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 06 11 1067

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (IPC)
X	DE 33 23 269 A1 (SIEMENS AG) 10. Januar 1985 (1985-01-10) * Seite 3, Absatz 1 - Seite 10, Zeile 24; Abbildung 1 * -----	1	INV. B61L21/04
E	WO 2006/051355 A (ABB AS; ROEDSETH, NILS-PETTER) 18. Mai 2006 (2006-05-18) * Zusammenfassung * -----	1	
P,X	GB 2 414 327 A (* BALFOUR BEATTY PLC) 23. November 2005 (2005-11-23) * Zusammenfassung * -----	1	
A	EP 0 473 834 A (SIEMENS AKTIENGESELLSCHAFT) 11. März 1992 (1992-03-11) * Zusammenfassung * -----	1	
			RECHERCHIERTE SACHGEBIETE (IPC) B61L

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
München	20. Juni 2006	Janhsen, A

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 : nichtschriftliche 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

1

EPO FORM 1503 03.82 (P04C03)

ANHANG ZUM EUROPÄISCHEN RECHERCHENBERICHT ÜBER DIE EUROPÄISCHE PATENTANMELDUNG NR. EP 06 11 1067

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.

20-06-2006

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 3323269 A1	10-01-1985	DK 62884 A	29-12-1984
		EP 0132548 A1	13-02-1985
		US 4641243 A	03-02-1987
		ZA 8404896 A	27-03-1985
WO 2006051355 A	18-05-2006	KEINE	
GB 2414327 A	23-11-2005	WO 2005113315 A1	01-12-2005
EP 0473834 A	11-03-1992	DE 59006247 D1	28-07-1994

EPO FORM P0461

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