



BUNDESPATENTGERICHT

23 W (pat) 4/14

(Aktenzeichen)

BESCHLUSS

In der Einspruchsbeschwerdesache

...

betreffend das Patent 10 2008 044 018

hat der 23. Senat (Techn. Beschwerdesenat) des Bundespatentgerichts unter Mitwirkung des Vorsitzenden Richters Dipl.-Phys. Dr. Strößner sowie der Richter Dipl.-Phys. Dr. Friedrich, Dipl.-Phys. Dr. Zebisch und Dr. Himmelmann am 12. August 2015

beschlossen:

Die Beschwerde wird zurückgewiesen.

Gründe

I.

Die Prüfungsstelle für Klasse G08C des Deutschen Patent- und Markenamts hat das am 24. November 2008 beim Deutschen Patent- und Markenamt angemeldete und mit der DE 10 2008 044 018 A1 offengelegte Patent 10 2008 044 018 (Streitpatent) mit der Bezeichnung „Verfahren zum Bestimmen einer Sicherheitsstufe und Sicherheitsmanager“ durch Beschluss vom 1. Februar 2010 erteilt. Das Patent wurde am 19. August 2010 mit der DE 10 2008 044 018 B4 veröffentlicht.

Im Prüfungsverfahren hat die Prüfungsstelle den Stand der Technik gemäß den folgenden Druckschriften zitiert:

- D1 DE 103 18 837 A1,
- D2 EP 1 300 657 A2,
- D3 DE 44 09 543 A1 und

- D4 „Wahrscheinlichkeitsrechnung leicht gemacht“. In: Service-Box des Online-Magazins: CICweb (Online-Service der Henrich Publikationen GmbH), Ausgabe AUT06/2005, S. 1-3, (<http://www.cicweb.de/index.cfm?pid=1473&pk=66042#>).

Gegen das Patent hat die Einsprechende mit Schriftsatz vom 18. November 2010, am Tag darauf beim Deutschen Patent- und Markenamt eingegangen, Einspruch erhoben. In ihrem Schriftsatz hat sie beantragt, das Streitpatent in vollem Umfang zu widerrufen (§ 61 PatG), wobei sie als Widerrufsgrund fehlende Patentfähigkeit (§ 21 Abs. 1 Nr. 1 PatG) auf Grund fehlender Neuheit (§ 3 PatG) und fehlender erfinderischer Tätigkeit (§ 4 PatG) angegeben hat. Sie hat sich bei ihrer Begründung im Hinblick auf die fehlende Patentfähigkeit neben den von der Prüfungsstelle genannten Druckschriften auf folgende Druckschriften gestützt:

- E1 EP 1 918 794 A1,
- E2 WO 2008/096 006 A1,
- E3 EP 1 980 964 A1,
- E4 US 2007/0 198 108 A1,
- E5 US 2005/0 027 374 A1 und
- E6 DE 10 2004 020 994 A1

Auf den Einspruch hin hat die Patentinhaberin mit Schriftsatz vom 29. Dezember 2011 den Ansichten der Einsprechenden in allen Punkten widersprochen und insbesondere ausgeführt, dass der Gegenstand des erteilten Anspruchs 1 sowohl neu sei als auch auf einer erfinderischen Tätigkeit des Fachmanns beruhe.

Dieser Ansicht ist die Einsprechende mit einem weiteren Schriftsatz vom 4. Mai 2012 entgegengetreten. Sie ist dabei auf die Argumentation der Patentinhaberin eingegangen und hat ihre Auslegung des Wortlautes der Ansprüche 1 und 8 in diesem Schriftsatz nochmals deutlich gemacht.

Mit Schriftsatz vom 24. September 2013 hat die Patentinhaberin nochmals ihre Sichtweise als Antwort auf den Schriftsatz der Einsprechenden dargestellt und ihre Ansicht, dass der Patentgegenstand sowohl neu sei als auch auf einer erfindnerischen Tätigkeit beruhe, nochmals bekräftigt.

In der Anhörung vor der Patentabteilung 31 des Deutschen Patent- und Markenamts am 24. Oktober 2013, in der die Patentabteilung ihre Sichtweise der in den Schriftsätzen kaum berücksichtigten Druckschrift E4 dargelegt hat, hat die Patentinhaberin einen neuen Satz Patentansprüche als Hilfsantrag eingereicht. Sie hat die Aufrechterhaltung gemäß Hauptantrag, also gemäß dem erteilten Patent, und hilfsweise die Aufrechterhaltung gemäß Hilfsantrag beantragt.

Die Einsprechende hat in der mündlichen Verhandlung den zusätzlichen Antrag gestellt, den Hilfsantrag der Patentinhaberin als verspätet vorgebracht zurückzuweisen, welchem seitens der Patentabteilung nicht stattgegeben wurde.

Als Ergebnis der Anhörung wurde das Streitpatent durch Beschluss der Patentabteilung 31 des Deutschen Patent- und Markenamts in der Anhörung gemäß § 61 Abs. 1 Satz 1 PatG widerrufen.

Die Patentabteilung hat in ihrer auf den 12. November 2013 datierten Beschlussbegründung ausgeführt, dass sowohl das Verfahren des erteilten Anspruchs 1 als auch des Anspruchs 1 des Hilfsantrags gegenüber der Lehre der Druckschrift E4 nicht neu seien (§ 3 PatG), weshalb diese Verfahren nicht patentfähig seien, so dass das Streitpatent zu widerrufen sei.

In der elektronischen Akte des DPMA finden sich zwei in Details unterschiedliche PDF-Dateien mit der Bezeichnung „Beschluss Widerruf - Signiert“ und jeweils drei zugehörige Signaturdateien „SIG-1“, „SIG-2“ und „SIG-3“.

Der Beschluss wurde dem Vertreter der Patentinhaberin am 18. November 2013 zugestellt und am 15. November 2013 im Abholfach der Einsprechenden niedergelegt.

Gegen diesen Beschluss der Patentabteilung 31 hat die Patentinhaberin mit Schriftsatz vom 12. Dezember 2013, am selben Tag beim Deutschen Patent- und Markenamt per Fax eingegangen, Beschwerde eingelegt und eine Beschwerdebegründung angekündigt, welche sie aber nicht eingereicht hat.

Da auch keine neuen Anträge eingereicht wurden, besteht die Aufgabe des Senats darin, die Entscheidung der Patentabteilung 31 zu überprüfen. Dies ist gleichbedeutend mit einem Antrag der Patentinhaberin,

1. Den angefochtenen Beschluss der Patentabteilung 31 des Deutschen Patent- und Markenamts vom 24. Oktober 2013 / 12. November 2013 aufzuheben.
- 2.1 Das Patent 10 2008 044 018 mit der Bezeichnung „Verfahren zum Bestimmen einer Sicherheitsstufe und Sicherheitsmanager“ und dem Anmeldetag 24. November 2008 wie erteilt aufrechtzuerhalten.
- 2.2 Hilfsweise das Patent 10 2008 044 018 mit der Bezeichnung „Verfahren zum Bestimmen einer Sicherheitsstufe und Sicherheitsmanager“ und dem Anmeldetag 24. November 2008 beschränkt aufrechtzuerhalten auf der Grundlage folgender Unterlagen:
 - Patentansprüche 1 bis 10 vom 24. Oktober 2013,
 - Beschreibung und Figuren gemäß Patentschrift 10 2008 044 018 B4.

Weder von der Patentinhaberin noch von der Einsprechenden wurden weitere Anträge gestellt. Insbesondere wurde von keiner Seite ein Antrag auf eine mündliche Verhandlung gestellt.

Der erteilte Anspruch 1 lautet (mit bei unverändertem Wortlaut eingefügter Gliederung entsprechend der im Einspruchsverfahren verwendeten):

- 1A Verfahren zum Bestimmen einer Sicherheitsstufe in einem Automatisierungsnetzwerk mit Teilnehmern, mit den Schritten:
- 1B selbsttätiges Ermitteln der daten- und ablauftechnischen Verknüpfungen zwischen den Teilnehmer im Automatisierungsnetzwerk durch ein Konfigurationserfassungsmodul (24);
- 1C selbsttätiges Ermitteln der teilnehmerspezifischen Sicherheitskenndaten durch ein Kenndatenerfassungsmodul (25);
und
- 1D Berechnen der Sicherheitsstufe in dem Automatisierungsnetzwerk mithilfe einer Berechnungsvorschrift,
- 1E die die ermittelten daten- und ablauftechnischen Verknüpfungen der Teilnehmer im Automatisierungsnetzwerk und die ermittelten teilnehmerspezifischen Sicherheitskenndaten verbindet.

Anspruch 1 des in der Anhörung überreichten Anspruchssatzes des Hilfsantrags lautet (mit bei unverändertem Wortlaut eingefügter Gliederung entsprechend der im Einspruchsverfahren verwendeten):

- 1A Verfahren zum Bestimmen einer Sicherheitsstufe in einem Automatisierungsnetzwerk mit Teilnehmern, mit den Schritten:
- 1B' selbsttätiges Ermitteln der daten- und ablauftechnischen Verknüpfungen zwischen den sicherheitsrelevanten Teilnehmern im Automatisierungsnetzwerk zum Ausführen der Sicherheitsfunktionen durch ein Konfigurationserfassungsmodul (24);

- 1C' selbsttätiges Ermitteln der teilnehmerspezifischen Sicherheitskenndaten der sicherheitsrelevanten Teilnehmer durch ein Kenndatenerfassungsmodul (25); und
- 1D Berechnen der Sicherheitsstufe in dem Automatisierungsnetzwerk mithilfe einer Berechnungsvorschrift,
- 1E die die ermittelten daten- und ablauftechnischen Verknüpfungen der Teilnehmer im Automatisierungsnetzwerk und die ermittelten teilnehmerspezifischen Sicherheitskenndaten verbindet.

Dabei bezeichnen die unterstrichenen Teile die Änderungen gegenüber dem erteilten Anspruch 1.

Bezüglich der auf ein Computerprogrammprodukt, einen Sicherheitsmanager und ein Automatisierungsnetzwerk gerichteten zu Anspruch 1 nebengeordneten Ansprüche 6, 8 bzw. 10 sowie der auf die Ansprüche 1, 6 und 8 direkt oder indirekt rückbezogenen Unteransprüche 2 bis 5, 7 bzw. 9 wird wie bezüglich der weiteren Einzelheiten auf den Akteninhalt verwiesen.

II.

Die rechtzeitig eingelegte Beschwerde ist zulässig aber unbegründet, da sowohl das Verfahren des erteilten Anspruchs 1 als auch das Verfahren des Anspruchs 1 gemäß Hilfsantrag gegenüber der Druckschrift E4 nicht neu sind (§ 3 PatG), weshalb das Patent zu widerrufen war (§§ 59 Abs. 1, 21 Abs. 1 Nr. 1 PatG). Der Beschluss der Patentabteilung 31 des Deutschen Patent- und Markenamtes hält somit einer Überprüfung stand.

1. In der elektronischen Akte des DPMA existieren zwei mit „Beschluss Widerruf - Signiert“ bezeichnete PDF-Dateien, von denen eine zudem, ebenso wie die Dokumentanzeige in den Signaturdateien, mehrere Beschlusstexte enthält, so dass eine präzise Bestimmung der Urschrift nicht möglich ist. Da aber der Tenor

und die Gründe der mehrfach vorhandenen Beschlusstexte in den beiden PDF-Dateien alle übereinstimmen, ist der Inhalt der Entscheidung, die mit den qualifizierten Signaturen versehen werden sollte, zumindest bestimmbar (vgl. *BPatG BIPMZ 2014, 355, 356 - Anordnung zur Erfassung von Berührungen auf einer Trägerplatte*), weshalb der Senat keine Veranlassung sieht, das Verfahren nach § 79 Abs. 3 Satz 1 Nr. 2 PatG an das Deutsche Patent- und Markenamt zurückzuverweisen.

2. Die Zulässigkeit des Einspruchs ist von Amts wegen in jedem Verfahrensstadium, auch im Beschwerdeverfahren, zu prüfen (vgl. *Schulte PatG, 9. Auflage, § 59 Rdn. 51 und 150 bis 152; BGH GRUR 1972, 592 – „Sortiergerät“*), da nur das Vorliegen eines zulässigen Einspruchs die weitere sachliche Überprüfung eines erteilten Patents erlaubt.

Vorliegend ist der form- und fristgerecht erhobene Einspruch zulässig, weil zu dem geltend gemachten Einspruchsgrund der mangelnden Patentfähigkeit auf Grund fehlender Neuheit und fehlender erfinderischer Tätigkeit (§ 21 Abs. 1 Nr. 1 PatG i. V. m. §§ 3, 4 PatG) substantiiert Stellung genommen wurde. So hat die Einsprechende genau angegeben, wo welche Merkmale des Verfahrens des Anspruchs 1 und des Gegenstandes des Anspruchs 8 in den einzelnen Druckschriften offenbart seien. Zudem hat sie in Bezug auf die mangelnde erfinderische Tätigkeit angegeben, wie sich der Gegenstand des Anspruchs 1 durch Zusammenschau der Druckschriften ihrer Meinung nach ergebe. Auch zu den übrigen Ansprüchen wurde Stellung genommen und angegeben, wo in den genannten Druckschriften die in diesen Ansprüchen beanspruchten Merkmale offenbart seien, oder wie sie sich ergäben. Insgesamt sind somit die Tatsachen, die den Einspruch rechtfertigen, im Einzelnen aufgeführt (§ 59 Abs. 1 Satz 4 PatG). Die Patentabteilung des Deutschen Patent- und Markenamts und auch die Patentinhaberin wurden demnach in die Lage versetzt, ohne eigene Nachforschungen festzustellen, ob die behaupteten Einspruchsgründe vorliegen (vgl. hierzu *BGH BIPMZ 1988, 250, Leit-*

satz 2, 251, liSp, Abs. 1 - „Epoxidation“; Schulte, PatG, 9. Auflage, § 59 Rdn. 83 bis 89).

3. Das Streitpatent betrifft ein Verfahren zum Bestimmen einer Sicherheitsstufe in einem Automatisierungsnetzwerk mit Teilnehmern, einen Sicherheitsmanager und ein Automatisierungsnetzwerk (vgl. Abs. [0001] des Streitpatents).

Moderne Konzepte der Industrieautomation, d. h. der Steuerung und Überwachung von technischen Prozessen mithilfe von Software beruhen auf der Idee einer zentralen Steuerung mit verteilter Sensor-/Aktorebene. Die Teilnehmer kommunizieren dabei untereinander und mit übergeordneten Systemen über industrielle lokale Netzwerke, welche auch als Automatisierungsnetzwerke bezeichnet werden. Die Automatisierungsnetzwerke sind in der Regel als sogenannte Master-Slave-Kommunikationsnetze ausgelegt, bei denen der Masterteilnehmer die Steuerungsebene und die Slaveteilnehmer die Sensor-/Aktorebene bilden.

Eine wesentliche Anforderung in der Industrieautomation ist die Sicherheit. Es muss bei der Ausführung von Automatisierungsaufgaben sichergestellt sein, dass vom Automatisierungsnetzwerk dann, wenn ein Teilnehmer ausfällt, oder ein anderer Fehler auftritt, keine Gefahr für Mensch und Umwelt ausgeht. Um die Gefährdung durch ein Automatisierungsnetzwerk einzustufen zu können, ist es Vorschrift, eine Gefahrenanalyse vorzunehmen. Gemäß der europäischen Norm EN1050 hat die Risikobeurteilung als eine Folge von logischen Schritten zu erfolgen, welche die systematische Untersuchung von Gefährdung erlaubt, die vom Automatisierungsnetzwerk bzw. den einzelnen Teilnehmern ausgehen. Auf der Grundlage der Gefahrenanalyse werden dann die technischen und organisatorischen Anforderungen an das Automatisierungsnetzwerk zur Gewährleistung einer ausreichenden Sicherheit festgelegt.

Die europäische Norm EN 954-1 „Sicherheit für Maschinen - Sicherheitsbezogene Teile von Steuerungen“ hat sich dabei im Bereich der Maschinen- und Anlagensi-

cherheit als internationaler Standard zur Durchführung einer Gefährdungsanalyse etabliert. Die Norm bezieht alle sicherheitsrelevanten Teilnehmer unabhängig vom Teilnehmertyp ein und unterteilt die sicherheitstechnische Leistungsfähigkeit in Kategorien. Ausgehend von der ermittelten Sicherheitskategorie wird dann die Steuerungsstruktur im Automatisierungsnetzwerk ausgelegt, um die Anforderungen an die Sicherheitsfunktionen und ein gefordertes Systemverhalten im Fehlerfall zu erreichen.

Um insbesondere auch programmierbaren elektronischen Steuerungssystemen in Bezug auf die Sicherheitsanforderungen gerecht zu werden, wurden in den letzten Jahren zusätzlich zur EN 954-1 weitere Normen verabschiedet. Für die Gefahrenanalyse in Automatisierungsnetzwerken sind insbesondere die Norm EN ISO13849-1 und IEC/EN 62061 relevant. Mit diesen beiden Normen erfolgt über den qualitativen Ansatz der Norm EN954-1 hinaus eine quantitative Betrachtung der Sicherheitsfunktionen. Sie spezifizieren die zur Risikoreduzierung erforderliche sicherheitstechnische Leistungsfähigkeit von programmierbaren elektronischen Steuerungssystemen. Zur Unterteilung der sicherheitstechnischen Leistungsfähigkeit werden in den beiden Normen Sicherheitsstufen definiert. Hierzu werden alle Sicherheitsfunktionen des Automatisierungsnetzwerks mit allen an ihrer Ausführung beteiligten Teilnehmern betrachtet.

Die Sicherheitsstufe des Automatisierungsnetzwerks wird auf der Grundlage von sicherheitstechnischen Kenngrößen der an den Sicherheitsfunktionen beteiligten Teilnehmer bestimmt. Diese Kenngrößen sind dabei gemäß der Norm EN ISO13849-1 u. a. die mittlere Zeit für einen gefährlichen Ausfall (MTTF), der Diagnosedeckungsgrad (DC), die durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls je Stunde (PFH), die Gebrauchsdauer (T_M), die Anzahl von Zyklen, bei denen 10% einer Stichprobe der betrachteten verschleißbehafteten Teilnehmer gefährlich ausgefallen sind (B_{10d}), und der Ausfall aufgrund gemeinsamer Ursache (CCF). Neben diesen genannten sicherheitstechnischen Kenngrößen können noch weitere Parameter, auch betriebliche Gesichtspunkte wie die Anforder-

rungrate oder die Testrate der Sicherheitsfunktion Einfluss auf die Sicherheitsstufe haben.

Zum Bestimmen der Sicherheitsstufe eines Automatisierungsnetzwerkes ist ferner neben der Kenntnis der sicherheitstechnischen Kenngrößen aller an der Sicherheitsfunktion beteiligten Teilnehmer eine genaue Information über die logische Verknüpfung der Teilnehmer im Automatisierungsnetzwerk erforderlich.

Um die Gefährdung durch ein Automatisierungsnetzwerk zuverlässig einstufen zu können, sind aufwendige Berechnungen, z. B. mithilfe der Markov-Analyse notwendig. Darüber hinaus muss die Ausfallwahrscheinlichkeit einzelner Teilnehmer aufgrund unzureichender Daten teilweise geschätzt werden, was eine gesicherte Aussage schwierig macht. Die Bestimmung der Sicherheitsstufe im Automatisierungsnetzwerk stellt deshalb insbesondere kleine und mittelständische Unternehmen vor erhebliche Probleme.

In den letzten Jahren kamen vermehrt Sicherheitstools auf den Markt. Diese Sicherheitstools berechnen die Sicherheitsstufe von Sicherheitsfunktionen in Automatisierungsnetzwerken abhängig von den verwendeten Teilnehmern. Die teilnehmerspezifischen Sicherheitskenndaten werden dabei einer Software-Bibliothek entnommen. Die Struktur der Anlage, d. h. die Daten- und ablaufspezifische Verknüpfung der Teilnehmer im Automatisierungsnetzwerk muss aber zusätzlich individuell eingegeben werden. Die Sicherheitstools verifizieren die berechnete Sicherheitsstufe mit der gemäß den Normen EN ISO13849-1 und EN/EC62061 erforderlichen Sicherheitsstufe und zeigen eventuellen Handlungsbedarf zur Verbesserung der Sicherheit im Automatisierungsnetzwerk auf.

Die Verwendung einer Software-Bibliothek zur Erfassung der teilnehmerspezifischen Sicherheitskenndaten macht es erforderlich, diese Bibliothek ständig zu aktualisieren, um bei der Sicherheitsberechnung neue Teilnehmer einbeziehen zu können bzw. in den Teilnehmern vorgenommene Veränderungen berücksichtigen

zu können. Ferner ist das Erfordernis, die daten- und ablaufspezifische Verknüpfung der Teilnehmer im Automatisierungsnetzwerk individuell in das Sicherheitstool einzugeben, zeitintensiv und auch fehleranfällig. In der Regel wird deshalb nur eine vereinfachte Betrachtung der Steuerungslogik im Automatisierungsnetzwerk bei der Bestimmung der Sicherheitsstufe durchgeführt. Bei einer Erweiterung oder Änderung des Automatisierungsnetzwerkes ist es außerdem erforderlich, die geänderte Struktur neu zu erfassen, um die aktuelle Sicherheitsstufe bestimmen zu können (*vgl. Abs. [0002] bis [0011] der Streitpatentschrift*).

Vor diesem Hintergrund liegt dem Streitpatent als technisches Problem die Aufgabe zugrunde, ein Verfahren zum Bestimmen der Sicherheitsstufe in einem Automatisierungsnetzwerk bzw. einen Sicherheitsmanager für ein solches Automatisierungsnetzwerk bereit zu stellen, die auf einfache und zuverlässige Weise eine automatische Berechnung der Sicherheitsstufe, insbesondere auch bei weiteren Änderungen im Automatisierungsnetzwerk ermöglichen (*Vgl. Abs. [0015] der geltenden Beschreibung*).

Diese Aufgabe wird durch die Verfahren und Gegenstände der selbständigen Ansprüche des erteilten Patents und des Hilfsantrags, insbesondere durch die Verfahren nach den Ansprüchen 1 der beiden Anträge gelöst.

Das in Anspruch 1 des Streitpatents beanspruchte Verfahren bestimmt eine Sicherheitsstufe in einem Automatisierungsnetzwerk, welches mehrere Teilnehmer hat. Es berechnet diese Sicherheitsstufe mit Hilfe einer Berechnungsvorschrift, welche beispielsweise durch Normen vorgegeben ist. Für diese Berechnung benötigt es mehrere Informationen, so beispielsweise die daten- und ablauftechnischen Verknüpfungen zwischen den Teilnehmern im Automatisierungsnetzwerk und die teilnehmerspezifischen Sicherheitskenndaten. Diese ermittelt das Verfahren selbsttätig. Für diese Ermittlungen sind jeweils eigene Module vorgesehen. Bei diesen Modulen handelt es sich, wie aus der Anmeldung ersichtlich ist, in erster

Linie um Softwaremodule, jedoch schließt Anspruch 1 eine Realisierung der Module in Hardware nicht aus.

Im Anspruch 1 des Hilfsantrags wird das Ermitteln der daten- und ablauftechnischen Verknüpfungen und das Ermitteln der teilnehmerspezifischen Sicherheitskenndaten auf die sicherheitsrelevanten Teilnehmer beschränkt, ohne dass dabei ausgeschlossen wird, dass das Ermitteln auch bei den nicht sicherheitsrelevanten Teilnehmern durchgeführt wird. Beim zusätzlich eingefügten Merkmal „zum Ausführen der Sicherheitsfunktionen“ bleibt der Bezug offen, so dass sich diese Zweckangabe sowohl auf das selbsttätige Ermitteln der daten- und ablauftechnischen Verknüpfungen als auch auf die sicherheitsrelevanten Teilnehmer oder das Automatisierungsnetzwerk beziehen kann.

4. Das Verfahren des erteilten Anspruchs 1 ist wie auch das Verfahren des Anspruchs 1 des Hilfsantrags gegenüber der Lehre der Druckschrift E4 nicht neu (§ 3 PatG), so dass es nicht patentfähig ist.

Bei dieser Sachlage kann die Erörterung der Zulässigkeit der Ansprüche des Hauptantrags und des Hilfsantrags dahingestellt bleiben (vgl. *BGH GRUR 1991, 120, 121, II.1 – „Elastische Bandage“*).

Als zuständiger Fachmann ist hier ein berufserfahrener Ingenieur der Fachrichtung Elektrotechnik oder ein Informatiker mit Hochschul- oder Fachhochschulabschluss zu definieren, der über langjährige Erfahrung auf dem Gebiet der Automatisierungsnetzwerke und der mit diesen verbundenen Sicherheitsfragen verfügt.

4.1 So offenbart Druckschrift E4, wie von der Patentabteilung 31 des Deutschen Patent- und Markenamts in ihrem Beschluss vom 24. Oktober/12. November 2013 angegeben, entsprechend den Merkmalen des Anspruchs 1 des **Hauptantrags** ein

1A Verfahren zum Bestimmen einer Sicherheitsstufe in einem Automatisierungsnetzwerk mit Teilnehmern.

Die Druckschrift E4 offenbart ein Industrieautomatisierungssystem, das Sicherheitsstufen visualisiert, wie sie beispielsweise in der Norm IEC 61508 definiert sind (vgl. die Ansprüche 1: *„An industrial automation system that visualizes availability and safety levels, comprising: an optimization component that generates a voting configuration that provides an optimized combination of a safety level and an availability level based upon available redundancy; and a graphical user interface that presents a visualization of the safety level and the availability level.”* und 4: *„The system of claim 1, the graphical user interface utilizes safety integrity levels as provided by IEC 61508.”*). Diese Sicherheitsstufen werden aber nicht nur angezeigt, sondern auch bestimmt (siehe Fig. 13 i. V. m. Abs. [0065]: *„At 1306, a voting configuration can be generated based on the allocation of safety and availability. When generating the voting configuration, a number of factors can be considered such as, for instance, a likelihood of common mode failure, faults associated with various industrial automation devices (e.g., historical data related to faults, faults that are currently existent, ...), etc. The generated voting configuration can be utilized to combine outputs from a number of industrial automation devices. At 1308, a visualization related to the allocation of safety and availability can be graphically displayed. For instance, a safety level (e.g., safety integrity level) and/or an availability level can be graphically provided.”*).

Das Industrieautomatisierungssystem erhält seine Eingangsdaten über eine Schnittstelle von den angeschlossenen Industrieautomatisierungsgeräten (vgl. Abs. [0027]: *„The interface component 102 can obtain the input data from one or more industrial automation devices“*), welche somit Teilnehmer in einem Automatisierungsnetzwerk sind (siehe die Fig. 11 und 12 i. V. m. Abs. [0057]: *„Referring to FIG. 11, illustrated is a system 1100 that utilizes a voting configuration to implement an optimized utilization of available redundancy. The system 1100 includes an optimization component 104 that can generate a voting configuration. For in-*

stance, the voting configuration can be provided by the optimization component 104 at a time of initialization of the system 1100, dynamically generated during operation of the system 1100, etc. Further, the system 1100 can include the graphical user interface 106 that generates a visualization related to safety and/or availability levels associated with the voting configuration. The system 1100 additionally can include N devices (e.g., device 11102, device 21104 ... device N 1106), where N is any positive integer. It is contemplated that the N devices 1102-1106 can be any type of industrial automation device. By way of example, the N devices 1102-1106 can be input devices (e.g., sensor, ...), logic solving devices (e.g., programmable logic controller (PLC), ...), output devices (e.g., actuator, cylinder, diaphragm, relay, solenoid, motor controller, robot, servo motion device, ...), etc. Additionally, the N devices 1102-1106 can provide redundancy that can be configured to implement safety, availability, or a combination thereof.”).

Das Verfahren weist folgende Schritte auf:

1B Selbsttätiges Ermitteln der daten- und ablauftechnischen Verknüpfungen zwischen den Teilnehmern im Automatisierungsnetzwerk durch ein Konfigurationserfassungsmodul:

Das Automatisierungssystem bestimmt zum einen die in ihm enthaltenen Teilnehmer, die mit einer Maschine oder einem Prozess verbunden sind, und es kann das Hinzufügen oder die Entnahme eines Teilnehmers feststellen und darauf reagieren (vgl. Abs. [0036]: *„The redundancy assessment component 202 can evaluate resources associated with an industrial automation environment, a machine, a process, etc. and determine an amount of available redundancy. For instance, the redundancy assessment component 202 can determine a number of available industrial automation devices. The redundancy assessment component 202 can further identify characteristics associated with the industrial automation devices. Thus, by way of example, the redundancy assessment component 202 can determine that four PLCs within the industrial automation environment can be utilized*

with a particular motor; [...] Thus, for instance, upon adding and/or removing an industrial automation device, input data related to the device (e.g., location, history, status, association with disparate devices and/or machines and/or processes, ...) can be provided to the redundancy assessment component 202 (e.g., by way of the interface component 102). It is to be appreciated that such information can be provided automatically upon adding and/or removing the industrial automation device, by a user, etc. According to an example, the redundancy assessment component 202 can thereafter store the input data related to the available redundancy (e.g., utilizing a data store (not shown), ...); ...”). Es bestimmt den Ort und den Zustand der Teilnehmer und ihre Beziehungen zueinander (vgl. Abs. [0065]: „At 1302, an evaluation can be effectuated to determine an amount of available redundancy. For example, a determination can be made related to a number of industrial automation devices (e.g., logic solvers, sensors, ...) included in the environment, locations of the devices, status of the devices, associations between devices, etc. ...”). Dies ist nichts anderes als das Ermitteln der daten- und ablauftechnischen Verknüpfungen zwischen den Teilnehmern im Automatisierungsnetzwerk. Da sich zumindest der letzte Absatz auf den Ablaufplan der Fig. 13 bezieht, wird diese Tätigkeit somit vom Automatisierungssystem selbst durchgeführt, worauf auch Abs. [0064] verweist, wo angegeben wird, dass der Verfahrensablauf auf einen Computer übertragen werden kann und in Form eines auf einem Datenträger vorhandenen Computerprogramms vorliegen kann (vgl. Abs. [0064]: „Referring to FIGS. 13-14, methodologies in accordance with various aspects of the claimed subject matter are illustrated. [...] Additionally, it should be further appreciated that the methodologies disclosed hereinafter and throughout this specification are capable of being stored on an article of manufacture to facilitate transporting and transferring such methodologies to computers. The term article of manufacture, as used herein, is intended to encompass a computer program accessible from any computer-readable device, carrier, or media.”). Das Ermitteln erfolgt demnach automatisch und wird durch ein Stück Software durchgeführt, das als “Konfigurationserfassungsmodul” bezeichnet werden kann.

1C Selbsttätiges Ermitteln der teilnehmerspezifischen Sicherheitskenndaten durch ein Kenndatenerfassungsmodul:

Als eine der Möglichkeiten, wie das Automatisierungssystem an teilnehmerspezifische Daten gelangt, wird der Erhalt dieser Daten aus den Teilnehmern angegeben (vgl. Abs. [0027]: *„The interface component 102 can receive the input data from any source. For instance, the interface component 102 can obtain the input data from one or more industrial automation devices. The industrial automation device(s) (not shown) can be an input device (e.g., sensor, ...), a logic solving device (e.g., programmable logic controller (PLC), . . .), an output device (e.g., actuator, cylinder, diaphragm, relay, solenoid, motor controller, robot, servo motion device, . . .), etc. ...”* und [0028]: *„... Further, the input data can relate to characteristics associated with the industrial automation devices (e.g., age, accuracy, location, history, status, ...). By way of example, the input data can be related to a risk of failure associated with the industrial automation device (e.g., a number of previous failures associated with the particular device, ...). According to another illustration, the input data can be associated with an amount of harm associated with a failure of the industrial automation device (e.g., damage caused to a person and/or property, downtime, ...).”*). Dass es sich dabei um ein selbsttätiges Ermitteln der teilnehmerspezifischen Daten handelt, wird deutlich, wenn als Alternative die Eingabe über das Graphic User Interface (GUI) angegeben wird (vgl. Abs. [0027]: *„...Additionally or alternatively, the interface component 102 can obtain input data from a user; for example, the graphical user interface 106 can be employed by a user to provide input data.”*) oder die Vorgehensweise beim Einfügen eines weiteren Teilnehmers geschildert wird. In letzterem Fall erfolgt die Bereitstellung und Übernahme der Daten ausdrücklich automatisch (vgl. Abs. [0036]: *„... Thus, for instance, upon adding and/or removing an industrial automation device, input data related to the device (e.g., location, history, status, association with disparate devices and/or machines and/or processes, ...) can be provided to the redundancy assessment component 202 (e.g., by way of the interface component 102). It is to be appreciated that such information can be provided automatically upon adding*

and/or removing the industrial automation device, by a user, etc. ...). Auch hier erfolgt das Ermitteln mittels eines Stückes Software (*vgl. die bereits zitierte Stelle in Abs. [0064]*), das als „Kenndatenerfassungsmodul“ bezeichnet werden kann.

1D Berechnen der Sicherheitsstufe in dem Automatisierungsnetzwerk mithilfe einer Berechnungsvorschrift:

Wie bereits zu Punkt 1A dargelegt, wird eine Sicherheitsstufe nach der Norm IEC 61508 bestimmt (*vgl. Ansprüche 1 und 4*), was eine Berechnung der Sicherheitsstufe nach einer Berechnungsvorschrift darstellt.

1E Die ermittelten daten- und ablauftechnischen Verknüpfungen der Teilnehmer im Automatisierungsnetzwerk und die ermittelten teilnehmerspezifischen Sicherheitskenndaten werden verbunden.

Druckschrift E4 unterscheidet nicht ausdrücklich zwischen den daten- und ablauftechnischen Verknüpfungen zwischen den Teilnehmern im Automatisierungsnetzwerk und den teilnehmerspezifischen Daten. Sie kennt nur Eingangsdaten (*input data*), welche miteinander zur Bestimmung der Sicherheitsstufe verknüpft werden. Diese Eingangsdaten enthalten beides, daten- und ablauftechnische Verknüpfungen, wie beispielsweise die verfügbare Redundanz oder ein überwachter Zustand eines Prozesses innerhalb der Automatisierungsumgebung, sowie teilnehmerspezifische Daten, wie das Alter, die Vorgeschichte und die Genauigkeit eines Teilnehmers (*vgl. Abs. [0028] und [0029]: „...According to an example, the input data can be a measured property associated with the industrial automation environment, a monitored condition related to a particular machine and/or process within the industrial automation environment, etc. Further, the input data can relate to characteristics associated with the industrial automation devices (e.g., age, accuracy, location, history, status, ...). [...] By way of example, the input data can include an indication of an amount of available redundancy. Additionally or alternatively, the optimization component 104 can identify an amount of available redun-*

dancy (e.g., from the input data). According to an illustration, the available redundancy can be related to a machine, a process, an environment, a combination thereof, etc. ...” und die bereits zitierten Stellen in den Abs. [0036] und [0065]). Aus den Eingangsdaten wird die Sicherheitsstufe bestimmt, womit dann auch die daten- und ablauftechnischen Verknüpfungen und die teilnehmerspezifischen Sicherheitskenndaten verknüpft werden.

Damit weist das in Druckschrift E4 offenbarte Verfahren alle Merkmale des erteilten Anspruchs 1 auf, so dass das Verfahren des Anspruchs 1 des Hauptantrags nicht neu (§ 3 PatG) und damit nicht patentfähig ist.

4.2 Die zusätzlichen einschränkenden Merkmale des Anspruchs 1 nach **Hilfsantrag** sind beim in Druckschrift E4 offenbarten Verfahren ebenfalls vorhanden, so dass sie die Neuheit des beanspruchten Verfahrens nicht begründen können.

So werden gemäß Fig. 11 der Druckschrift E4 alle Teilnehmer (*Device 1 bis Device N*) in das Verfahren einbezogen (*vgl. die bereits zitierte Stelle Abs. [0057]*). Damit sind insbesondere die sicherheitsrelevanten Teilnehmer mit ihren daten- und ablauftechnischen Verknüpfungen und ihren teilnehmerspezifischen Kenndaten in das Verfahren einbezogen.

Zudem gibt Druckschrift E4 an, dass die in Fig. 11 gezeigte Ausgabe (*combined output*) genutzt werden kann, um eine Maschine anzuhalten oder langsamer laufen zu lassen (*vgl. Abs. [0058]: „...For instance, the combined output can be provided back to the devices 1102-1106 (e.g., to enable halting operation, continuing operation, modifying operation such as by reducing speed, torque, human exposure, ...).”*), was eine Sicherheitsfunktion darstellt. Damit dienen auch das Ermitteln der daten- und ablauftechnischen Verknüpfungen zwischen den Teilnehmern im Automatisierungsnetzwerk und auch das Automatisierungsnetzwerk selbst dem Ausführen der Sicherheitsfunktionen.

Da das Verfahren des Anspruchs 1 des Hilfsantrags keine weiteren Zusatzmerkmale aufweist, ist es demnach ebenfalls nicht neu (§ 3 PatG) und damit nicht patentfähig.

5. Auf Grund der Antragsbindung fallen auch die nebengeordneten Ansprüche sowie die auf die selbständigen Ansprüche zurückbezogenen Unteransprüche mit dem jeweiligen Anspruch 1 (vgl. *BGH GRUR 2007, 862 – „Informationsübermittlungsverfahren II“*).

6. Da die Patentinhaberin und Beschwerdeführerin ausreichend Zeit zum Einreichen der angekündigten Beschwerdebegründung hatte, und weder die Patentinhaberin noch die Einsprechende eine mündliche Verhandlung beantragt haben, war nunmehr bei dieser Sachlage im schriftlichen Verfahren Beschluss zu fassen und die Beschwerde der Patentinhaberin zurückzuweisen. Damit bleibt der Beschluss der Patentabteilung, das Patent zu widerrufen, bestehen.

III. Rechtsmittelbelehrung

Gegen diesen Beschluss steht den am Verfahren Beteiligten - vorbehaltlich des Vorliegens der weiteren Rechtsmittelvoraussetzungen, insbesondere einer Beschwerde - das Rechtsmittel der **Rechtsbeschwerde** zu. Da der Senat die Rechtsbeschwerde nicht zugelassen hat, ist sie nur statthaft, wenn einer der nachfolgenden Verfahrensmängel gerügt wird, nämlich

1. dass das beschließende Gericht nicht vorschriftsmäßig besetzt war,
2. dass 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. dass einem Beteiligten das rechtliche Gehör versagt war,
4. dass ein Beteiligter im Verfahren nicht nach Vorschrift des Gesetzes vertreten war, sofern er nicht der Führung des Verfahrens ausdrücklich oder stillschweigend zugestimmt hat,
5. dass der Beschluss aufgrund einer mündlichen Verhandlung ergangen ist, bei der die Vorschriften über die Öffentlichkeit des Verfahrens verletzt worden sind, oder
6. dass der Beschluss nicht mit Gründen versehen ist.

Die Rechtsbeschwerde ist **innerhalb eines Monats** nach Zustellung des Beschlusses

schriftlich durch einen beim Bundesgerichtshof zugelassenen Rechtsanwalt als Bevollmächtigten beim Bundesgerichtshof, Herrenstr. 45 a, 76133 Karlsruhe, einzureichen oder

durch einen beim Bundesgerichtshof zugelassenen Rechtsanwalt als Bevollmächtigten in elektronischer Form bei der elektronischen Poststelle des BGH, www.bundesgerichtshof.de/erv.html. Das elektronische Dokument ist mit einer prüfbaren qualifizierten elektronischen Signatur nach dem Signaturgesetz oder

mit einer prüfbaren fortgeschrittenen elektronischen Signatur zu versehen. Die Eignungsvoraussetzungen für eine Prüfung und für die Formate des elektronischen Dokuments werden auf der Internetseite des Bundesgerichtshofs www.bundesgerichtshof.de/erv.html bekannt gegeben.

Dr. Strößner

Dr. Friedrich

Dr. Zebisch

Dr. Himmelmann

prä