(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
27. Oktober 2011 (27.10.2011)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2011/131414 A2

(51) Internationale Patentklassifikation:
G01D 21/00 (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2011/053420

(22) Internationales Anmeldedatum:
8. März 2011 (08.03.2011)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2010 017 938.8
22. April 2010 (22.04.2010) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **SIEMENS AKTIENGESELLSCHAFT** [DE/DE]; Wittelsbacherplatz 2, 80333 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **FRIES, Steffen** [DE/DE]; Eberweg 3, 85598 Baldham (DE). **NIEDERMAYR, Erich** [AT/DE]; Luitpoldring 38, 85591 Vaterstetten (DE). **SCHATTLEITNER, Angela** [DE/DE]; Bergstraße 1, 83104 Tuntenhausen (DE).

(74) Gemeinsamer Vertreter: **SIEMENS AKTIENGESELLSCHAFT**; Postfach 22 16 34, 80506 München (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

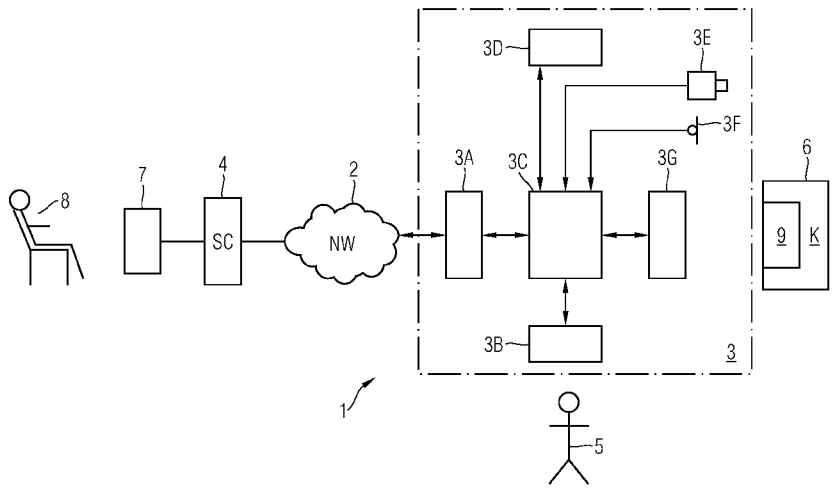
— *ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts (Regel 48 Absatz 2 Buchstabe g)*

[Fortsetzung auf der nächsten Seite]

(54) **Title**: SYSTEM AND METHOD FOR PROVIDING SENSOR DATA

(54) **Bezeichnung** : SYSTEM UND VERFAHREN ZUM BEREITSTELLEN VON SENSORDATEN

FIG 1



(57) **Abstract**: The present invention relates to a system and a method for providing sensor data relating to a state of a component (6) for a service centre (4) by means of at least one sensor, which is provided on a mobile device (3) authorized for this, after successful authentication has been carried out between the mobile device (3) and the component (6). The system according to the invention allows the use of remote maintenance communication devices (3) in closed operational areas of a company without jeopardizing the protection of trade secrets.

(57) **Zusammenfassung**: Die vorliegende Erfindung betrifft ein System und ein Verfahren zum Bereitstellen

[Fortsetzung auf der nächsten Seite]

WO 2011/131414 A2

von Sensordaten über einen Zustand einer Komponente (6) für ein Service-Center (4) durch mindestens einen Sensor, der an einem dazu autorisierten mobilen Gerät (3) vorgesehen ist, nachdem zwischen dem mobilen Gerät (3) und der Komponente (6) eine erfolgreiche Authentisierung erfolgt ist. Das erfindungsgemäße System erlaubt den Einsatz von Fernwartungskommunikationsgeräten (3) in geschlossenen Betriebsbereichen eines Unternehmens ohne den Schutz von Betriebsgeheimnissen zu gefährden.

Beschreibung

System und Verfahren zum Bereitstellen von Sensordaten

Die Erfindung betrifft ein System und ein Verfahren zum Bereistellen von Sensordaten über einen Zustand einer Komponente, insbesondere einer Maschinenkomponente.

Maschinen innerhalb von technischen Anlagen werden zunehmend komplexer und verlangen zunehmende Fertigkeiten und Fähigkeiten bei ihrer Instandsetzung und Wartung durch einen Wartungstechniker. Servicetechniker, die Servicearbeiten, beispielsweise Reparatur- oder Wartungsmaßnahmen, an einer Maschine oder einem Gerät einer technischen Anlage durchzuführen haben, benötigen daher in vielen Fällen die Unterstützung eines technischen Experten für die jeweilige Maschine bzw. Maschinenkomponente, der sich in einem entfernt gelegenen Service-Center aufhält. Besteht beispielsweise ein Reparatur- oder Wartungsbedarf an einer komplexeren technischen Komponente, kann sich der vor Ort befindlicher Service-Techniker über eine Kommunikationsverbindung mit einem Mitarbeiter eines Service-Centers in Verbindung setzen, um dessen Unterstützung bei der notwendigen Reparatur- und Wartungsmaßnahme der Komponente zu erhalten. Damit der Experte bzw. der Mitarbeiter in dem Service-Center den Vorort befindlichen Techniker wirksam unterstützen kann, werden hierzu auch Sprach-, Bild- und Videodaten der Kommunikationsverbindung ausgetauscht. Dies ist insbesondere dann hilfreich, wenn ein mechanisches Bauteil oder eine mechanische Komponente betroffen ist, die durch den Wartungstechniker vor Ort zu warten bzw. zu reparieren ist. Weiterhin kann die Übertragung von Sprach-, Bild- oder Videodaten hilfreich sein, um bei einer Prozessautomatisierung bestimmte Abläufe zur Fehlereingrenzung zu beobachten. Der Wartungstechniker trägt dabei ein Fernwartungskommunikationsgerät mit sich, das beispielsweise Ton- oder Bilddaten der zu wartenden bzw. zu reparierenden Maschinenkomponente an das Service-Center über die Kommunikationsverbindung überträgt.

Bei vielen Anwendungsfällen finden sich die zu reparierenden bzw. zu wartenden Geräte bzw. Maschinenkomponenten auf einem Betriebsgelände eines Anlagenbetreibers bzw. Unternehmens. Innerhalb dieses Betriebsgeländes sind sensible betriebliche Daten oder personenbezogene Daten vor einem unerlaubten Zugriff Dritter zu schützen. Daher ist es in vielen Betrieben nicht erlaubt, Fernwartungskommunikationsgeräte, insbesondere Fernwartungskommunikationsgeräte, die über Kameras oder sonstige Sensoren verfügen, auf dem Betriebsgelände mit sich zu führen. Dies verhindert herkömmlicher Weise in vielen Fällen eine effiziente Unterstützung eines Wartungstechnikers durch einen Experten bzw. Mitarbeiter eines entfernt gelegenen Service-Centers.

Es ist daher eine Aufgabe der vorliegenden Erfindung, ein System und ein Verfahren zu schaffen, das es ermöglicht, einen Nutzer bei seiner Tätigkeit auf einem Betriebsgelände gezielt durch einen Mitarbeiter eines Service-Centers zu unterstützen, ohne den Schutz betrieblicher oder personenbezogener Daten gegenüber einem unerlaubten Zugriff zu beeinträchtigen.

Diese Aufgabe wird erfindungsgemäß durch ein System mit den in Patentanspruch 1 angegebenen Merkmalen gelöst.

Die Erfindung schafft ein System zum Bereitstellen von Sensordaten über einen Zustand einer Komponente für einen Service-Center durch mindestens einen Sensor, der an einem dazu autorisierten mobilen Gerät vorgesehen ist, nachdem zwischen dem mobilen Gerät und der Komponente eine erfolgreiche Authentisierung erfolgt ist.

Bei der Komponente kann es sich beispielsweise um eine Maschinenkomponente einer Maschine handeln, die sich auf einem Betriebsgelände oder in einem sonstigen geschlossenen Bereich befindet. Bei der Maschinenkomponente kann es sich beispielsweise um ein mechanisches Bauteil einer Maschine handeln. Bei der Komponente kann es sich allerdings auch um immaterielle

Komponenten handeln, beispielsweise einen zu wartenden Programmcode, der sich auf einem Datenträger, beispielsweise einer Festplatte befindet.

Bei dem mobilen Gerät handelt es sich beispielsweise um ein Fernwartungskommunikationsgerät, das von einem Nutzer bzw. Techniker getragen wird, der Wartungs- oder Reparaturmaßnahmen an der jeweiligen Komponente vorzunehmen hat.

Bei einer möglichen Ausführungsform des erfindungsgemäßen Systems weist das mobile Gerät ein Nahfeld-Kommunikationsmodul auf, mittels dessen sich das mobile Gerät gegenüber der Komponente authentisiert oder mittels dessen sich die Komponente gegenüber dem mobilen Gerät authentisiert.

Bei einer möglichen Ausführungsform des erfindungsgemäßen Systems weist das mobile Gerät eine Netzwerkschnittstelle auf, die zum Aufbau einer Kommunikationsverbindung mit dem Service-Center über ein Datennetzwerk vorgesehen ist.

Bei einer möglichen Ausführungsform des erfindungsgemäßen Systems handelt es sich bei dem Sensor um eine Kamera, die Bild- oder Videodaten der Komponente oder deren Umgebung liefert.

Weiterhin kann es sich bei dem Sensor um ein Mikrofon handeln, das Geräuschdaten der Komponente aufnimmt.

Bei einer weiteren möglichen Ausführungsform ist der Sensor ein Mikrofon, das Sprachdaten eines Nutzers, welcher das mobile Gerät trägt, erfasst.

Bei einer möglichen Ausführungsform des erfindungsgemäßen Systems können auch weitere Sensoren in dem mobilen tragbaren Gerät vorgesehen sein, beispielsweise Sensoren, die physikalische Parameter der Komponente erfassen, beispielsweise Temperatur- oder Drucksensoren.

Bei einer möglichen Ausführungsform des erfindungsgemäßen Systems werden die von den verschiedenen Sensoren des mobilen Geräts bereitgestellten Sensordaten entsprechend der Autorisierung des mobilen Gerätes beschränkt von dem mobilen Gerät an das Service-Center übertragen.

Bei einer möglichen Ausführungsform des erfindungsgemäßen Systems erfolgt die Beschränkung der von dem mobilen Gerät an das Service-Center übertragenen Sensordaten hinsichtlich der Art der Sensordaten, welche beispielsweise Bilddaten, Videodaten, Geräuschdaten und Sprachdaten umfassen.

Bei einer weiteren möglichen Ausführungsform des erfindungsgemäßen Systems erfolgt die Beschränkung der von dem mobilen Gerät an das Service-Center übertragenen Sensordaten hinsichtlich eines aktuellen Aufenthaltsortes des mobilen Gerätes.

Bei einer weiteren möglichen Ausführungsform des erfindungsgemäßen Systems erfolgt die Beschränkung der von dem mobilen Gerät an das Service-Center übertragenen Sensordaten hinsichtlich eines Zeitpunktes der Erzeugung der Sensordaten durch den jeweiligen Sensor.

Bei einer weiteren möglichen Ausführungsform des erfindungsgemäßen Systems erfolgt die Beschränkung der von dem mobilen Gerät an das Service-Center übertragenen Sensordaten hinsichtlich der Komponente, die von dem Sensor sensorisch erfasst wird.

Die jeweilige Beschränkung der von dem mobilen Gerät an das Service-Center übertragenen Sensordaten erfolgt in jedem Falle in Abhängigkeit von der für das mobile Gerät bestehenden Autorisierung.

Bei einer möglichen Ausführungsform des erfindungsgemäßen Systems erfolgt die Authentisierung zwischen dem mobilen Ge-

rät und der Komponente mittels eines kryptographischen Authentisierungsverfahrens, insbesondere eines kryptographischen Challenge-Response-Verfahrens.

Bei einer möglichen Ausführungsform des erfindungsgemäßen Systems authentisiert sich das mobile Gerät oder ein Nutzer, der das mobile Gerät trägt, gegenüber dem Service-Center.

Bei einer möglichen Ausführungsform des erfindungsgemäßen Systems erfolgt die Authentisierung des Nutzers, welcher das mobile Gerät trägt, gegenüber dem Service-Center anhand von biometrischen Körpermerkmalen des Nutzers.

Bei einer weiteren möglichen Ausführungsform des erfindungsgemäßen Systems erfolgt die Authentisierung des Nutzers, welcher das mobile Gerät trägt, gegenüber dem Service-Center anhand der mittels eines Mikrofons sensorisch erfassten Sprache des Nutzers.

Bei einer möglichen Ausführungsform des erfindungsgemäßen Systems ist das mobile Gerät ein Fernwartungskommunikationsgerät , das von einem Wartungstechniker als Nutzer getragen wird und das den Zustand einer zu wartenden oder zu reparierenden Komponente mittels darin integrierter Sensoren erfasst.

Bei einer möglichen Ausführungsform des erfindungsgemäßen Systems werden die von dem mobilen Gerät über das Datennetzwerk an das Service-Center übertragenen Sensordaten des Zustandes der Komponente in dem Service-Center einem Experten zur Verfügung gestellt, welcher über das Datennetzwerk Instruktionen an den Nutzer, welcher das mobile Gerät trägt, zurück überträgt.

Bei einer möglichen Ausführungsform des erfindungsgemäßen Systems wird mittels des Nahfeld-Kommunikationsmoduls des mobilen Gerätes ein Tag, beispielsweise ein RFID-Tag, welches an der Komponente angebracht ist, drahtlos ausgelesen, wobei

in dem Tag eine Komponenten-ID der Komponente gespeichert sein kann.

Bei einer möglichen Ausführungsform des erfindungsgemäßen Systems ist in dem mobilen Gerät ein konfigurierbarer Zugriffskontrollspeicher vorgesehen, in welchem Komponenten-ID's von denjenigen Komponenten gespeichert sind, für welche der Nutzer des mobilen Gerätes autorisiert ist, eine bestimmte Wartungs- oder Reparaturmaßnahme durchzuführen.

Dabei werden vorzugsweise nur Sensordaten von denjenigen Komponenten von dem mobilen Gerät des Nutzers zu dem Service-Center übertragen, für welche der jeweilige Nutzer autorisiert ist.

Die Erfindung schafft ferner ein mobiles Fernwartungskommunikationsgerät mit den in Patentanspruch 14 angegebenen Merkmalen.

Die Erfindung schafft ein mobiles Fernwartungskommunikationsgerät zur Wartung einer Komponente, mit Sensoren, die Sensordaten über den Zustand der Komponente an ein Service-Center übertragen, falls das mobile Fernwartungskommunikationsgerät dazu autorisiert ist und zwischen dem mobilen Fernwartungskommunikationsgerät und der zu wartenden Komponente eine erfolgreiche Authentisierung erfolgt ist.

Die Erfindung schafft ferner ein Verfahren mit den in Patentanspruch 15 angegebenen Merkmalen.

Die Erfindung schafft ein Verfahren zum Bereitstellen von Sensordaten über einen Zustand einer Komponente für ein Service-Center durch Sensoren, die an einem dazu autorisierten mobilen Gerät vorgesehen sind, nachdem zwischen dem mobilen Gerät und der Komponente eine erfolgreiche Authentisierung erfolgt ist.

Im Weiteren werden bevorzugten Ausführungsformen des erfindungsgemäßen Systems, des erfindungsgemäßen Fernwartungskommunikationsgerät es sowie des erfindungsgemäßen Verfahrens zum Bereitstellen von Sensordaten unter Bezugnahme auf die beigefügten Figuren zur Erläuterung möglicher Ausführungsformen beschrieben.

Es zeigen:

Fig. 1 ein Blockschaltbild zur Darstellung einer möglichen Ausführungsform des erfindungsgemäßen Systems zum Bereitstellen von Sensordaten;

Fig. 2 ein mögliches Anwendungsszenario des erfindungsgemäßen Systems zur Bereitstellung von Sensordaten;

Fig. 3 ein Ablaufdiagramm zur Darstellung einer möglichen Ausführungsform des erfindungsgemäßen Verfahrens zum Bereitstellen von Sensordaten;

Fig. 4A, 4B Ablaufdiagramme zur Darstellung eines weiteren Ausführungsbeispiels des erfindungsgemäßen Verfahrens zum Bereitstellen von Sensordaten.

Wie man aus Fig. 1 erkennen kann, umfasst ein erfindungsgemäßes System 1 zum Bereitstellen von Sensordaten ein Datennetzwerk 2, über das ein mobiles Gerät 3 mit einem Server 4 eines Service-Centers SC eine Kommunikationsverbindung aufbauen kann. Bei dem mobilen Gerät 3 handelt es sich beispielsweise um ein Fernwartungskommunikationsgerät eines Nutzers, beispielsweise eines Wartungstechnikers 5. Der Nutzer 5 trägt das mobile Gerät 3 mit sich, um an einer Komponente 6 eine Servicemaßnahme durchzuführen. Bei dieser Servicemaßnahme handelt es sich beispielsweise um eine Wartungs- oder Reparaturmaßnahme. An dem Service-Center SC kann ein Terminal 7 angeschlossen sein, über das ein Mitarbeiter des Service-

Centers SC, beispielsweise ein technischer Experte 8, mit dem mobilen Gerät 3 des Nutzers 5 kommuniziert.

Bei dem in Fig. 1 dargestellten Ausführungsbeispiel weist das mobile Gerät 3 eine Netzwerkschnittstelle 3A auf, um eine Kommunikationsverbindung mit dem Datennetzwerk 2 herzustellen. Bei der Netzwerkschnittstelle 3A kann es sich um eine drahtgebundene oder drahtlose Schnittstelle handeln. Vorzugsweise ist die Schnittstelle 3A eine drahtlose Schnittstelle, damit der Nutzer 5 das mobile Gerät 3 problemlos mit sich führen bzw. an seinem Körper tragen kann. Das mobile Gerät 3 verfügt über eine Nutzerschnittstelle 3B, die von dem Nutzer 5 bedient werden kann. Die Netzwerkschnittstelle 3A sowie die Nutzerschnittstelle 3B sind mit einer Datenverarbeitungseinheit 3C des mobilen Gerätes 3 verbunden. Die Datenverarbeitungseinheit 3C des mobilen Gerätes 3 kann einen oder mehrere Mikroprozessoren zur Ausführung eines Steuerprogramms aufweisen. Die Datenverarbeitungseinheit 3C hat Zugriff auf einen Datenspeicher 3D, in dem Daten abspeicherbar sind. Ferner sind bei dem in Fig. 1 dargestellten Ausführungsbeispiel Sensoren mit der Datenverarbeitungseinheit 3C verbunden. Beispielsweise verfügt das mobile Gerät 3 über eine Kamera 3E, die Bild- oder Videodaten an die Datenverarbeitungseinheit 3C liefert. Weiterhin kann das mobile Gerät 3 über ein Mikrofon 3F verfügen, das Geräuschdaten der Komponente 6 liefert.

Darüber hinaus verfügt das mobile Gerät 3 gemäß der Erfindung über ein Nahfeld-Kommunikationsmodul 3G mittels dessen sich das mobile Gerät 3 gegenüber der Komponente 6 authentisiert oder mittels dessen sich die Komponente 6 gegenüber dem mobilen Gerät 3 authentisiert. Bei einer möglichen Ausführungsform ist an der Komponente 6, beispielsweise einer Maschinenkomponente, ein Tag 9 angebracht, welches mittels des Nahfeld-Kommunikationsmoduls 3G des mobilen Gerätes 3 drahtlos auslesbar ist. Auf dem Tag 9 der Komponente 6 kann beispielsweise eine Komponenten-ID der Komponente 6 abgespeichert sein und ausgelesen werden. Bei einer möglichen Ausführungsform handelt es sich bei dem Tag 9 um ein RFID-Tag, das durch ein

in dem mobilen Gerät 3 integriertes RFID-Lesegerät als Nahfeld-Kommunikationsmodul 3G auslesbar ist. Bei dieser Ausführungsform des mobilen Gerätes 3 ist somit das Nahfeld-Kommunikationsmodul 3G ein RFID-Kommunikationsmodul bzw. ein RFID-Lesegerät. Bei einer alternativen Ausführungsform weist das Nahfeld-Kommunikationsmodul 3G des mobilen Gerätes 3 ein Bluetooth-Kommunikationsmodul, ein ZigBee-Kommunikationsmodul oder ein IEEE802.15.4-Kommunikationsmodul auf.

Bei einer möglichen Ausführungsform ist das mobile Gerät 3 ein Fernwartungskommunikationsgerät mit einer integrierten RFID-Leseeinheit 3G, die über ein Funkprotokoll zur Nahfeld-Kommunikation mit dem RFID-Tag 9 kommuniziert, das in der zu wartenden oder der zu reparierenden Komponente 6 eingebaut sein kann. Bei dem RFID-Tag 9 handelt es sich vorzugsweise um ein passives RFID-Tag. Bei einer möglichen Ausführungsform wird das RFID-Tag 9 in regelmäßigen Zeitabständen von dem Fernwartungskommunikationsgerät 3 abgefragt.

Bei einer weiteren möglichen Ausführungsform authentisiert sich das RFID-Tag 9 in regelmäßigen Zeitabständen gegenüber dem mobilen Gerät 3 über ein kryptographisches Authentisierungsverfahren, beispielsweise über ein kryptographisches Challenge-Response-Protocol. Kann die vom RFID-Tag 9 gelieferte Response nicht verifiziert werden, so wird die Kommunikation zwischen dem Nahfeld-Kommunikationsmodul 3G und dem Tag 9 für einen längeren Zeitraum unterbrochen und es kann eine Beschränkung der von dem mobilen Gerät 3 an das Service-Center 4 übertragenen Sensordaten erfolgen. Die Beschränkung kann in einer vollständigen Unterbindung der übertragenen Sensordaten bestehen oder sogar in einem vollständigen Abschalten des mobilen Gerätes 3.

Nachdem eine erfolgreiche Authentisierung zwischen dem Nahfeld-Kommunikationsmodul 3G des mobilen Gerätes 3 und dem Tag 9 der zu wartenden oder zu reparierenden Komponente 6 erfolgt ist, kann das mobile Wartungsgerät 3 für die Übertragung von Sensordaten an das entfernte Service-Center 4 freigeschaltet

werden. Nach Aufbau der Kommunikationsverbindung zu dem Service-Center 4 kann sich der Nutzer 5, der sich vor Ort bei der zu wartenden Komponente 6 befindet, bei dem Service-Center-Betreiber über das Datennetzwerk 2 anmelden. Bei einer möglichen Ausführungsform stellt die Netzwerkschnittstelle 3A eine Funkverbindung zu einer Basisstation eines Zugangsnetzwerkes her, das seinerseits über ein oder mehrere Datennetzwerke mit dem Service-Center 4 verbunden ist.

Bei einer möglichen Ausführungsform muss sich der Nutzer 5 bzw. der Wartungstechniker gegenüber dem Service-Center 4 authentisieren bevor Sensordaten an das Service-Center 4 übertragen werden können. Diese Authentisierung des Nutzers 5 gegenüber dem Service-Center 4 kann bei einer möglichen Ausführungsform anhand von geometrischen Körpermerkmalen des Nutzers 5 erfolgen. Bei einer weiteren möglichen Ausführungsform erfolgt die Authentisierung des Nutzers 5 gegenüber dem Service-Center 4 anhand von sensorisch erfassten Sprachdaten des Nutzers 5. Beispielsweise erfolgt innerhalb des mobilen Gerätes 3 zunächst eine Sprecherverifikation des Wartungstechnikers 5, der in ein Mikrofon der Nutzerschnittstelle 3B spricht. Alternativ kann die Sprecherverifikation kann auch in dem Service-Center 4 anhand übertragenen Sprachdaten erfolgen. Bei einer weiteren möglichen Ausführungsform erfolgt die Authentisierung des Nutzers 5 gegenüber dem Service-Center 4 anhand eines Fingerprints oder anhand eines Iris-Scan. Bei einer möglichen Ausführungsform hat der Nutzer 5 seine biometrischen Daten in einem sogenannten Enrollement-Verfahren bei dem Betreiber des Service-Centers 4 hinterlegt. Weiterhin kann eine Security-Association zwischen dem mobilen Gerät 3 und dem Service-Center 4 aufgebaut sein, beispielsweise eine VPN- oder UMTS-Security-Association. Hierüber können sowohl die biometrischen Authentisierungsdaten für die Authentisierung des Nutzers 5 gegenüber dem Service-Center 4 als auch Autorisierungsdaten abhör- und fälschungssicher übertragen werden. Die Autorisierungsdaten können mögliche Beschränkungen bei der Übertragung der Sensordaten von dem mobilen Gerät 3 an das Service-Center 4 angeben. Hat sich der

Nutzer 5 gegenüber dem Service-Center 4 erfolgreich authentisiert, so kann die Autorisierung des Mitarbeiters bzw. Nutzers 5 vor Ort stattfinden. Dabei kann ein hinterlegtes Zugriffsprofil, welches beispielsweise Zugriffsrechte oder Zugriffsrollen umfasst, mit dem von dem Nutzer 5 gewünschten an der Komponente 6 zu erbringenden Service bzw. Dienstleistung abgeglichen werden, wobei die Erbringung des gewünschten Dienstes erlaubt oder abgebrochen werden kann. Dabei können neben der verifizierten Identität optional weitere Daten von dem autorisierten Dienst ausgewertet werden, beispielsweise eine ID des mobilen Gerätes 3, eine ID der zu wartenden Komponente 6, eine gewünschte Kontaktperson bzw. Experte sowie eine gewünschte Verbindungsart, beispielsweise Audio, Video oder Einzelbild. Ferner ist es möglich, dass Integritätsmerkmale des mobilen Endgerätes 3 verifiziert werden, beispielsweise durch Überprüfung von Softwaresignaturen einer RFID-Lesesoftware.

Bei der in Fig. 1 dargestellten Ausführungsform ist das Tag 9 an der zu wartenden Komponente 6 angebracht und wird durch ein Nahfeld-Kommunikationsmodul 3G, beispielsweise ein RFID-Lesegerät, ausgelesen. Bei einer alternativen Ausführungsform verfügt das mobile Gerät 3 über ein Tag, beispielsweise ein RFID-Tag und die zu wartende Maschinenkomponente 6 weist ein RFID-Lesegerät auf. Bei dieser Ausführungsform ist die zu wartende Maschinenkomponente 6 über eine Fernwartungsdatenverbindung an das Service-Center 4 angeschlossen. Bei dieser Ausführungsform wird das mobile Gerät 3 des Servicetechnikers 5 ebenfalls mit dem Service-Center 4, beispielsweise einer Wartungszentrale, verbunden und der Service-Techniker 5 authentisiert sich gegenüber dem Service-Center 4 beispielsweise mittels eines biometrischen Authentisierungsverfahrens.

Kommt bei dieser Ausführungsform der Servicetechniker 5 mit seinem tragbaren mobilen Gerät 5 in die räumliche Nähe der Komponente 6, kann das RFID-Tag des mobilen Gerätes 3 ausgelesen bzw. authentisiert werden. Ist bei dieser Ausführungsform die empfangene ID des mobilen Gerätes 3, die in dem

Speicher 3D abgelegt sein kann, in der zu wartenden Anlage bzw. Maschinenkomponente 6 als zugriffsberechtigt administriert, kann ein Kommunikationsmodul der zu wartenden Anlage über die separate Wartungsverbindung diese Informationsdaten an das Service-Center 4 bzw. das Wartungszentrum übertragen. Wenn das mobile Gerät 3 des Servicetechnikers 5 ebenfalls mit dem Service-Center 4 verbunden ist, kann bei dieser Ausführungsform das Wartungszentrum 4 einen oder mehrere Sensoren des mobilen Gerätes 3, beispielsweise die Kamera 3E, freigeben.

Bei einer weiteren möglichen Ausführungsform empfängt das mobile Gerät 3 des Servicetechnikers 5 über das Datennetzwerk 2 ein sogenanntes Ticket (Kerberos, SAML: Security Assertion Markup Language), in welchem Informationsdaten zu den zu wartenden Komponenten bzw. Geräten 6 sowie eine Technikerkennung enthalten sein kann. Das Ticket kann beispielsweise eine Geräte- bzw. Komponenten-ID der zu wartende Komponente 6 enthalten. Bei einer möglichen Ausführungsform wird das Ticket von dem mobilen Gerät 3 angefordert. Alternativ kann das Ticket über einen existierenden Übertragungskanal gesendet, und lokal per Drahtlosverbindung an das mobile Gerät 3 übermittelt werden. Auf dem mobilen Gerät 3 wird dazu das empfangene Ticket mit einer lokalen Authentisierung des Servicetechnikers 5 sowie der empfangenen Komponenten-ID verglichen. Bei Übereinstimmung der Rechte und erfolgreiche Authentisierung wird ein Zugriff auf einen Sensor, beispielsweise die Kamera 3E, freigeschaltet.

Bei den bisher beschriebenen Ausführungsvarianten erfolgt die Authentisierung zwischen dem mobilen Gerät 3 und der Komponente 6 mittels eines Nahfeld-Kommunikationsmoduls bzw. durch Kommunikation zwischen einem RFID-Lesegerät und einem RFID-Tag. Bei alternativen Ausführungsformen kann die Authentisierung zwischen dem mobilen Gerät 3 und der Komponente 6 mittels anderer Verfahren erfolgen, beispielsweise durch einen Abgleich von Ortskoordinaten eines aktuellen Aufenthaltsortes des mobilen Gerätes 3 und einem Aufstellungsort der zu war-

tenden Komponente 6. Bei einer möglichen Ausführungsform weist hierzu das mobile Gerät 3 ein GPS-Modul auf, über das es lokalisiert werden kann. Stimmen die Raumkoordinaten des mobilen Gerätes 3 annähernd mit den Raumkoordinaten der zu wartenden bzw. zu reparierenden Komponente 6 überein, die beispielsweise anhand der Komponenten-ID identifiziert ist, befindet sich der Servicetechniker 5 bei der richtigen Komponente 6 und der Authentisierungsvorgang ist erfolgreich abgeschossen. Ferner kann auch eine Lokalisierung des mobilen Gerätes 3 mittels WLAN oder Triangulation erfolgen.

Bei dem in Fig. 1 dargestellten Ausführungsbeispiel verfügt das mobile Gerät 3 über zwei Sensoren 3E, 3F zur Übertragung von Sensordaten an das Service-Center 4. Durch die Kamera 3E können Bild- oder Videodaten der Komponente 6 übertragen werden. Bei der Komponente 6 kann es sich beispielsweise um eine Turbinenschaufel einer Turbine handeln. In einer derartigen Turbinenschaufel können beispielsweise Haarrisse entstehen. Der Servicetechniker 5 kann auf diese Weise ein Bild über den Zustand der Turbinenschaufel visuell an einen im Service-Center 4 befindlichen Mitarbeiter bzw. Experten übertragen. Bei dem in Fig. 1 dargestellten Ausführungsbeispiel ist die Kamera 3E über eine drahtgebundene Schnittstelle mit der Datenverarbeitungseinheit 3C des mobilen Gerätes 3 verbunden. Bei einer möglichen Ausführungsform ist die Kamera 3E des mobilen Gerätes 3 über eine drahtlose Schnittstelle mit dem mobilen Gerät 3 verbunden.

Sobald der Experte 8 in dem Service-Center 4 die Bilddaten von der zu wartenden Turbinenschaufel 6 erhält, kann er dem Servicetechniker 5 vor Ort Instruktionen über das Datennetzwerk 2 geben. Diese Instruktionen können beispielsweise Sprachbefehle sein. Weiterhin ist es möglich, dass der Experte 8 im Service-Center 4 auf eine Datenbank zugreift und dem Servicetechniker 5 Daten, die Informationen über die zu wartende Komponente 6 enthalten, überträgt, beispielsweise Baupläne oder Geometriedaten der Turbinenschaufel 6. Derartige

Daten können beispielsweise auf einem Display des mobilen Gerätes 3 dem Servicetechniker 5 angezeigt werden.

Bei einer möglichen Ausführungsform trägt der Servicetechniker ein Headset, an dem die Kamera 3E angebracht ist. Weiterhin kann an dem Headset ein Mikrofon der Nutzerschnittstelle 3B angebracht sein, über das der Nutzer 5 mit dem Experten 8 kommunizieren kann, beispielsweise indem er entsprechende Fragen stellt. Das mobile Gerät 3 kann, wie in Fig. 1 dargestellt, ferner ein Mikrofon 3F aufweisen, mit dem Geräuschdaten der zu wartenden Maschinenkomponente 6 aufgenommen werden. Bei einer möglichen Ausführungsform werden die aufgezeichneten Bild-, Video- und Audiodaten zusätzlich in dem lokalen Speicher 3D des mobilen Gerätes 3 zur späteren Auswertung aufgezeichnet. Zur Speicherung der Daten kann alternativ oder zusätzlich auch an dem Service-Center 4 erfolgen.

Bei einer möglichen Ausführungsform verfügt das mobile Gerät 3 neben dem Datenspeicher 3D über einen konfigurierbaren Zugriffskontrollspeicher, bei welchem verschiedene Komponenten-ID's von denjenigen Komponenten 6 gespeichert sind, für welche der Service-Techniker bzw. Nutzer 5 des jeweiligen mobilen Gerätes 3 autorisiert ist, eine Wartungs- oder Reparaturmaßnahme durchzuführen. Bei dieser Ausführungsform werden nur Sensordaten von denjenigen Komponenten 6 von dem mobilen Gerät 3 des Nutzers 5 zu dem Service-Center 4 übertragen, für welche der Nutzer 5 autorisiert ist bzw. die entsprechenden Übertragungsrechte besitzt.

Die Beschränkung der von dem mobilen Gerät 3 an das Service-Center 4 übertragenen Sensordaten kann entsprechend der bestehenden Autorisierung des jeweiligen Service-Technikers 5 unterschiedlich erfolgen. Einerseits kann die Beschränkung der übertragenen Sensordaten hinsichtlich deren Art erfolgen. Beispielsweise kann ein bestimmter Servicetechniker 5 von einer bestimmten Maschinenkomponente 6 nur Geräuschdaten aber keine Bilddaten übertragen.

Weiterhin kann die Beschränkung der übertragenen Sensordaten hinsichtlich eines aktuellen Aufenthaltsortes des mobilen Gerätes 3 stattfinden. Beispielsweise darf das mobile Gerät 3 nur sensorisch erfasste Daten an das Service-Center 4 übertragen, sofern es sich in einem bestimmten Gebiet befindet oder in der Nähe einer bestimmten Maschinenkomponente 6, beispielsweise in einem Umkreis von 10m.

Weiterhin kann die Beschränkung der übertragenen Sensordaten hinsichtlich eines Zeitpunktes der Erzeugung der Sensordaten durch den Sensor erfolgen. Beispielsweise darf ein Servicetechniker 5 nur Sensordaten übertragen, die er während eines bestimmten Zeitraumes erzeugt, beispielsweise während der Öffnungszeiten des Betriebes oder Unternehmens, in dem die Maschinenkomponente 6 steht.

Weiterhin kann die Beschränkung der übertragenen Sensordaten hinsichtlich der Komponente 6 erfolgen, die durch den Sensor sensorisch erfasst wird. Beispielsweise darf der Servicetechniker 5 nur Sensordaten einer Maschinenkomponente mit einer bestimmten Maschinenkomponenten-ID an das Service-Center 4 übertragen.

Nähert sich der Servicetechniker 5 mit dem mobilen Gerät 3 beispielsweise zu einer verbotenen geheimen Maschinenkomponente 6 kann bei einer möglichen Ausführungsform das mobile Gerät 3 automatisch deaktiviert werden. Auf diese Weise ist dem Anlagenbetreiber die Möglichkeit gegeben, zu definieren, welche Maschinenkomponenten 6 der Anlage mit einem Fernwartungskommunikationsgerät 3 gewartet werden dürfen und für welche Maschinenkomponenten dies nicht erlaubt ist. Hierdurch kann die Sicherheit gegenüber ungewollter Verbreitung von Betriebsgeheimnissen erhöht werden. Die Beschränkung der Übertragung der Sensordaten durch das mobile Endgerät 3 sowie des zugelassenen Benutzerkreises als auch die räumliche Ausdehnung eines möglichen Einsatzes des mobilen Gerätes 3 ermöglicht den Einsatz eines mobilen Fernwartungskommunikationsgerät es zur Audio- und Videoübertragung an ein entferntes Ser-

vice-Center 4 ohne die Sicherheit beim Schutz firmeninterner Daten zu reduzieren.

Bei einer möglichen Ausführungsform ist die zulässige Reichweite für eine erfolgreiche Authentisierung zwischen dem mobilen Gerät 3 und der zu wartenden Komponente 6 einstellbar. Beispielsweise kann die zulässige Reichweite Millimeter oder einige Zentimeter oder einige Meter betragen. Für diese Ausführungsform ist ein zulässiger Arbeitsbereich des Servicetechnikers 5 flexibel einstellbar.

Die Fig. 2 zeigt ein Anwendungsszenario für das erfindungsgemäße System 1. Bei diesem Anwendungsszenario befindet sich ein Servicetechniker 5 mit seinem mobilen Gerät 3 in der Anlage eines Anlagenbetreibers beispielsweise in der Nähe einer zu wartenden Komponente 6, die über ein lokales Netzwerk und einen Zugangsrouter (Access Router) über das Internet mit einem Service-Center 4 verbunden ist. Ein Experte 8 sitzt an einem Terminal 7, das an einem lokalen Netzwerk des Service-Center-Betreibers angeschlossen ist. Über ein Zugangsportal und einen Firewall FW ist dieses lokale Netzwerk des Service-Centers 4 ebenfalls mit dem Internet 2 verbunden. Zwischen einem Zugangsserver (Access Server) des Service-Centers 4 und dem Zugangsrouter des Kundennetzwerkes kann ein Remote-Servicezugang, beispielsweise ein VPN-Tunnel aufgebaut sein, der eine sichere Datenübertragung zwischen dem Service-Center 4 und dem mobilen Gerät 3 des Nutzers 5 erlaubt. Bei einer möglichen Ausführungsform ist das mobile Gerät 3 in einem Kleidungsstück des Nutzers 5 integriert. Beispielsweise ist das mobile Gerät 3 an einer Mütze oder Kappe oder einem Helm des Nutzers 5 integriert und überträgt über eine drahtlose Schnittstelle Sensordaten über den VPN-Tunnel an das Netzwerk des Service-Centers 4.

Bei einer möglichen Ausführungsform sind, wie in Fig. 2 dargestellt, an das Datennetzwerk 2 bzw. das Internet weitere Service-Center bzw. Dienstleistungsanbieter angeschlossen. Bei einer möglichen Ausführungsform werden die von dem mobi-

len Gerät 3 gelieferten Sensordaten je nach Bedarf an verschiedene Service-Center SC geroutet. Beispielsweise kann das Routing der Sensordaten in Abhängigkeit der jeweiligen zu wartenden Maschinenkomponente 6 erfolgen.

Bei einer möglichen Ausführungsform authentisiert sich nicht nur der Servicetechniker 5 gegenüber dem Service-Center 4, sondern auch ein Mitarbeiter des Service-Centers 4 gegenüber dem vor Ort befindlichen Servicetechniker 5, um die Sicherheit gegenüber Fehlweisungen bzw. Missverständnissen zu erhöhen. Erst nach gegenseitiger Authentisierung erfolgt dann eine Übertragung der Sensordaten an das Service-Center 4 und eine Zurückübertragung entsprechender Serviceinstruktionen durch den Mitarbeiter 8 des Service-Centers 4 an den Nutzer 5 bzw. den Servicetechniker.

Fig. 3 zeigt ein Ablaufdiagramm einer möglichen Ausführungsform des erfindungsgemäßen Verfahrens zum Bereitstellen von Sensordaten. Bei der in Fig. 3 dargestellten Ausführungsvariante befindet sich das Tag 9 an der zu wartenden Maschinenkomponente 6. Bei dieser Variante erfolgt die Freischaltung eines Sensors, beispielsweise der Kamera 3E in Abhängigkeit einer empfangenen RFID-Kennung des Tags 9. Bei dieser Ausführungsvariante ist in dem mobilen Endgerät 3 eine Liste mit Gerätekennungen bzw. Komponentenkennungen verfügbar, welche angibt, welche Komponenten 6 durch das mobile Gerät 3 aufgenommen werden dürfen.

Nach einem Startschritt S0 wird zunächst in einem Schritt S1 geprüft, ob das Tag 9 sich in der Reichweite des Nahfeld-Kommunikationsmoduls 3G des mobilen Gerätes 3 befindet. Ist dies der Fall wird in einem Schritt S2 geprüft, ob sich die Kennung der Komponente 6, die aus dem Tag 9 ausgelesen wird, in der Zugriffskontrollliste befindet. Ist dies der Fall, erfolgt eine Authentisierung in einem Schritt S3 über das RFID-Tag 9. In einem weiteren Schritt S4 wird entschieden, ob die Authentisierung erfolgreich abgeschlossen worden ist. Nach erfolgreicher Authentisierung der Maschinenkomponente 6 ge-

genüber dem mobilen Gerät 3 erfolgt beispielsweise in einem Schritt S5 ein lokales Freischalten eines in dem mobilen Gerät 3 befindlichen Sensors, beispielsweise der Kamera 3E. Ferner wird ein Verbindungsaufbau zum Aufbau einer Kommunikationsverbindung zu dem Service-Center 4 im Schritt S5 durchgeführt. Falls der Sensor freigeschaltet wird, kann in einem Schritt S6 die Verbindung zu dem Service-Center 4 aufgebaut werden. Weiterhin wird in einem Schritt S7 beispielsweise ein VPN-Tunnel zur sicheren Datenübertragung gebildet. Sobald die Verbindung zu dem Service-Center 4 besteht, wird vorzugsweise eine Nutzer-Authentisierung durchgeführt. In dem Schritt S8 authentisiert sich dabei der Servicetechniker 5, beispielsweise durch biometrische Verfahren, gegenüber dem Service-Center 4. In einem Schritt S9 wird entschieden, ob die Authentisierung erfolgreich abgeschlossen worden ist. Nach erfolgreicher Nutzer-Authentisierung werden die von dem Sensor, beispielsweise der Kamera 3E gelieferten Sensordaten im Schritt S10 an das Service-Center 4 übertragen.

Die Fig. 4A, 4B zeigen Ablaufdiagramme zur Darstellung einer weiteren Ausführungsvariante des erfindungsgemäßen Verfahrens. Bei dieser Variante befindet sich das Nahfeld-Kommunikationsmodul, beispielsweise ein RFID-Lesegerät, an der zu wartenden Komponente 6 und ein entsprechendes Tag befindet sich an dem mobilen Gerät 3. Der in Fig. 4A dargestellte Ablauf erfolgt auf Seiten der zu wartenden Komponente 6. Der in Fig. 4B dargestellte Ablauf erfolgt auf Seiten des Fernwartungskommunikationsgerätes 3.

Wie in Fig. 4A dargestellt, erfolgt nach einem Start der Wartungsmaßnahme im Schritt S0 durch das in der Komponente 6 befindliche Lesegerät eine Überprüfung, ob sich ein RFID-Tag eines mobilen Fernwartungskommunikationsgerätes 3 in seiner Reichweite an ist. Ist dies der Fall, erfolgt im Schritt S3 eine Authentisierung über das RFID-Tag. Wird im Schritt S4 entschieden, dass die Authentisierung erfolgreich abgeschlossen ist, kann in einem Schritt S5 eine Kennung bzw. ID des mobilen Gerätes 3 über eine existierende separate Wartungs-

verbindung der Maschinenkomponente 6 zu dem Service-Center 4 übertragen werden.

Wie in Fig. 4B dargestellt, wird bei der auf dem Wartungsgerät 3 ablaufenden Prozedur zunächst eine Verbindung von dem mobilen Gerät 3 zu dem Service-Center 4 im Schritt S0 aufgebaut. Weiterhin wird in einem Schritt S1 vorzugsweise ein VPN-Tunnel zu dem Service-Center 4 gebildet. Anschließend authentisiert sich der Servicetechniker 5, beispielsweise durch ein biometrisches Verfahren, gegenüber dem Service-Center 4 im Schritt S2. Wird im Schritt S3 erkannt, dass die Authentisierung erfolgreich abgeschlossen ist, werden in einem Schritt S4 die Zugriffsrechte des Servicetechnikers 5 mit Hilfe der empfangenen ID im Schritt S4 abgeglichen. Schließlich erfolgt im Schritt S5 eine Freischaltung des Sensors, beispielsweise der Kamera 3E durch das Service-Center 4. Der Abgleich der Zugriffsrechte im Schritt S4 kann beispielsweise an dem Service-Center 4 erfolgen.

Das erfindungsgemäße System 1 erlaubt die Bereitstellung von universell einsetzbaren Endgeräten bzw. Fernwartungskommunikationsgeräten 3 zur Audio- und Videoübertragung, beispielsweise mit Hilfe hochauflösender Kameras, auf einem Kommunikationskanal über eine Betriebs- bzw. Firmengrenze hinweg. Das erfindungsgemäße System 1 minimiert ein potentielles Sicherheitsrisiko für zu schützende, firmeninterne Daten. Das erfindungsgemäße System 1 eignet sich zur Fernwartung oder Ferndiagnose bei beliebigen Komponenten 6, insbesondere Maschinenkomponenten.

Bei den Sensoren kann es sich ebenfalls um verschiedene Arten von Sensoren handeln, insbesondere Video- oder Audiosensoren. Darüber hinaus können die Sensoren des mobilen Gerätes 3 auch physikalische Parameter der Komponente 6 erfassen, beispielsweise Temperatur, Druck etc.#

Bei den oben beschriebenen Ausführungsbeispielen sind die Sensoren Videosensoren bzw. Mikrofone oder Kameras, die Au-

dio- bzw. Videodaten liefern. Bei einer weiteren möglichen Ausführungsform können die Sensoren des mobilen Gerätes 3 auch an die zu wartende Komponente 6 angebracht oder sogar an die zu wartende Komponente 6 angeschlossen werden. Weiterhin kann es sich bei den Sensoren 6 um nicht invasive Sensoren aber auch um invasive Sensoren handeln. Beispielsweise können die Sensoren auch in die zu wartende Komponente 6 eingeführt werden. Beispielsweise kann es sich bei der zu wartenden Komponente 6 auch um einen chemischen Stoff handeln, in den ein Sensor eingeführt wird. Dieser Sensor kann dann Daten über die chemische Zusammensetzung oder physikalische Eigenschaften des jeweiligen Stoffes liefern. Bei einer möglichen Ausführungsform handelt es sich bei dem Sensor um eine Sonde, die in die Komponente 6 bzw. im Stoff eingeführt wird.

Bei der Komponente 6 kann es sich um eine stationär aufgestellte Komponente, beispielsweise eine Maschinenkomponente handeln, aber auch um eine bewegliche Komponente, beispielsweise ein mobiles Gerät. Bei diesem mobilen Gerät kann es sich beispielsweise auch um ein Transportfahrzeug handeln.

Bei einer möglichen Ausführungsform umfassen die Sensoren des mobilen Fernwartungskommunikationsgerätes 3 gleichzeitig mehrere Komponenten gleichzeitig. Diese Komponenten 6 können verschiedene Tags, insbesondere RFID-Tags aufweisen, in denen verschiedene Komponenten-ID's abgespeichert sind. Bei einer weiteren möglichen Ausführungsform kommuniziert das mobile Gerät 3 direkt mit dem Service-Center 4 über eine entsprechende Funkverbindung, ohne dass ein Datennetzwerk 2, beispielsweise das Internet dafür notwendig ist.

Patentansprüche

1. System (1) zum Bereitstellen von Sensordaten über einen Zustand einer Komponente (6) für ein Service-Center (4) durch mindestens einen Sensor (3E, 3F), der an einem dazu autorisierten mobilen Gerät (3) vorgesehen ist, nachdem zwischen dem mobilen Gerät (3) und der Komponente (6) eine erfolgreiche Authentisierung erfolgt ist.

2. System nach Anspruch 1,
wobei das mobile Gerät (3) ein Nahfeld-Kommunikationsmodul (3G) aufweist, mittels dessen sich das mobile Gerät (3) gegenüber der Komponente (6) authentisiert oder mittels dessen sich die Komponente (6) gegenüber dem mobilen Gerät (3) authentisiert.

3. System nach Anspruch 1 oder 2,
wobei das mobile Gerät (3) eine Netzwerkschnittstelle (3A) aufweist, die zum Aufbau einer Kommunikationsverbindung mit dem Service-Center (4) über ein Datennetzwerk (2) vorgesehen ist.

4. System nach Ansprüchen 1-3,
wobei die Sensoren (3)
eine Kamera (3E), die Bild- oder Videodaten der Komponente und/oder deren Umgebung liefert,
ein erstes Mikrofon (3F), das Geräuschdaten der Komponente erfasst, ein zweites Mikrofon, das Sprachdaten eines Nutzers (5) erfasst, welcher das mobile Gerät (3) trägt, und Sensoren, die physikalische Parameter der Komponente (6) erfassen, aufweisen.

5. System nach Ansprüchen 1-4,
wobei die von dem Sensor (3E, 3F) des mobilen Geräts (3) bereitgestellten Sensordaten entsprechend der Autorisierung des mobilen Gerätes (3) beschränkt von dem mobilen Gerät (3) an das Service-Center (4) übertragen werden.

6. System nach Anspruch 5,
wobei die Beschränkung der von dem mobilen Gerät (3) an das Service-Center (4) übertragenen Sensordaten hinsichtlich der Art der Sensordaten, welche Bilddaten, Videodaten, Geräuschdaten und Sprachdaten umfassen, erfolgt oder
hinsichtlich eines aktuellen Aufenthaltsortes des mobilen Gerätes (3) oder
hinsichtlich eines Zeitpunktes der Erzeugung der Sensordaten durch den Sensor (3E, 3F) oder
hinsichtlich der Komponente, die durch den Sensor (3E, 3F) sensorisch erfasst wird,
in Abhängigkeit von der für das mobile Gerät (3) bestehenden Autorisierung erfolgt.

7. System nach Ansprüchen 1-6,
wobei die Authentisierung zwischen dem mobilen Gerät (3) und der Komponente (6) mittels eines kryptographischen Challenge-Response-Verfahrens erfolgt.

8. System nach Ansprüchen 1-7,
wobei das mobile Gerät (3) oder ein Nutzer (5), der das mobile Gerät (3) trägt, sich gegenüber dem Service-Center (4) authentisiert.

9. System nach Anspruch 8,
wobei die Authentisierung des Nutzers (5), welcher das mobile Gerät (3) trägt, gegenüber dem Service-Center (4) anhand von biometrischen Körpermerkmalen des Nutzers (5) oder anhand von sensorisch erfasster Sprache des Nutzers (5) erfolgt, wobei die Körpermerkmale oder die sensorisch erfasste Sprache von dem mobilen Gerät (3) über das Datennetzwerk (2) an das Service-Center (4) übertragen werden.

10. System nach Ansprüchen 1-9,
wobei das mobile Gerät (3) ein Fernwartungskommunikationsgerät ist, das von einem Wartungstechniker als Nutzer

(5) getragen wird und das den Zustand einer zu wartenden oder zu reparierenden Komponente (6) mittels darin integrierter Sensoren (3E, 3F) erfasst.

11. System nach Ansprüchen 1-10,
wobei die von dem mobilen Gerät (3) über das Datennetzwerk (2) an das Service-Center (4) übertragenen Sensordaten des Zustandes der Komponente (6) in dem Service-Center (4) einem Experten (8) zur Verfügung gestellt werden, welcher über das Datennetzwerk (2) Instruktionen an den Nutzer (5), welcher das mobile Gerät (3) trägt, zurück überträgt.

12. System nach Ansprüchen 2-11,
wobei mittels des Nahfeld-Kommunikationsmoduls (3G) des mobilen Gerätes (3) ein Tag (9), welches an der Komponente (6) angebracht ist, drahtlos auslesbar ist, wobei in dem Tag (9) eine Komponenten-ID der Komponente (6) gespeichert ist.

13. System nach Ansprüchen 1-12,
wobei in dem mobilen Gerät (3) ein konfigurierbarer Zugriffskontrollspeicher vorgesehen ist, in welchem die Komponenten-ID's von denjenigen Komponenten gespeichert sind, für welche der Nutzer (5) des mobilen Gerätes (3) autorisiert ist eine Wartungs- oder Reparaturmaßnahme durchzuführen,
wobei nur Sensordaten von denjenigen Komponenten (6) von dem mobilen Gerät (3) des Nutzers (5) zu dem Service-Center (4) übertragen werden, für welche der jeweilige Nutzer (5) autorisiert ist.

14. Mobiles Fernwartungskommunikationsgerät (3) zur Wartung einer Komponente (6), mit Sensoren (3), die Sensordaten über den Zustand der Komponente (6) an ein Service-Center (4) übertragen, falls das mobile Fernwartungskommunikationsgerät (3) dazu autorisiert ist und zwischen dem mobilen Fernwartungskommunikationsgerät (3) und der zu war-

tenden Komponente (6) eine erfolgreiche Authentisierung erfolgt ist.

15. Verfahren zum Bereitstellen von Sensordaten über einen Zustand einer Komponente (6) für ein Service-Center (4) durch Sensoren (3E, 3F), die an einem dazu autorisierten mobilen Gerät (3) vorgesehen sind, nachdem zwischen dem mobilen Gerät (3) und der Komponente (6) eine erfolgreiche Authentisierung erfolgt ist.

FIG 1

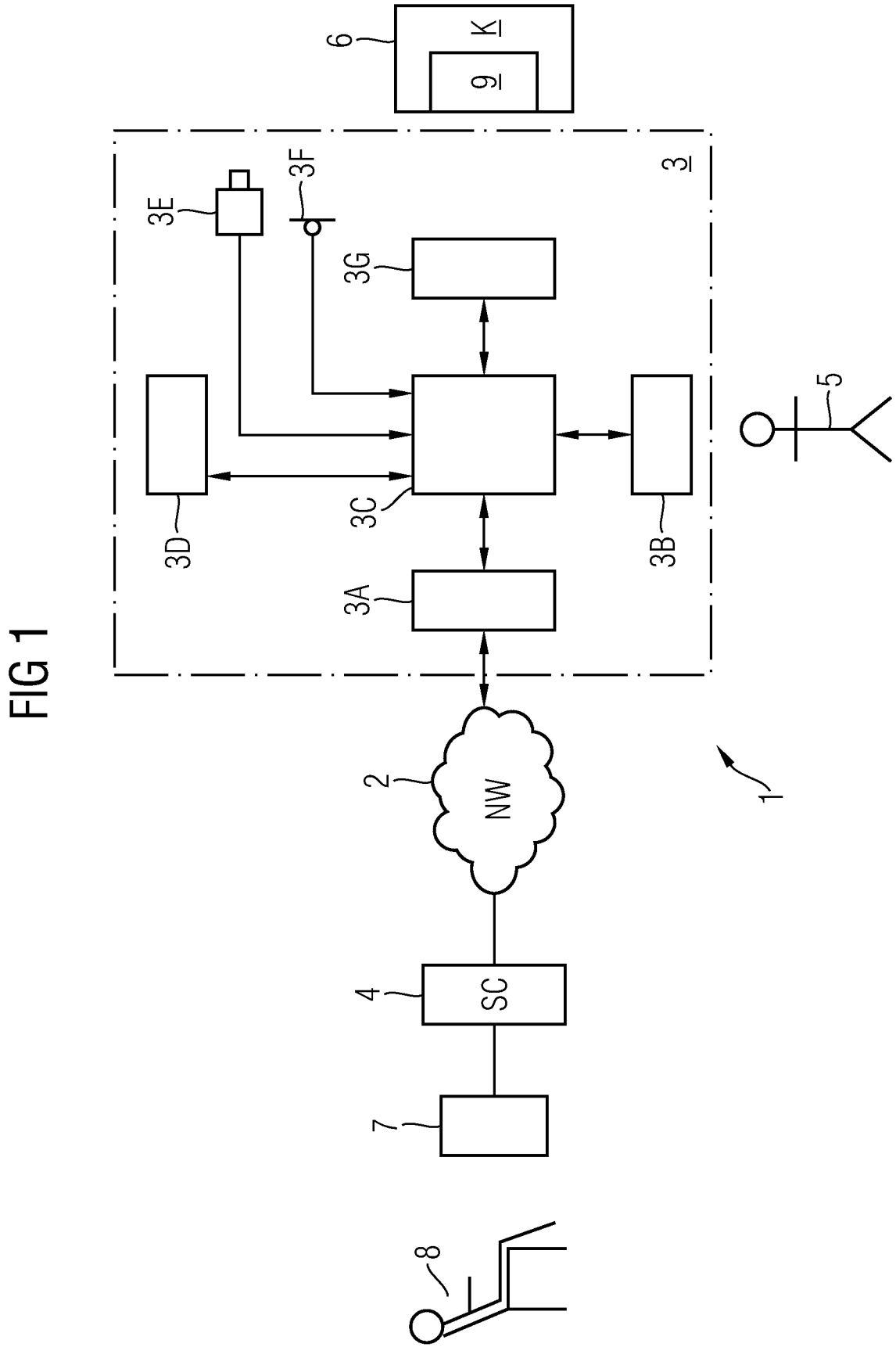


FIG 2

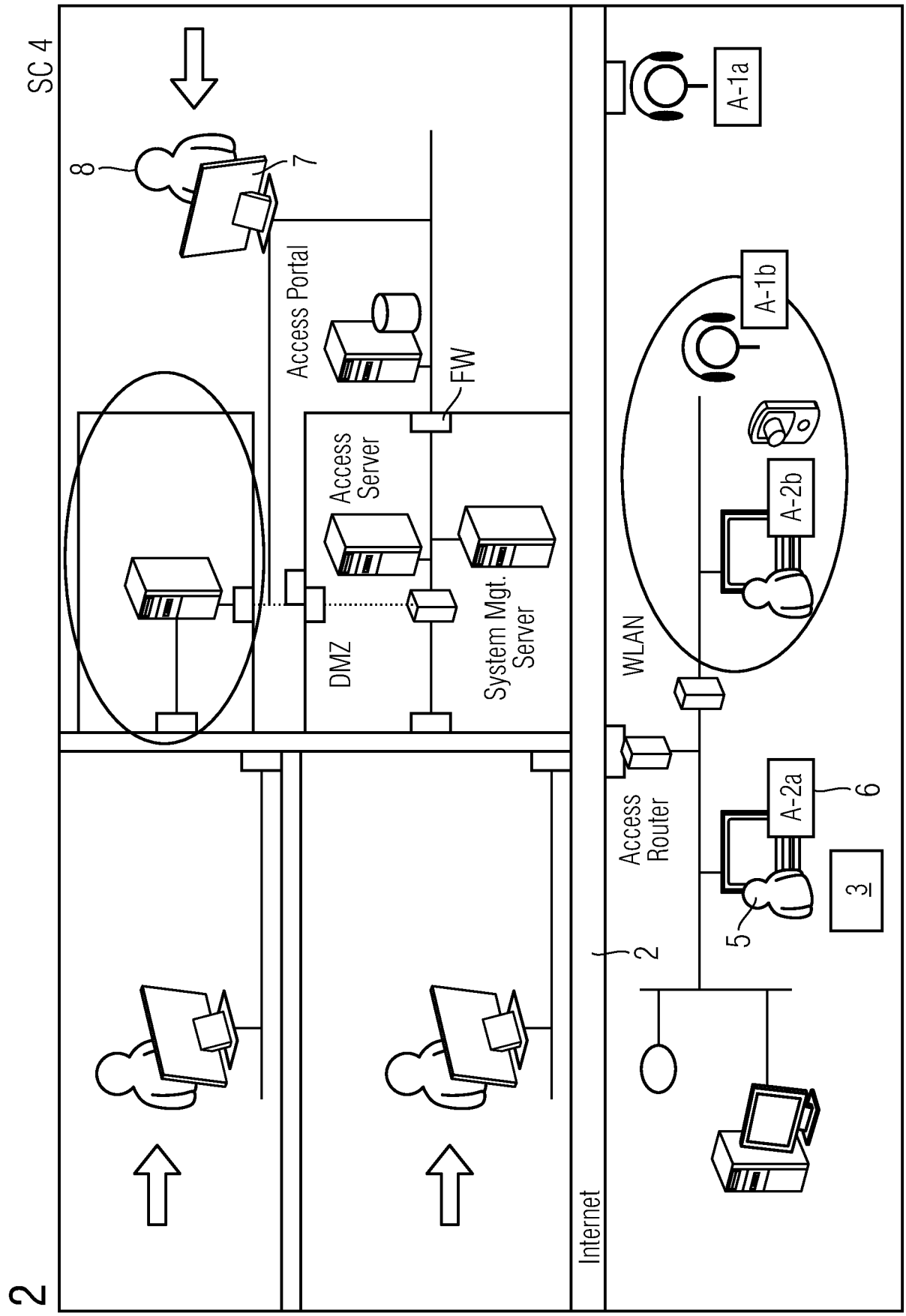

SC 4
8
7
Access Portal
FW
Access Server
DMZ
System Mgt. Server
A-1a
A-1b
A-2b
WLAN
Access Router
A-2a
6
5
2
3
Internet

FIG 3

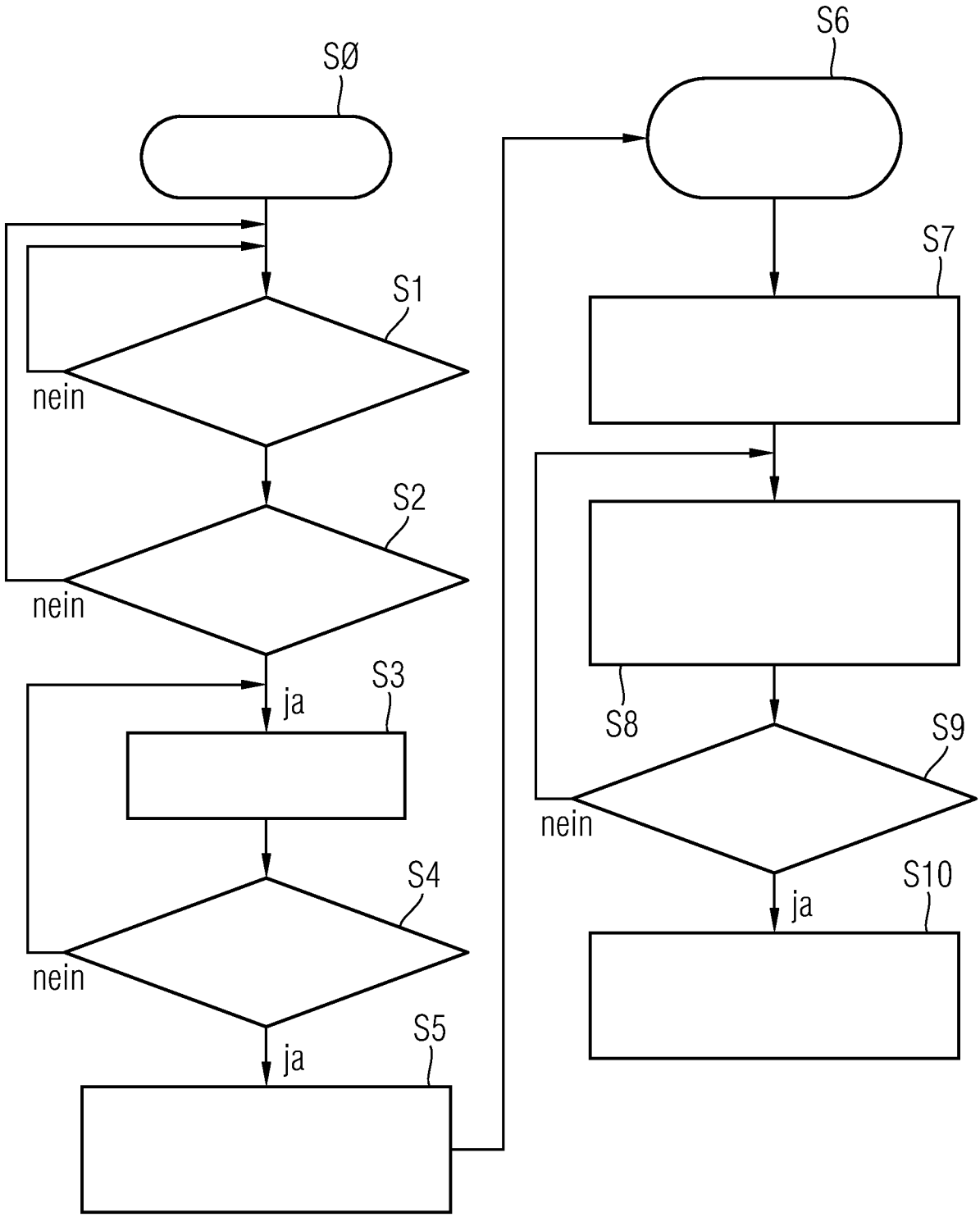


FIG 4A

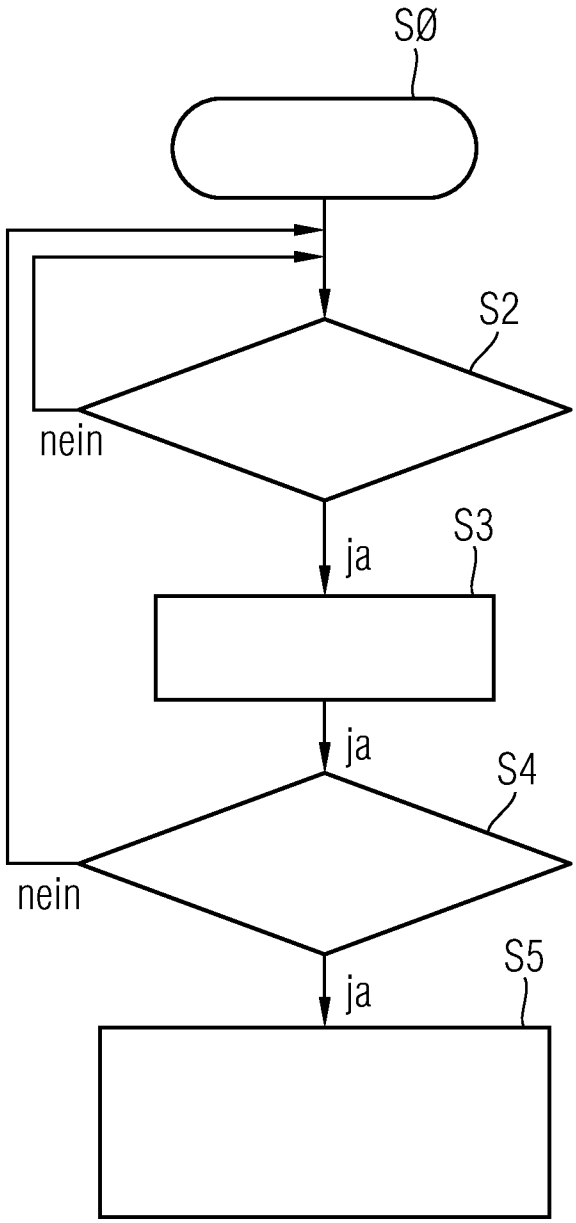


FIG 4B