BUNDESPATENTGERICHT

20 W (pat) 54/13

_____

(Aktenzeichen)

Verkündet am
5. Oktober 2016
…

B E S C H L U S S

In der Beschwerdesache

…

…

betreffend das Patent 10 2009 042 354

hat der 20. Senat (Technischer Beschwerdesenat) des Bundespatentgerichts auf die mündliche Verhandlung vom 5. Oktober 2016 unter Mitwirkung des Richters Dipl.-Ing. Musiol als Vorsitzendem, der Richterin Dorn sowie der Richter Dipl.-Ing. Albertshofer und Dipl.-Phys. Bieringer

beschlossen:

Der Beschluss der Patentabteilung 31 des Deutschen Patent- und Markenamts vom 29. November 2012 wird aufgehoben und das Patent 10 2009 042 354 wie folgt aufrechterhalten:

Bezeichnung:
Verfahren und Vorrichtung zur sicherheitsgerichteten Kommunikation im Kommunikations-Netzwerk einer Automatisierungs-Anlage

Anmeldetag:
23.09.2009

Patentansprüche:
Patentansprüche 1 bis 5, dem BPatG als neuer Hauptantrag überreicht in der mündlichen Verhandlung am 05.10.2016

Beschreibung:
Beschreibung Abs. [0001] bis Abs. [0070], dem BPatG überreicht in der mündlichen Verhandlung am 05.10.2016

Zeichnungen:
Figuren wie Patentschrift.

G r ü n d e

I.

Das am 23. September 2009 beim Deutschen Patent- und Markenamt (DPMA) unter der Nr. 10 2009 042 354 angemeldete und am 10. Februar 2011 erteilte Patent mit der Bezeichnung „Verfahren und Vorrichtung zur sicherheitsgerichteten

Kommunikation im Kommunikations-Netzwerk einer Automatisierungs-Anlage“ wurde am 7. Juli 2011 veröffentlicht.

Gegen dieses Patent haben jeweils

1) die Einsprechende zu 1) am 6. Oktober 2011,

2) die Einsprechende zu 2) am 7. Oktober 2011 und

3) die Einsprechende zu 3) am 7. Oktober 2011

Einspruch eingelegt.

Die Patentabteilung 31 des DPMA hat das Patent daraufhin mit am Ende der mündlichen Anhörung am 29. November 2012 verkündetem Beschluss widerrufen. Zur Begründung hat sie ausgeführt, das Streitpatent sei weder in der mit Hauptantrag verteidigten Fassung noch in der hilfsweise beantragten Fassung patentfähig, da der Gegenstand des jeweiligen Patentanspruchs 1 nicht neu sei gegenüber dem Stand der Technik, wie er aus der DE 10 2007 050 708 A1 (D4) bekannt sei. Der begründete Beschluss wurde der Patentinhaberin am 31. Januar 2013 zugestellt.

Gegen diesen Beschluss richtet sich die am 25. Februar 2013 beim DPMA eingegangene Beschwerde der Patentinhaberin. Zur Begründung stützt sie sich im Wesentlichen darauf, dass der Gegenstand der unabhängigen Patentansprüche gegenüber dem aus der Druckschrift D4 bekannten Stand der Technik neu sei.

Die Bevollmächtigten der Patentinhaberin beantragen,

den Beschluss der Patentabteilung 31 des Deutschen Patent- und Markenamts vom 29. November 2012 aufzuheben und das Patent 10 2009 042 354 auf der Grundlage folgender Unterlagen aufrechtzuerhalten:

Patentansprüche:
Patentansprüche 1 bis 5, dem BPatG als neuer Hauptantrag überreicht in der mündlichen Verhandlung am 05.10.2016

Beschreibung:
Beschreibung Abs. [0001] bis Abs. [0070], dem BPatG überreicht in der mündlichen Verhandlung am 05.10.2016, mit der Maßgabe, dass in Abs. [0016] das Bzz. (3) hinter “Kommunikations-Master” gestrichen wird

Zeichnungen:
Figuren wie Patentschrift.

Die Bevollmächtigten der Einsprechenden zu 1), 2) und 3) beantragen übereinstimmend,

die Beschwerde zurückzuweisen.

Der mit Hauptantrag verteidigte geltende Patentanspruch 1 (Vorrichtungsanspruch) lautet mit eingefügten Gliederungszeichen:

M1.1 Automatisierungs-Anlage mit einem insbesondere nicht sicheren Kommunikations-Master (3) und mehreren dezentralen Modulen (70, 80-83, 90, 91),

M1.2 wobei die dezentralen Module (70, 80-83, 90, 91) als Netzwerkteilnehmer ausgebildet sind und mit dem Kommunikations-Master (3) mittels eines Kommunikationsnetzwerkes vernetzt sind,

M1.3 wobei die Kommunikation zwischen den dezentralen Modulen im Kommunikationsnetzwerk über Telegramme realisiert wird,

M1.4.1 wobei zumindest zwei der Module Sicherheitsmodule sind, zwischen denen sicherheitsgerichtete Daten übermittelt werden und

M1.4.2 die eine logische Gruppe von Modulen zur Ausführung einer sicherheitsgerichteten Funktion bilden,

$M1.4.3_{E/A}$ wobei von den Sicherheitsmodulen der logischen Gruppe mindestens ein Sicherheitsmodul ein Eingabemodul und mindestens ein Sicherheitsmodul ein Ausgabemodul umfasst,

M1.5 wobei der vorzugsweise nicht sichere Kommunikations-Master (3) eine Routing-Tabelle enthält, in welcher logische Verbindungen zwischen den dezentralen Sicherheitsmodulen entsprechend der sicherheitsgerichteten Funktion abgelegt sind,

$M1.6.1_{E/A}$ wobei der Kommunikations-Master dazu eingerichtet ist, gesteuert anhand der Routing-Tabelle ein automatisches Routing der Daten vom sendenden Eingabemodul zum empfangenden Ausgabemodul vorzunehmen,

$M1.6.2_{E/A}$ so dass eine Kommunikation zwischen den zu der logischen Gruppe gehörenden Sicherheitsmodulen jeweils über zwei Punkt-zu-Punkt Verbindungen, nämlich vom sendenden Eingabemodul zum Kommunikations-Master (3) und weiter vom Kommunikations-Master (3) zum empfangenden Ausgabemodul erfolgt,

$M1.7_{E/A}$ wobei das empfangende Ausgabemodul der logischen Gruppe dazu eingerichtet ist, unter Ansprechen auf ein Telegramm des Eingabemoduls, eine sicherheitsgerichtete Aktion entsprechend den empfangenen Daten auszuführen,

M1.8 wobei das Kommunikationsnetzwerk eine Einrichtung aufweist, um Informationen für das Erstellen der Routing-Tabelle von den Sicherheitsmodulen abzufragen und die Routing-Tabelle anhand dieser Informationen zu erstellen,

M1.9 wobei die Adressen der Sicherheitsmodule so konfiguriert sind, dass diese jeweils die Zugehörigkeit zu der logischen Gruppe reflektieren, und

M1.10 wobei der Kommunikations-Master (3) dazu eingerichtet ist, logische Gruppen jeweils bestimmten Adressräumen zuzuordnen.

Der mit Hauptantrag verteidigte nebengeordnete Patentanspruch 5 (Verfahrensanspruch) lautet mit eingefügten Gliederungszeichen:

M5.1 Verfahren zum Überwachen von Sicherheitsfunktionen in einer Automatisierungs-Anlage mit einem insbesondere nicht sicheren Kommunikations-Master (3) und mehreren dezentralen Modulen,

M5.2 wobei die dezentralen Module als Netzwerkteilnehmer ausgebildet sind und mit dem Kommunikations-Master mittels eines Kommunikationsnetzwerkes vernetzt sind,

M5.3 wobei die Kommunikation zwischen den dezentralen Modulen im Kommunikationsnetzwerk über Telegramme realisiert wird,

M5.4.1 wobei zumindest zwei der Module Sicherheitsmodule sind, zwischen denen sicherheitsgerichtete Daten übermittelt werden und

M5.4.2 die eine logische Gruppe von Modulen zur Ausführung einer sicherheitsgerichteten Funktion bilden,

$M5.4.3_{E/A}$ wobei von den Sicherheitsmodulen der logischen Gruppe mindestens ein Sicherheitsmodul ein Eingabemodul und mindestens ein Sicherheitsmodul ein Ausgabemodul umfasst,

M5.5 wobei der vorzugsweise nicht sichere Kommunikations-Master (3) eine Routing-Tabelle enthält, in welcher logische Verbindungen zwischen den dezentralen Sicherheitsmodulen entsprechend der sicherheitsgerichteten Funktion abgelegt sind,

$M5.6.1_{E/A}$ wobei der Kommunikations-Master anhand der Routing-Tabelle ein automatisches Routing der Daten vom sendenden Eingabemodul zum empfangenden Ausgabemodul vornimmt,

$M5.6.2_{E/A}$ so dass eine Kommunikation zwischen den zu einer logischen Gruppe gehörenden Sicherheitsmodulen jeweils über zwei Punkt-zu-Punkt Verbindungen, nämlich vom sendenden Einga-

bemodul zum Kommunikations-Master (3) und weiter vom Kommunikations-Master (3) zum empfangenden Ausgabemodul durchgeführt wird,

M5.7$_{E/A}$ wobei vom empfangenden Ausgabemodul der logischen Gruppe unter Ansprechen auf ein Telegramm des Eingabemoduls eine sicherheitsgerichtete Aktion entsprechend den empfangenen Daten ausgeführt wird, und

M5.8 wobei von einer Einrichtung des Kommunikationsnetzwerkes, vorzugsweise vom Kommunikations-Master, Informationen für das Erstellen der Routing-Tabelle von den Sicherheitsmodulen abgefragt werden und die Routing-Tabelle anhand dieser Information erstellt wird,

M5.9 wobei die Adressen der Sicherheitsmodule so konfiguriert werden, dass diese jeweils die Zugehörigkeit zu einer logischen Gruppe reflektieren, und

M5.10 wobei der Kommunikations-Master (3) logische Gruppen jeweils bestimmten Adressräumen zuordnet.

Wegen weiterer Einzelheiten und des Wortlauts der Unteransprüche wird auf die Akte verwiesen.

II.

Die zulässige Beschwerde der Patentinhaberin ist begründet mit der Folge, dass der angefochtene Beschluss aufgehoben und das Patent gemäß dem neuen Hauptantrag beschränkt aufrechterhalten wird.

1. Das Streitpatent betrifft allgemein Automatisierungs-Anlagen und deren Automatisierungs-Bussysteme. lm Speziellen betrifft der Gegenstand des Streitpatents die Kommunikation zwischen sicherheitsgerichteten Modulen im Kommunikations-Netzwerk einer solchen Automatisierungs-Anlage (Streitpatentschrift,

DE 10 2009 042 354 B4, Abs. [0001]). Häufig sei es erforderlich, Sicherheitsfunktionen in Automatisierungsanlagen vorzusehen, wobei hinsichtlich der Anforderungen auf die IEC 61508 und ISO 13489 verwiesen werde (Abs. [0002]). ln der Automatisierungstechnik ließen sich zwei Tendenzen erkennen: Zum einen existierten Bestrebungen, die Steuerungsfunktionen zu dezentralisieren. Weiterhin bestünde Interesse an der lntegration der Sicherheitstechnik in die Steuerungs- und Netzwerktechnik. Die zunehmende Integration der Sicherheitstechnik in Steuerungen und Netzwerke erzeuge starke Abhängigkeiten im Applikationsprozess und führe zu einer komplexen Projektierung (Abs. [0005] bis [0007]).

Somit liege die Aufgabe zugrunde, die Installation und Projektierung sicherheitsgerichteter Module in einem Automatisierungs-Netzwerk zu vereinfachen (Abs. [0008]).

Diese Aufgabe werde mit der grundlegenden Idee gelöst, die Sicherheitsfunktion einer Automatisierunganlage in Gruppen von Modulen aufzuteilen, die mehr oder weniger autarke Inseln innerhalb des gesamten Kommunikations-Netzwerks darstellten (Abs. [0009]). Damit werde auch eine Trennung der Sicherheitsfunktion von Standard-Funktionen vorgenommen (Abs. [0010]).

Die Figur 1 der Streitpatentschrift zeigt zwei logische Gruppen von Sicherheitsmodulen. Die erste Gruppe wird gebildet aus den mit 80, 82, 81 und 83 bezeichneten Modulen (diesseits schattiert) und die zweite Gruppe wird gebildet aus den mit 90 und 91 bezeichneten Modulen. Der Kommunikations-Master 3 enthält eine Routing-Tabelle, in der die logischen Gruppen durch Verbindungen und Adressen abgebildet sind, so dass nur Module innerhalb einer logischen Gruppe einen sicherheitskritischen Prozess steuern. Ein Routing zwischen Modulen verschiedener Gruppen findet nicht statt.

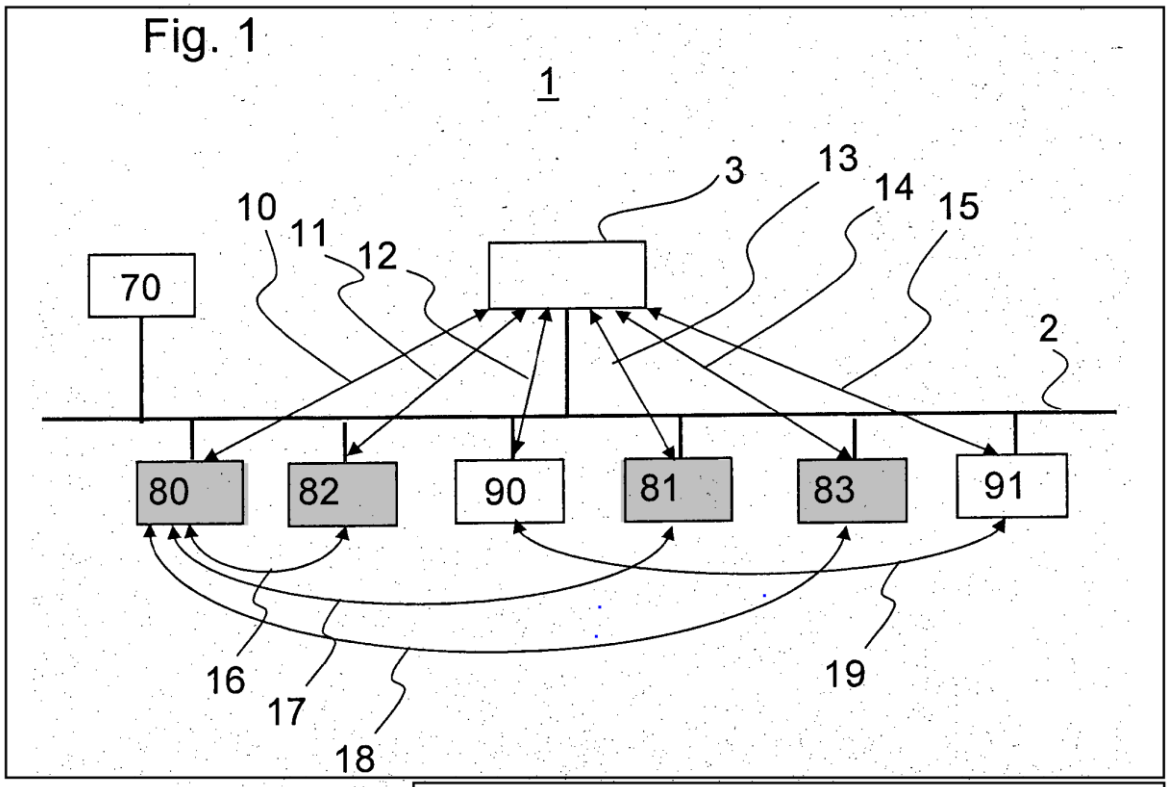

Fig. 1 der Streitpatentschrift, Schattierungen diesseits eingefügt

2. Als Fachmann ist ein Entwicklungsingenieur der Fachrichtung Elektrotechnik mit einem Hochschulabschluss (Univ.) und mehrjähriger Erfahrung in der Entwicklung von Kommunikationssystemen in der Automatisierungstechnik anzusehen. Er hat profunde Kenntnisse über Anforderungen und Prüfvorschriften für sicherheitsrelevante Anwendungen in Automatisierungssystemen.

3. Zum Verständnis der Patentansprüche:

Der Gegenstand des Patentanspruchs 1 betrifft eine Automatisierungsanlage, wobei die Kommunikation über ein Netzwerk von einem Eingabemodul zu einem Ausgabemodul ohne Zwischenschaltung weiterer Verbindungen als der beiden Punkt-zu-Punkt-Verbindungen vom Eingabemodul zum Kommunikations-Master und vom Kommunikations-Master zum Ausgabemodul erfolgt (M1.1; M1.2; Merkmalsgruppe M1.6). Der Fachmann versteht, dass ein steuernder Sicherheitsserver nicht erforderlich ist und ein Telegramm (M1.3; $M1.7_{E/A}$) vom Eingabemodul mittels

der Routing-Tabelle im Kommunikations-Master an das (oder mehrere) Ausgabemodul(e) geleitet wird. Die Steuerlogik wird daher durch die Verbindungslisten im Kommunikations-Master abgebildet (vgl. auch Streitpatent, Abs. [0061] und [0062]). Sie erlaubt, dass auf ein oder mehrere Ereignisse an einem Eingabemodul ein oder mehrere Aktionen an einem oder mehreren Ausgabemodulen derselben logischen Gruppe ausgeführt werden (sicherheitsgerichtete Funktion).

Eine *„logische Gruppe“* im Sinne des Streitpatents weist dabei folgende Eigenschaften auf:

- die logische Gruppe besteht aus zwei oder mehr dezentralen Sicherheitsmodulen (M1.4.1),
- die logische Gruppe dient der Ausführung einer sicherheitsgerichteten Funktion (M1.4.2),
- die logische Gruppe enthält zumindest ein Eingabemodul und ein Ausgabemodul ($M1.4.3_{E/A}$),
- die Sicherheitsmodule einer logischen Gruppe sind durch logische Verbindungen verknüpft (M1.5),
- es kann mehrere logische Gruppen geben (Fig. 1 i. V. m. Abs. [0033]),
- die Zugehörigkeit eines Sicherheitsmoduls zu einer logischen Gruppe wird durch seine Adresse reflektiert (M1.9).

An das Kommunikationsnetzwerk (M1.2) ist eine Einrichtung zum Erstellen der Routing-Tabelle angeschlossen (M1.8), welche von den Sicherheitsmodulen (zumindest Eingabemodul und Ausgabemodul) bereitgestellte Informationen (z. B. Adressen, vgl. Streitpatent, Abs. [0055]) verwendet. Der Fachmann versteht die Merkmale M1.9 und M1.10 unter Berücksichtigung der Beschreibung dahingehend, dass die Adress-Information der Sicherheitsmodule auszuwerten ist und die logischen Gruppen durch den Kommunikations-Master bestimmten Adressräumen zugeordnet werden.

Der Fachmann entnimmt den Absätzen [0054] und [0055], wie die richtige Zuordnung der Sicherheitsmodule zu einer logischen Gruppe ausgeführt werden kann: Der Kommunikations-Master ist dazu eingerichtet, von den Sicherheitsmodulen eine Information abzufragen und diese Information zu nutzen, um festzustellen, welche Sicherheitsmodule zu einer logischen Gruppe gehören (und damit dann entsprechende Verbindungen in der Routing-Tabelle vorzunehmen). Damit die logischen Gruppen der Sicherheitsmodule mit den durch den Master zugeordneten logischen Gruppen korrespondieren, werden die Adressen an den Sicherheitsmodulen konfiguriert. Dabei sind die Adressen der Sicherheitsmodule einer logischen Gruppe so zu konfigurieren, dass sie innerhalb eines bestimmten Adressraumes liegen, den der Kommunikations-Master dieser logischen Gruppe zuordnet. Analog gilt dies für weitere logische Gruppen (vgl. M1.10: „Adressräumen“, Plural).

4. Die Gegenstände der nunmehr geltenden Patentansprüche sind mit den ursprünglich eingereichten Unterlagen offenbart (§ 21 Abs. 1 Nr. 4 PatG). Sie beschränken auch die erteilte Fassung des Streitpatents. Die Merkmale der Ansprüche 1 und 5 entsprechen den folgenden ursprünglich eingereichten Unterlagen:

Merkmal M1.1, M1.2, M1.3	Anspruch 1
Merkmal M1.4.1, M1.4.2	Anspruch 1
Merkmal $M1.4.3_{E/A}$	Anspruch 8, Seite 20, Zeilen 5 bis 10
Merkmal M1.5	Anspruch 1
Merkmal $M1.6.1_{E/A}$, $M1.6.2_{E/A}$	Anspruch 1 und Anspruch 8
Merkmal $M1.7_{E/A}$	Anspruch 8, Seite 20, Zeilen 10 bis 15
Merkmal M1.8	Anspruch 1
Merkmal M1.9, M1.10	Seite 19, Zeilen 5 bis 18

Soweit der Bevollmächtigte der Einsprechenden zu 1) vorgetragen hat, Absatz [0055] der Streitpatentschrift (wortgleich mit der ursprünglich am Anmeldetag eingereichten Beschreibung, Seite 19, Zeilen 5 bis 18) lehre die Merkmale M1.9 und

M1.10 nur als alternative Möglichkeiten, kann der Senat dies aus der Streitpatentschrift bzw. aus der ursprünglichen Beschreibung nicht entnehmen. Denn jedes der beiden Merkmale für sich allein – ohne Hinzunahme des jeweils anderen in Rede stehenden Merkmals – könnte die mit Absatz [0054] geforderte Zuordnung nicht vornehmen: Das Konfigurieren von Adressen an den Sicherheitsmodulen einer logischen Gruppe kann steuerungstechnisch nicht wirksam werden, wenn dem Kommunikations-Master nicht bekannt ist, welche Adressen zu einer logischen Gruppe gehören. Andererseits kann das Zuordnen eines bestimmten Adressraumes zu einer logischen Gruppe durch den Kommunikations-Master steuerungstechnisch nicht wirken, wenn die Adressen der Sicherheitsmodule die Zugehörigkeit zu einer logischen Gruppe nicht reflektieren (d. h. nicht entsprechend konfiguriert sind) und/oder außerhalb des Adressraumes liegen.

Die mit Hauptantrag beanspruchten Merkmale M1.9 und M1.10 sind daher sowohl ursprünglich offenbart als auch innerhalb des Schutzbereichs des erteilten Patents. Gleiches gilt für die Merkmale M5.9 und M5.10 des nebengeordneten Patentanspruchs 5.

Soweit der Bevollmächtigte der Einsprechenden zu 1) vorgetragen hat, dass hinsichtlich des Begriffs „Daten“ im Merkmal $M1.7_{E/A}$ eine unzulässige Erweiterung gegenüber dem ursprünglich verwendeten Begriff „Telegramm“ vorliegen würde, ist dem Fachmann nach Überzeugung des Senats klar, dass die hier in Rede stehenden Daten von dem Telegramm (oder Teilen desselben) gebildet werden.

5. Die Gegenstände der geltenden nebengeordneten Patentansprüche 1 und 5 sind neu (§ 3 PatG) und beruhen auf einer erfinderischen Tätigkeit (§ 4 PatG).

Zu den Druckschriften

D4 DE 10 2007 050 708 A1,

D17 Beckhoff Automation GmbH: "TwinCAT/TwinSAFE-Schulung". Präsentation der Firma Beckhoff Automation GmbH. 33415 Verl, 15.09.2006 in Gütersloh, Foliensatz "BECKHOFF New Automation Technology", S. 1-56, Firmenschrift, und

D19 „TwinSAFE: Sicherheits- und I/O-Technik in einem System“. In: Beckhoff Automation GmbH: BECKHOFF New Automation Technology: Neuheiten und Ergänzungen - NEWS. 04|2005. 33415 Verl, 2005. Titelseite/Deckblatt S. 1, S.38-43, Firmenschrift

wurde in der mündlichen Verhandlung vorgetragen.

a) Die technische Lehre der Druckschrift D4 betrifft die Auftrennung eines Gesamtprozesses innerhalb einer Automatisierungsanlage in einen sicherheitsgerichteten und einen nicht-sicherheitsgerichteten – auch als Standard-Applikationsprozess bezeichneten – Prozess (Abs. [0022]). Die Vorrichtung gemäß der Druckschrift D4 betrifft ein Netzwerk mit Netzwerkmaster und mehreren dezentralen Modulen (Abs. [0023] u. [0024]: angeschlossene E/A-Geräte), von denen einige sicherheitsgerichtete E/A-Module (m. d. W. des Streitpatents: Sicherheitsmodule) sind (vgl. Abs. [0026] unten: *„sichere E/A Geräte*“ (Plural); vgl. Abs. [0028]: mehrere Punkt-zu-Punkt-Verbindungen zwischen Sicherheitsserver und sicheren E/A-Modulen). Zusätzlich ist ein Sicherheitsserver mit dem Netzwerk verbunden, der den sicherheitskritischen Applikationsprozess steuert, dessen Daten verarbeitet und die Übertragung der Daten über den Netzwerkmaster organisiert (vgl. Abs. [0024]). Da der Netzwerkmaster den Standard-Applikationsprozess verwaltet, der den wesentlichen Anteil am Gesamtprozess einnimmt, wird er als führender Master eingesetzt (Abs. [0023]). So kommt dem Sicherheitsserver die Rolle eines Kommunikationsslaves zu (wie anderen Modulen auch) (vgl. Abs. [0036] und [0037]). Innerhalb des sicherheitsgerichteten Applikationsprozesses hat die si-

cherheitsbezogene Servereinrichtung jedoch eine steuernde Rolle, ihr sind daher alle Informationen (auch Adressen) zu den sicherheitsrelevanten Netzwerkelementen bekannt (vgl. Abs. [0043], letzter Satz). Sie werden ihr von einem *„Safety-Agent“*, der diese Informationen in einem Initialisierungsprozess ermittelt, übertragen (vgl. Abs. [0041] i. V. m. Fig. 2). Alternativ können die Informationen auch direkt in den Sicherheitsserver projektiert werden, falls die Adressen der Netzteilnehmer bekannt sind (vgl. Abs. [0044]). Die sicherheitsgerichtete Servereinrichtung nimmt hinsichtlich der sicherheitsgerichteten Applikation die Rolle eines Sicherheitsmasters (vgl. Abs. [0028], letzter Satz) und hinsichtlich der Netzwerkkommunikation die Rolle eines Kommunikationsslaves ein (vgl. Abs. [0036], [0037]; Fig. 1).

In beiden Ausführungsbeispielen der Druckschrift D4 laufen die logischen Verbindungen (Punkt-zu-Punkt-Verbindungen) der sicherheitsgerichteten Applikation zwischen sicherheitsgerichteter Servereinrichtung und den E/A-Geräten. Es sind keine Punkt-zu-Punkt-Verbindungen der sicherheitsrelevanten E/A-Module untereinander offenbart, vielmehr ist der sicherheitsgerichtete Server an jeder sicherheitsgerichteten Kommunikation beteiligt (vgl. Fig. 2: SS1 zwischen Server und Gerät 1 Eingang; SS2a zwischen Server und Gerät 2 Eingang bzw. SS2b zwischen Server und Gerät 2 Ausgang; vgl. Fig. 1: „*SK“* zwischen Server und SDI). Eine Liste dieser Punkt-zu-Punkt-Verbindungen wird vom „Safety-Agent“ ermittelt und befindet sich insofern auch im Netzwerkmaster, soweit der „Safety-Agent“ in den Netzwerkmaster integriert ist. Es handelt sich um die Adressen (und andere Informationen) aller sicherheitsrelevanten Netzwerkteilnehmer.

Gemäß der Druckschrift D4 erfolgt jede Kommunikation zwischen dem Sicherheitsserver und einem sicherheitsgerichteten E/A-Modul über zwei Punkt-zu-Punkt-Verbindungen via Netzwerkmaster, nämlich eine zwischen Sicherheitsserver und Netzwerkmaster und eine zwischen Netzwerkmaster und dem sicherheitsgerichteten E/A-Modul (vgl. Fig. 1).

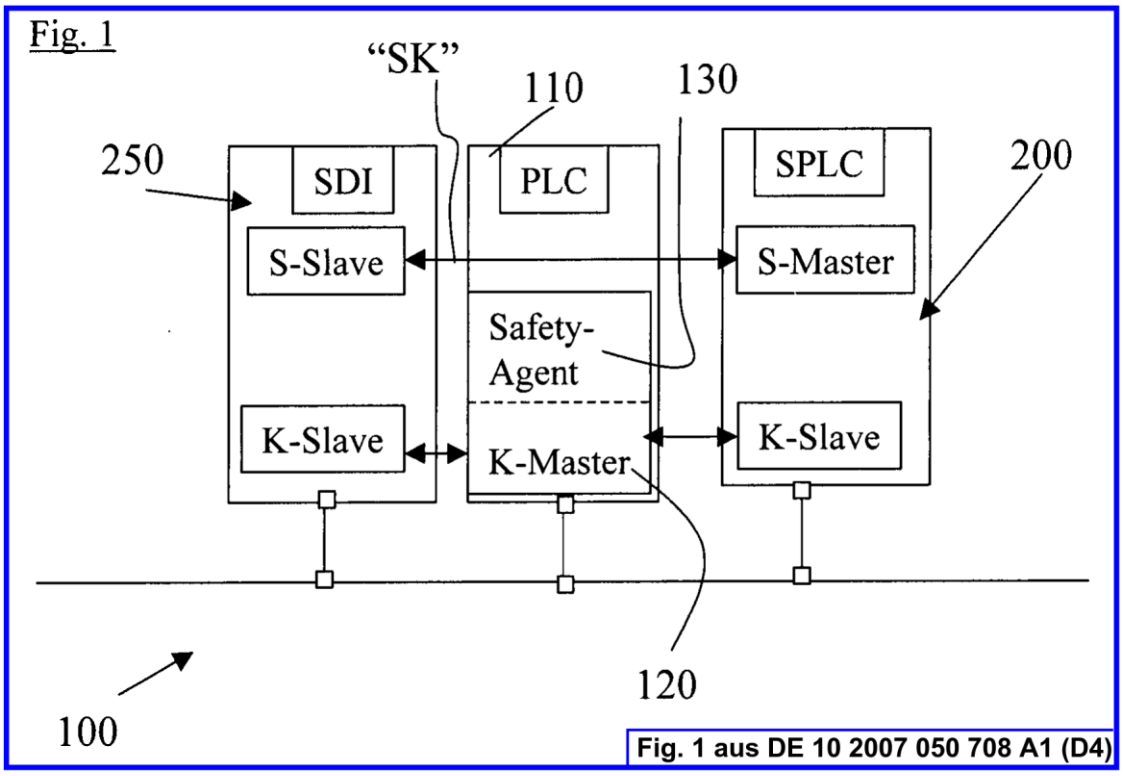

Fig. 1 aus DE 10 2007 050 708 A1 (D4)

Eine Punkt-zu-Punkt-Verbindung zwischen zwei E/A-Modulen ohne Umweg über den Sicherheitsserver ist der Druckschrift D4 nicht zu entnehmen.

Mit den Worten des geltenden Patentanspruchs 1 weist der Gegenstand der Druckschrift D4 im Einzelnen folgende Merkmale auf (nicht erfüllte Merkmale sind als durchgestrichen markiert):

M1.1 Automatisierungs-Anlage (D4, Abs. [0008]; [0009]) mit einem insbesondere nicht sicheren Kommunikations-Master (D4, Abs. [0023]; D4, Fig. 1 i. V. m. Abs. [0032]: *„Die Steuereinheit 110 ist zum Steuern eines nicht-sicheren bzw. Standard-Applikations-prozesses angepasst und beinhaltet einen Netzwerk-Master 120“*) und mehreren dezentralen Modulen (D4 zeigt zwei dezentrale Module: Fig. 1, Bz. 200 und 250; Abs. [0035]: *„Dargestellt sind zwei an den Netzwerk angeschlossene sicherheitsbezogene Ein-richtungen“*; Abs. [0033]: Es gibt noch weitere, in Fig. 1 nicht dargestellte Module),

M1.2 wobei die dezentralen Module als Netzwerkteilnehmer ausgebildet sind und mit dem Kommunikations-Master mittels eines Kommunikationsnetzwerkes vernetzt sind (D4, [0032]: *„Der bei Fig. 1 auch als K-Master bezeichnete Netzwerk-Master 120, gewährleistet also grundsätzlich die Kommunikation zwischen den einzelnen Netzwerkteilnehmern 110, 200, 250 im Netzwerk.“*),

M1.3 wobei die Kommunikation zwischen den dezentralen Modulen im Kommunikationsnetzwerk über Telegramme realisiert wird (D4, [0052]: *„Telegrammverlust, -vertausch, -Verzögerung“;* [0049]: Ethernet, Feldbusse),

M1.4.1 wobei zumindest zwei der Module Sicherheitsmodule sind, zwischen denen sicherheitsgerichtete Daten übermittelt werden (beide in Fig. 1 dargestellten Module 200 und 250 sind Sicherheitsmodule, vgl. Abs. [0035]: *„zwei an den Netzwerk angeschlossene sicherheitsbezogene Einrichtungen, zum einen eine separate Sicherheitssteuerung 200 […] zum anderen […] eine sicherheitsbezogene Dateneingangseinheit 250“;* zwischen ihnen werden Daten übermittelt: „*SK*“ in Fig. 1) und

M1.4.2 die eine logische Gruppe von Modulen (D4, [0026]: *„[…] eine Zuordnung der am Netzwerk angeschlossen Netzwerkelemente vorgenommen […]“*) zur Ausführung einer sicherheitsgerichteten Funktion (ebenda: *„die für die Steuerung des sicherheitskritischen Applikationsprozesses relevant sind.“* i. V. m. [0032], wonach die beiden Module 200 und 250 zugeordnet werden und eine überlagerte Sicherheitskommunikation *„SK“* ausführen) bilden,

$M1.4.3_{E/A}$ wobei von den Sicherheitsmodulen der logischen Gruppe mindestens ein Sicherheitsmodul ein Eingabemodul und mindestens ein Sicherheitsmodul ein Ausgabemodul umfasst (gemäß D4 ist zwar auch ein Ausgabemodul anschließbar, jedoch ist dies weder das mit Bezugszeichen 200, noch das mit Bezugszeichen 250 bezeichnete Modul, sondern ein drittes nicht in der Figur 1 dargestelltes Modul, vgl. D4, Abs. [0035]),

M1.5 wobei der vorzugsweise nicht sichere Kommunikations-Master eine Routing-Tabelle enthält, in welcher logische Verbindungen zwischen den dezentralen Sicherheitsmodulen entsprechend der

sicherheitsgerichteten Funktion abgelegt sind (D4, Abs. [0026]: „*an das Netzwerk angeschlossene Zuordnungseinrichtung, welche auch in der Mastereinrichtung integriert sein kann, und nachfolgend auch als "Safety-Agent" bezeichnet wird.*“; D4, Abs. [0028]: der Safety-Agent erzeugt Verbindunglisten; D4, Abs. [0027]: „*für den sicherheitskritischen Prozess notwendigen, angeschlossenen sicheren und nicht-sicheren Netzwerkelemente und deren notwendigen Kommunikationsbeziehungen untereinander*“),

M1.6.1$_{E/A}$ wobei der Kommunikations-Master dazu eingerichtet ist, gesteuert anhand der Routing-Tabelle ein automatisches Routing der Daten vom sendenden Eingabemodul zum empfangenden Ausgabemodul vorzunehmen (D4, Fig. 1, die Adressen sind im Safety-Agent gespeichert, der in den Netzwerkmaster integriert ist; Abs. [0028]: *„woraufhin die Mastereinrichtung das Netzwerk in einer Art und Weise betreibt, dass auf Basis der Standard-Kommunikation eine übergelagerte Sicherheits-Kommunikation zwischen sicherheitsbezogenen Netzwerk-Teilnehmern ermöglicht wird*“),

~~M1.6.2$_{E/A}$~~ so dass eine Kommunikation zwischen den zu der logischen Gruppe gehörenden Sicherheitsmodulen jeweils über zwei Punkt-zu-Punkt Verbindungen, ~~nämlich vom sendenden Eingabemodul zum Kommunikations-Master und weiter vom Kommunikations-Master zum empfangenden Ausgabemodul~~ erfolgt (gemäß D4 erfolgt die Kommunikation vom Eingabemodul 250 über den Master 120 zur separaten Sicherheitssteuerung 200 über zwei Punkt-zu-Punkt-Verbindungen; zum Ansprechen eines Ausgangsmoduls erfordert D4 zwei weitere Verbindungen von der separaten Sicherheitssteuerung 200 über den Server zu einem - in Fig. 1 nicht dargestellten - Ausgabemodul),

~~M1.7$_{E/A}$~~ ~~wobei das empfangende Ausgabemodul der logischen Gruppe dazu eingerichtet ist, unter Ansprechen auf ein Telegramm des Eingabemoduls, eine sicherheitsgerichtete Aktion entsprechend den empfangenen Daten auszuführen~~ (gemäß D4 erfolgt die sicherheitsgerichtete Kommunikation über die separate Sicherheitssteuerung 200; zur Weiterleitung von Telegrammen verhält sich die D4 nicht),

M1.8 wobei das Kommunikationsnetzwerk eine Einrichtung aufweist, um Informationen für das Erstellen der Routing-Tabelle von den Sicherheitsmodulen abzufragen und die Routing-Tabelle anhand dieser Informationen zu erstellen (entspricht dem *„Safety-Agent“* der D4, Abs. [0028]: *„[…] durch Erzeugung entsprechender Verbindungslisten […]“;* Abs. [0041]),

~~M1.9 wobei die Adressen der Sicherheitsmodule so konfiguriert sind, dass diese jeweils die Zugehörigkeit zu der logischen Gruppe reflektieren, und~~

~~M1.10 wobei der Kommunikations-Master dazu eingerichtet ist, logische Gruppen jeweils bestimmten Adressräumen zuzuordnen~~.

Der Lehre gemäß Druckschrift D4 fehlen das Merkmal $M1.6.2_{E/A}$ teilweise, die Merkmale $M1.7_{E/A}$, M1.9 und M1.10 gänzlich. Der Gegenstand des geltenden Patentanspruchs 1 gilt somit als neu gegenüber dem Stand der Technik nach der Druckschrift D4.

Soweit der Bevollmächtigte der Einsprechenden zu 1) vorgetragen hat, das in Fig. 2 der Druckschrift D4 gezeigte Gerät 2 weise einen Eingang und einen Ausgang auf, die zusammen eine logische Gruppe bilden würden, da sie einen gemeinsamen Adressraum hätten (vgl. Web-Adressen in Fig. 2), lässt sich dies nicht mit der technischen Lehre der Druckschrift D4 vereinbaren. Denn gemäß der Druckschrift D4 erfolgt eine Kommunikation vom Eingang des Geräts 2 zum Ausgang des Geräts 2 über den separaten Safety-Server 201 (vgl. D4, Fig. 2), wobei der Fachmann aus der Druckschrift D4 entnimmt, dass der Netzwerk-Master für die ordnungsmäße Kommunikation jeweils zwischengeschaltet ist. Soweit der Bevollmächtigte der Einsprechenden zu 1) vorgetragen hat, der Signalpfad gemäß der Druckschrift D4 verlaufe folgendermaßen: Eingang 252 → Internet (~Netzwerkmaster) → Safety-Server → Internet (~Netzwerkmaster) → Ausgang, schließt sich der Senat dieser Auffassung an. Nach Überzeugung des Senats

verläuft der korrespondierende Signalpfad gemäß Patentanspruch 1 im Gegensatz dazu aber anders: Eingang → Kommunikations-Master → Ausgang.

Der geltende Patentanspruch 1 gilt auch als neu gegenüber den weiteren im Prüfungsverfahren und im Einspruchsverfahren benannten Entgegenhaltungen nach den Druckschriften D1 bis D3 und D5 bis D23, da zumindest die Merkmale M1.9 und M1.10 von keinem dieser Dokumente offenbart werden. Im Übrigen haben die Einsprechenden zu 1) bis 3) zur Frage der Neuheit des geltenden Patentanspruchs 1 gegenüber den vorgenannten weiteren Entgegenhaltungen weder schriftsätzlich noch mündlich vorgetragen.

b) Der Gegenstand des geltenden Patentanspruchs 1 beruht auch auf einer erfinderischen Tätigkeit.
Als nächstliegenden Stand der Technik sieht der Senat die Druckschrift D4 an. Aus dieser Druckschrift ist eine Automatisierungsanlage bekannt, bei der die sicherheitsgerichteten Applikationen von den Standard-Applikationen getrennt sind, insbesondere eine separate Sicherheitssteuerung für die Steuerung sicherheitsrelevanter Funktionen vorgesehen ist. Um zum Gegenstand des Patentanspruchs 1 zu gelangen, hätte der Fachmann erstens die Struktur der in der Druckschrift D4 gelehrten Automatisierungsanlage grundliegend verändern sowie zweitens den Adressräumen logische Gruppen und damit auch das Ausführen sicherheitsgerichteter Funktionen zuordnen müssen.
Bereits für die erste Maßnahme gab weder die Druckschrift D4 noch ein anderer druckschriftlich genannter Stand der Technik eine Veranlassung. Der Fachmann hätte die der zentralen Servereinrichtung obliegenden Steuerfunktionen in die dezentralen Steuermodule und die Routing-Tabelle des Kommunikations-Masters übertragen müssen. Damit wäre ein grundliegender Umbau der gemäß Druckschrift D4 gelehrten Systemarchitektur verbunden gewesen, was der Fachmann zur Überzeugung des Senats vermieden hätte. Auch für die zweite Maßnahme hatte der Fachmann ausgehend von der technischen Lehre der Druckschrift D4 keine Veranlassung. Denn gemäß dieser Lehre ist es nicht erforderlich, mit

Adressräumen korrespondierende logische Gruppen zu bilden, da der Sicherheitsserver der Druckschrift D4 die zentrale Steuerungsaufgabe (Sicherheitsmaster) übernimmt und grundsätzlich sicherheitsgerichtete Verbindungen mit dezentralen Sicherheitsmodulen (via Kommunikations-Master 3) aufbauen kann. Allein die in der sicherheitsgerichteten Servereinrichtung gespeicherte Steuerlogik legt die auszuführende sicherheitsgerichtete Funktion fest. Dass der Fachmann bei der Systemarchitektur gemäß der Druckschrift D4 die Funktionalität des Sicherheitsservers ungenutzt gelassen und stattdessen entsprechend den Merkmalen M1.9 und M1.10 festgelegte logische Gruppen zur Ausführung sicherheitsgerichteter Funktionen in der Routing-Tabelle des Kommunikations-Masters vorgesehen hätte, sieht der Senat als abwegig an.

Soweit die Bevollmächtigten der Einsprechenden vorgetragen haben, die sicherheitsbezogene Servereinrichtung 200 der Druckschrift D4 weise auch ein (integriertes) Ausgabemodul auf und der Fachmann würde ihr entnehmen, dass eine Punkt-zu-Punkt-Verbindung zwischen diesem Ausgangsmodul (als integraler Bestandteil der separaten sicherheitsbezogenen Servereinrichtung 200) und dem Kommunikations-Master sowie eine weitere Punkt-zu-Punkt-Verbindung zwischen dem Kommunikations-Master und der sicherheitsbezogenen Dateneingabeeinheit 250 bestehe, vermag diese Argumentation nicht durchzugreifen. Denn die Druckschrift D4 zeigt weder explizit ein Ausgangsmodul als Teil der Servereinrichtung, noch entnimmt der Fachmann ihr einen Hinweis darauf, dass ein Ausgangsmodul in der Servereinrichtung enthalten sein könnte. Vielmehr offenbart Fig. 2 in Verbindung mit Absatz [0045], dass Ausgänge an den Geräten 1 und 2 angeordnet sein sollen.

Soweit der Bevollmächtigte der Einsprechenden zu 3) vorgetragen hat, der Fachmann würde an die Steuereinheit gemäß der Druckschrift D4 einen Ausgang anschließen, und dazu auf die Baugruppe KL6904 gemäß Druckschrift D17, Folien 9, 10, 13 und 53, und gemäß Druckschrift D19 verwiesen hat, teilt der Senat zwar die Auffassung, dass die in den vorgenannten Druckschriften beschriebene

„TwinSafe-Logic-Busklemme“ eine Steuerung mit integrierten lokalen Ausgängen betrifft. Jedoch hatte der Fachmann keine Veranlassung, die sicherheitsbezogene Servereinrichtung („Safety Server“) der Druckschrift D4 durch eine Steuerungsvorrichtung mit integrierten Ausgängen gemäß dem Baustein KL6904 zu ersetzen. Denn die für eine Automatisierungsanlage vorgesehenen Bausteine KL6904 und KL1904 der Druckschrift D19 sind für eine gemischte Kommunikation mit Standard-Applikation und sicherheitsgerichteten Applikationen vorgesehen. In der Druckschrift D19 ist explizit erwähnt, dass die Trennung von Standard- und Sicherheitssteuerung entfalle (vgl. S. 39, mittlere Spalte unten).

Der Fachmann hätte sich von der Modularität und gelehrten Auftrennung von Standard- und Sicherheitsteuerung gemäß Druckschrift D4 abwenden müssen und stattdessen die sicherheitsbezogene Servereinrichtung der Druckschrift D4 mit den Ausgabemodulen funktional verknüpfen müssen. Dies hätte eine Abkehr von der Struktur der Verbindungen bedeutet, da dann zwei verschiedene Arten von Verbindungen (mit je zwei bzw. drei Teilnehmern) gebildet und verwaltet werden müssten.

Aber selbst wenn der Fachmann die Lehre der Druckschrift D4 mit dem Baustein KL6904 der Druckschrift D19 (bzw. D17) kombiniert hätte, hätte er damit nicht zum Gegenstand des geltenden Patentanspruchs 1 gelangen können, da auch bei dieser mosaikartigen Zusammenschau die Merkmale M1.9 und M1.10 nicht entnehmbar wären. Dies gilt in gleicher Weise für die Annahme eines „Zusammenfallens“ von Kommunikations-Master und Sicherheitsmaster für die allein der Senat schon keine fachmännische Anregung sehen kann.

Insofern kann die von der Patentinhaberin bestrittene Vorveröffentlichung der Druckschrift D17 dahinstehen.

Auch keine der weiteren Druckschriften (D1 bis D3, D5 bis D16, D18 und D20 bis D23) liefert dem Fachmann eine Anregung, der Lehre der Druckschrift D4 noch die Merkmale M1.9 und M1.10 hinzuzufügen.

Der Gegenstand des geltenden Patentanspruchs 1 beruht somit auf einer erfinderischen Tätigkeit. Gleiches gilt für den Gegenstand des geltenden nebengeordneten Patentanspruchs 5, der das der Automatisierungsanlage gemäß Patentanspruch 1 zugrundeliegende Verfahren zum Überwachen der Sicherheitsinformationen betrifft.

Die auf Patentanspruch 1 rückbezogenen Unteransprüche 2 bis 4 bilden den Gegenstand des sie tragenden Bezugsanspruchs in nicht selbstverständlicher Weise weiter und erweisen sich daher ebenfalls als patentfähig.

6. Im Ergebnis ist das Patent daher mit geänderten Unterlagen im beschränkten Umfang aufrechtzuerhalten.

Rechtsbehelfsbelehrung

Gegen diesen Beschluss des Beschwerdesenats steht den am Beschwerdeverfahren Beteiligten die Rechtsbeschwerde zu (§ 99 Absatz 2, § 100 Absatz 1, § 101 Absatz 1 des Patentgesetzes).

Da der Senat die Rechtsbeschwerde nicht zugelassen hat, ist sie nur statthaft, wenn gerügt wird, dass

1. das beschließende Gericht nicht vorschriftsmäßig besetzt war,
2. bei dem Beschluss ein Richter mitgewirkt hat, der von der Ausübung des Richteramtes kraft Gesetzes ausgeschlossen oder wegen Besorgnis der Befangenheit mit Erfolg abgelehnt war,
3. einem Beteiligten das rechtliche Gehör versagt war,
4. ein Beteiligter im Verfahren nicht nach Vorschrift des Gesetzes vertreten war, sofern er nicht der Führung des Verfahrens ausdrücklich oder stillschweigend zugestimmt hat,

5. der Beschluss aufgrund einer mündlichen Verhandlung ergangen ist, bei der die Vorschriften über die Öffentlichkeit des Verfahrens verletzt worden sind, oder
6. der Beschluss nicht mit Gründen versehen ist

(§ 100 Absatz 3 des Patentgesetzes).

Die Rechtsbeschwerde ist beim Bundesgerichtshof einzulegen (§ 100 Absatz 1 des Patentgesetzes). Sitz des Bundesgerichtshofes ist Karlsruhe (§ 123 GVG).
Die Rechtsbeschwerde ist innerhalb eines Monats nach Zustellung des Beschlusses beim Bundesgerichtshof schriftlich einzulegen (§ 102 Absatz 1 des Patentgesetzes). Die Postanschrift lautet: Bundesgerichtshof, Herrenstraße 45 a, 76133 Karlsruhe.
Sie kann auch als elektronisches Dokument eingereicht werden (§ 125a Absatz 2 des Patentgesetzes in Verbindung mit der Verordnung über den elektronischen Rechtsverkehr beim Bundesgerichtshof und Bundespatentgericht (BGH/BPatGERVV) vom 24. August 2007 (BGBl. I S. 2130)). In diesem Fall muss die Einreichung durch die Übertragung des elektronischen Dokuments in die elektronische Poststelle des Bundesgerichtshofes erfolgen (§ 2 Absatz 2 BGH/BPatGERVV).
Die Rechtsbeschwerde kann nur darauf gestützt werden, dass der Beschluss auf einer Verletzung des Rechts beruht (§ 101 Absatz 2 des Patentgesetzes). Die Rechtsbeschwerde ist zu begründen. Die Frist für die Begründung beträgt einen Monat; sie beginnt mit der Einlegung der Rechtsbeschwerde und kann auf Antrag von dem Vorsitzenden verlängert werden (§ 102 Absatz 3 des Patentgesetzes). Die Begründung muss enthalten:

1. die Erklärung, inwieweit der Beschluss angefochten und seine Abänderung oder Aufhebung beantragt wird;
2. die Bezeichnung der verletzten Rechtsnorm;
3. insoweit die Rechtsbeschwerde darauf gestützt wird, dass das Gesetz in Bezug auf das Verfahren verletzt sei, die Bezeichnung der Tatsachen, die den Mangel ergeben

(§ 102 Absatz 4 des Patentgesetzes).

Vor dem Bundesgerichtshof müssen sich die Beteiligten durch einen beim Bundesgerichtshof zugelassenen Rechtsanwalt als Bevollmächtigten vertreten lassen (§ 102 Absatz 5 des Patentgesetzes).

Musiol Dorn Albertshofer Bieringer

Hu