(19) Deutsches Patent- und Markenamt

(10) **DE 10 2022 125 355 A1** 2024.04.04

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2022 125 355.4**
(22) Anmeldetag: **30.09.2022**
(43) Offenlegungstag: **04.04.2024**

(51) Int Cl.: ***H04L 41/0869*** (2022.01)
H04L 41/16 (2022.01)
H04L 43/00 (2022.01)
G05B 23/02 (2006.01)
G06N 20/00 (2019.01)

(71) Anmelder:
CodeWrights GmbH, 76137 Karlsruhe, DE

(74) Vertreter:
Kratt-Stubenrauch, Kai, Dr.-Ing., 79576 Weil am Rhein, DE

(72) Erfinder:
Vetter, Immanuel, 76547 Sinzheim, DE; Deuser, Thorsten, 74214 Schöntal, DE; Benjamin, Ulrich, 76131 Karlsruhe, DE

(56) Ermittelter Stand der Technik:

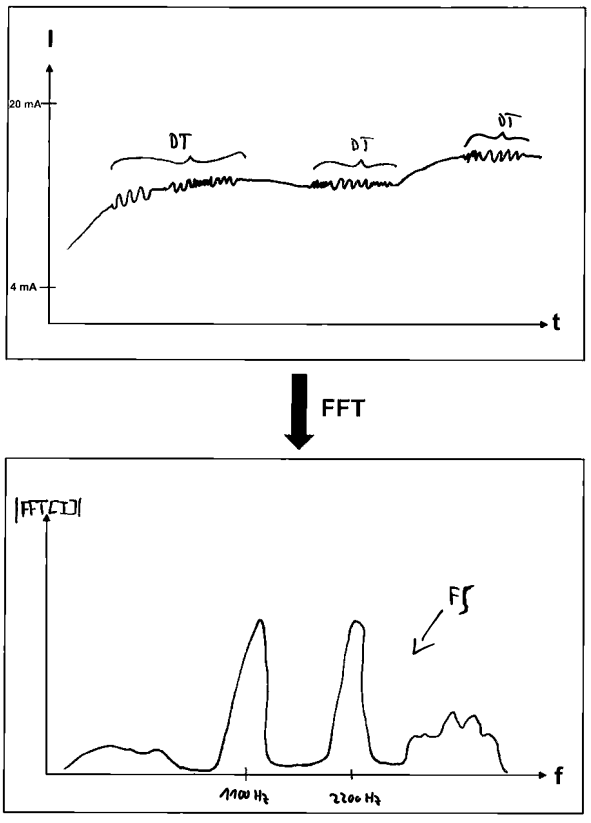
DE	**102 18 830**	**C1**
DE	**10 2007 045 529**	**A1**
DE	**600 30 715**	**T2**
EP	**3 553 616**	**A1**

Rechercheantrag gemäß § 43 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **Verfahren zum Überprüfen eines Feldgeräts der Automatisierungstechnik**

(57) Zusammenfassung: Die Erfindung umfasst ein Verfahren zum Überprüfen eines Feldgeräts (FG1, FG2, FG3, FG4) der Automatisierungstechnik, wobei das Feldgerät (FG1, FG2, FG3, FG4) an ein Kommunikationsnetzwerk (KN) angeschlossen ist, wobei das Feldgerät (FG1, FG2, FG3, FG4) über das Kommunikationsnetzwerk (KN) Datentelegramme (DT) empfängt und aussendet, wobei das Feldgerät (FG1, FG2, FG3, FG4) die Datentelegrame (DT) in einem vorbestimmten Kommunikationsfrequenzband aussendet, umfassend:
- Erfassen der von dem Feldgerät (FG1, FG2, FG3, FG4) ausgesendeten Datentelegramme (DT) über zumindest einen vorbestimmten Zeitraum;
- Durchführen einer Fourier-Transformation an den über den vorbestimmten Zeitraum erfassten Datentelegrammen (DT) zum Erlangen eines spezifischen Frequenzspektrums (FS), wobei die Fourier-Transformation mit einer Abtastrate durchgeführt wird, welche höher ist als die maximale Frequenz des Kommunikationsfrequenzbands;
- Vergleichen des spezifischen Frequenzspektrums (FS) mit einem vorbestimmten Frequenzspektrum; und
- Erstellen einer Notifikation im Falle einer Abweichung des spezifischen Frequenzspektrums (FS) von dem vorbestimmten Frequenzspektrum.



Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zum Überprüfen eines Feldgeräts der Automatisierungstechnik, wobei das Feldgerät an ein Kommunikationsnetzwerk angeschlossen ist, wobei das Feldgerät über das Kommunikationsnetzwerk Datentelegramme empfängt und aussendet, wobei das Feldgerät die Datentelegrame in einem vorbestimmten Kommunikationsfrequenzbands aussendet.

[0002] Aus dem Stand der Technik sind bereits Feldgeräte bekannt geworden, die in industriellen Anlagen zum Einsatz kommen. In der Prozessautomatisierungstechnik ebenso wie in der Fertigungsautomatisierungstechnik werden vielfach Feldgeräte eingesetzt. Als Feldgeräte werden im Prinzip alle Geräte bezeichnet, die prozessnah eingesetzt werden und die prozessrelevante Informationen liefern oder verarbeiten. So werden Feldgeräte zur Erfassung und/oder Beeinflussung von Prozessgrößen verwendet. Zur Erfassung von Prozessgrößen dienen Messgeräte, bzw. Sensoren. Diese werden beispielsweise zur Druck- und Temperaturmessung, Leitfähigkeitsmessung, Durchflussmessung, pH-Messung, Füllstandmessung, etc. verwendet und erfassen die entsprechenden Prozessvariablen Druck, Temperatur, Leitfähigkeit, pH-Wert, Füllstand, Durchfluss etc. Zur Beeinflussung von Prozessgrößen werden Aktoren verwendet. Diese sind beispielsweise Pumpen oder Ventile, die den Durchfluss einer Flüssigkeit in einem Rohr oder den Füllstand in einem Behälter beeinflussen können. Neben den zuvor genannten Messgeräten und Aktoren werden unter Feldgeräten auch Remote I/Os, Funkadapter bzw. allgemein Geräte verstanden, die auf der Feldebene angeordnet sind.

[0003] In modernen Industrieanlagen sind Feldgeräte in der Regel über Kommunikationsnetzwerke wie beispielsweise Feldbusse (Profibus®, Foundation® Fieldbus, HART®, etc.) mit übergeordneten Einheiten verbunden. Normalerweise handelt es sich bei den übergeordneten Einheiten um Leitsysteme (DCS) bzw. Steuereinheiten, wie beispielsweise eine SPS (speicherprogrammierbare Steuerung). Die übergeordneten Einheiten dienen unter anderem zur Prozesssteuerung, Prozessvisualisierung, Prozessüberwachung sowie zur Inbetriebnahme der Feldgeräte.

[0004] Die von den Feldgeräten, insbesondere von Sensoren, erfassten Messwerte werden über das jeweilige Bussystem an eine (oder gegebenenfalls mehrere) übergeordnete Einheit(en) übermittelt. Daneben ist auch eine Datenübertragung von der übergeordneten Einheit über das Bussystem an die Feldgeräte erforderlich, insbesondere zur Konfiguration und Parametrierung von Feldgeräten sowie zur Ansteuerung von Aktoren.

[0005] Die Feldgeräte können je nach Netzwerktyp verschieden angeordnet werden. Gängige Anordnungen sind beispielsweise:

- Punkt zu Punkt-Topologie: Eine Systemkomponente verbunden mit einem Peripheriegerät (Feldgerät oder ebenfalls eine Systemkomponente)

- Stern-Topologie: Eine Systemkomponente (Bsp.: Remote-IO, E/A Karte, Multiplexer) mit mehreren Peripheriegeräten

- Ring-Topologie: Eine Ringanordnung mehrerer Geräte (sowohl System-, als auch Peripherie-Geräte)

- Netz-Topologie: Hierarchische Netzstrukturen als Kombination der oben genannten Strukturen.

[0006] Die digitale Kommunikation der Feldgeräte hat den entsprechenden elektrotechnischen Normen zu folgen, welche durch das jeweilige Feldbusprotokoll vorgegeben wird. Die Geräte sind dementsprechend passend elektrotechnisch ausgelegt und erfüllen den jeweiligen Standard im Rahmen der zulässigen Toleranzen. Heutzutage existieren im Zusammenhang mit Feldbussystemen strenge Anforderungen für die Bus-Zulassung eines Feldgeräts. Zentrale Prüf- und Zertifizierungsstellen gewährleisten hierbei die Einhaltung des entsprechenden Standards.

[0007] Einige Feldbussysteme definieren darüber hinaus ausgeprägte Schutzmechanismen, um ein Feldbussystem gegen unberechtigte Manipulation zu schützen.

[0008] Industrieanlagen der Automatisierungstechnik können manipulationsanfällig und auf verschiedenste Arten angreifbar sein. Mögliche Szenarien für einen solchen Angriff sind beispielsweise:

- Manipulation der Datenleitungen zwischen den in der Anlage verbauten Feldgeräten und Netzwerkkomponenten;

- Manipulation an der Transmitter- oder Sensor-Elektronik eines Feldgeräts;

- Austausch des Transmitters oder Sensors eines Feldgeräts ohne Wissen des Anlagenbetreibers.

[0009] Die Folgen können vielfältig und gravierend sein. Beispielsweise können Denial of Service (DoS)-Attacken auf Feldbussysteme durch sporadische Protokollverletzung zu längeren Ausfallzeiten von (Teil)-Anlagen führen. Manipulation der Daten von Feldgeräten können zu Ausfällen von (Teil)-Anla-

gen, aber auch zu Beschädigungen am Anlagenequipment und Gefahren für das in der Anlage tätige Personal und die Umwelt führen.

[0010] Ausgehend von dieser Problematik liegt der Erfindung die Aufgabe zugrunde, ein Verfahren vorzustellen, welches eine Überprüfung eines Feldgeräts hinsichtlich Manipulationen und/oder Fehlfunktionen auf einfache und sichere Art und Weise ermöglicht.

[0011] Die Aufgabe wird durch ein Verfahren zum Überprüfen eines Feldgeräts der Automatisierungstechnik gelöst, wobei das Feldgerät an ein Kommunikationsnetzwerk angeschlossen ist, wobei das Feldgerät über das Kommunikationsnetzwerk Datentelegramme empfängt und aussendet, wobei das Feldgerät die Datentelegrame in einem vorbestimmten Kommunikationsfrequenzbands aussendet, umfassend:

- Erfassen der von dem Feldgerät ausgesendeten Datentelegramme über zumindest einen vorbestimmten Zeitraum;

- Durchführen einer Fourier-Transformation an den über den vorbestimmten Zeitraum erfassten Datentelegrammen zum Erlangen eines spezifischen Frequenzspektrums, wobei die Fourier-Transformation mit einer Abtastrate durchgeführt wird, welche höher ist als die maximale Frequenz des Kommunikationsfrequenzbands;

- Vergleichen des spezifischen Frequenzspektrums mit mindestem einem vorbestimmten Frequenzspektrum; und

- Erstellen einer Notifikation im Falle einer Abweichung des spezifischen Frequenzspektrums von dem mindestens einen vorbestimmten Frequenzspektrum.

[0012] Erfindungsgemäß werden vom Feldgerät über das Kommunikationsnetzwerk Datentelegramme ausgesendet, die entsprechend dem Protokoll des Kommunikationsnetzwerks ausgestaltet sind. Über einen vorbestimmten Zeitraum werden solche Datentelegramme erfasst und aufgezeichnet. Konkret wird der Verlauf der Spannung oder der Stromstärke über die Zeit aufgezeichnet. Durch eine Fourier-Transformation der aufgezeichneten Datentelegramme wird der zeitliche Verlauf der Spannung oder der Stromstärke in ein spezifisches Frequenzspektrum umgewandelt. Dieses spezifische Frequenzspektrum enthält die in dem vorbestimmten Zeitraum aufgezeichneten Frequenzen und deren Anteil.

[0013] Über die nachfolgende Analyse des spezifischen Frequenzspektrums mit einem vorbestimmten Frequenzspektrum können Abweichungen des Feldgeräts, bzw. des Netzwerksegments, in welchem das Feldgerät integriert ist, detektiert werden. Im Frequenzraum können Fehlfunktionen und Abweichungen detektiert werden, welche über eine Analyse des Verlaufs der Spannung oder der Stromstärke im zeitlichen Raum nicht oder nur schwer detektierbar wären.

[0014] Mittels des Verfahrens kann nicht nur detektiert werden, dass eine Abweichung vorliegt, also ein Fehler am Feldgerät, bzw. am Netzwerksegment wahrscheinlich ist. Es lässt sich darüber hinaus auch auf den vorliegenden Fehlertyp schließen. Hierfür wird die Art der Abweichung betrachtet, also in welchen Frequenzanteilen eine Abweichung in welcher Größe vorliegt, was spezifisch für bestimmte Fehlertypen sein kann. Beispielsweise wird das spezifische Frequenzspektrum hierfür mit einem oder mehreren weiteren Referenzspektren verglichen, welche spezifisch für bestimmte Fehlertypen sind.

[0015] Die Abweichungen lassen beispielsweise auf folgende Fehlertypen schließen:

- ob die Elektronik des Feldgeräts in einem kritischen Alterungsstadium ist;

- ob Manipulationen an der Physik des Anlagen- oder Kommunikationsnetzwerksegments vorgenommen wurden;

- ob Feldgeräte getauscht wurden oder ein Feldgerät physikalisch verändert wurde (bspw. Elektronikmodule getauscht wurden);

- welches Datentelegramm von welchem Feldgerät geschickt wurde (DoS-Angriffe lassen sich so direkt zuordnen) - Voraussetzung hierfür ist, dass mehrere Feldgeräte vorhanden sind, welche Datentelegramme aussenden.

[0016] Feldgeräte, welche im Zusammenhang mit der Erfindung genannt werden, sind bereits im einleitenden Teil der Beschreibung aufgeführt worden.

[0017] Eine Ausgestaltung des Verfahrens sieht vor, dass für den Schritt des Vergleichens des spezifischen Frequenzspektrums mit dem vorbestimmten Frequenzspektrum ein KI- oder Machine Learning-Algorithmus verwendet wird. Hierfür können im Stand der Technik geläufige Algorithmen verwendet werden, beispielsweise basierend auf neuronalen Netzwerken oder Deep Learning.

[0018] Eine Ausgestaltung des Verfahrens sieht vor, dass der KI- oder Machine Learning-Algorithmus mit einer Vielzahl von Frequenzspektren des Feldgeräts eingelernt wird und daraus das vorbestimmte Frequenzspektrum erstellt. Hierfür werden mehrere Frequenzspektren desselben Feldgerätetyps verwendet, die einen guten, fehlerfreien Zustand des Feldgeräts zeigen. Der Grund dafür ist, dass jedes Feldgerät, auch von gleichem Gerätetyp aufgrund

der Streuung in den Bauteilen eine eigene Charakteristik. Die Charakteristiken unterscheiden sich minimal in Innenwiderstand und Impedanz, was sich auf die Qualität eines ausgesendeten Datentelegramms auswirkt. Das Transformieren dieser Datentelegramme mittels einer Fourier-Analyse führt zu leicht abweichenden Frequenzspektren, welche für jedes einzelne Feldgerät einzigartig sind. Durch das Zuführen der verschiedenen Frequenzspektren zu dem KI- oder Machine Learning-Algorithmus wird dieser möglichst breit eingelernt, so dass dieser Abweichungen zu einem guten, fehlerfreien Zustand möglichst gut erkennen kann.

[0019] In einer ersten Variante des Verfahrens ist vorgesehen, dass ein Benutzer nach dem Erstellen einer Notifikation eine Rückmeldung gibt, ob eine unerwünschte Abweichung aufgetreten ist. Es können beispielsweise neue, unbekannte Abweichungen detektiert werden, die eine Notifikation veranlassen, aber keinen tatsächlichen Fehlerfall des Feldgeräts und/oder des Netzwerks zeigen. Dadurch kann KI- oder Machine Learning-Algorithmus weiter eingelernt und verbessert werden.

[0020] In einer zweiten Variante des Verfahrens ist vorgesehen, dass der KI- oder Machine Learning-Algorithmus bestimmt, ob eine unerwünschte Änderung aufgetreten ist und dies als Rückmeldung an sich selbst zurückführt. Der KI- oder Machine Learning-Algorithmus lernt daduch selbstständig.

[0021] Eine Ausgestaltung der ersten Variante oder der zweiten Variante des Verfahrens sieht vor, dass der der KI- oder Machine Learning-Algorithmus das vorbestimmte Frequenzspektrum basierend auf der Rückmeldung anpasst. Durch das Anpassen des Referenzspektrums können falsch-negative Notifikationen reduziert werden.

[0022] Eine Ausgestaltung des Verfahrens sieht vor, dass das Feldgerät selbst den Schritt des Erfassens der ausgesendeten Datentelegramme durchführt. Hierfür ist beispielsweise ein Modul vorgesehen, welches an dem Feldgerät angebracht, bzw. mit diesem verbunden ist. Dieses verfügt über entsprechende Schnittstellen zum Empfang der ausgesendeten Datentelegramme. Ein solches Modul kann eigene Ressourcen, bspw. ein eigenes Elektronikmodul oder eine eigene Speichereinheit aufweisen, oder Ressourcen des Feldgeräts mitbenutzen.

[0023] Eine Ausgestaltung des Verfahrens sieht vor, dass ein weiterer Teilnehmer des Kommunikationsnetzwerks, insbesondere ein weiteres Feldgerät oder ein Netzwerkgerät, den Schritt des Erfassens der ausgesendeten Datentelegramme durchführt. Ein solches Netzwerkgerät ist beispielsweise ein mit dem Kommunikationsnetzwerk verbundenes Gateway oder Edge Device.

[0024] In einer vorteilhaften Ausgestaltung des Verfahrens ist vorgesehen, dass die Schritte des Durchführens der Fourier-Transformation und/oder des Vergleichens von einem weiteren Netzwerkteilnehmer, insbesondere ein lokaler PC, durchgeführt werden, wobei die erfassten Daten über das Kommunikationsnetzwerk an den weiteren Netzwerkteilnehmer übermittelt werden.

[0025] Die Schritte des Erfassens der ausgesendeten Datentelegramme und des Durchführens der Fourier-Transformation und/oder des Vergleichens können natürlich auch von einem einzigen Gerät ausgeführt werden, beispielsweise von dem Feldgerät selbst oder dem weiteren Netzwerkteilnehmer.

[0026] In einer alternativen vorteilhaften Ausgestaltung des Verfahrens ist vorgesehen, dass die Schritte des Durchführens der Fourier-Transformation und/oder des Vergleichens von einer cloudbasierten Plattform durchgeführt werden, wobei die erfassten Daten über das Internet an die cloudbasierte Plattform übermittelt werden. Eine cloudbasierte Plattform (auch vereinfacht „Cloud“ genannt) ist ein Server, auf welchen per Internet Daten gesendet und von diesem empfangen werden können und auf welchem sich eine oder mehrere Applikationen befinden. Auf diese Applikationen, welche beispielsweise den KI- oder Machine Learning-Algorithmus enthalten können, kann von einem Benutzer mittels Internet zugegriffen werden.

[0027] Eine Ausgestaltung des Verfahrens sieht vor, dass das Feldgerät physikalische Messgrößen eines verfahrenstechnischen Prozesses und/oder und Diagnosedaten als Datentelegramme aussendet. Dem Fachmann ist bekannt, dass ein Feldgerät eine Vielzahl unterschiedlicher Daten generieren kann, welche im Rahmen des Verfahrens als Inhalt von Datentelegrammen ausgesendet werden können.

[0028] Eine Ausgestaltung des Verfahrens sieht vor, dass als Kommunikationsnetzwerk ein Feldbus der Automatisierungstechnik verwendet wird. Im Prinzip kann jedes gebräuchliche Protokoll eines drahtgebundenen Feldbusnetzwerks, insbesondere eines Feldbusnetzwerks der Automatisierungstechnik, wie beispielsweise Foundation Fieldbus®, Profibus®, Profinet®, HART®, Modbus®, etc. verwendet werden. Eine dazu alternative Ausgestaltung des Verfahrens sieht vor, dass als Kommunikationsnetzwerk ethernetbasiertes Netzwerk, beispielsweise Industrial Ethernet oder Profinet® verwendet wird.

[0029] Die Erfindung wird anhand der nachfolgenden Figuren näher erläutert. Es zeigt

Fig. 1: eine erste Netzwerkanordnung zur Durchführung des erfindungsgemäßen Verfahrens;

Fig. 2: Beispiele für ausgesendete Datentelegramme im zeitlichen Raum und ein daraus Fourier-transformiertes Frequenzspektrum; und

Fig. 3: eine zweite Netzwerkanordnung zur Durchführung des erfindungsgemäßen Verfahrens.

[0030] **Fig.** 1 zeigt eine Anordnung, bestehend aus einem Feldgerät FG1 und einem Bediengerät BE. Bei dem Feldgerät handelt es sich um ein Gerät zum Erfassen oder Beeinflussen einer physikalischen Größe eines verfahrenstechnischen Prozesses. Beispielsweise handelt es sich bei dem Feldgerät FG1 um ein Druckmessgerät. Weitere Beispiele für Feldgeräte sind bereits im einleitenden Teil der Beschreibung aufgeführt worden.

[0031] Bei dem Bediengerät BE handelt es sich beispielweise um einen PC oder Laptop mit einem entsprechenden Kommunikationsmodem oder um eine mobile Bedieneinheit. Das Bediengerät BE und das Feldgerät FG1 sind mittels zweiter Kommunikationsleitungen miteinander verbunden und bilden ein Kommunikationsnetzwerk, welches das Kommunikationsprotokoll HART verwendet. Mittels dieses Protokolls sendet das Bediengerät BE Anfragen an das Feldgerät FG1, das Feldgerät FG1 antwortet dem Bediengerät BE mittels Datentelegrammen DT. Das Feldgerät FG1 kann derart eingestellt sein, dass dieses der Bedieneinheit BE in regelmäßig Zeitabständen selbstständig Datentelegramme DT übermittelt, ohne dass die Bedieneinheit BE hierfür Anfragen aussenden muss. Die Datentelegramme DT enthalten vom Feldgerät erzeugte Daten, beispielsweise Prozessvariablen und/oder Statusdaten.

[0032] Der Zustand eines Feldgeräts FG1 kann sich über die Zeit verschlechtern. Beispielsweise können elektronische Komponenten schleichend Ausfälle entwickeln, bzw. ihre Charakteristiken ändern. Auch kann sich der Zustand des Kommunikationsnetzwerks KN selbst ändern, bspw. durch Beschädigungen der Leitungen oder durch Korrosionen an den Kontakten zwischen Feldgerät FG und den Leitungen. Solche Zustandsänderungen können nicht immer direkt mittels Statusanzeigen des Feldgeräts, bzw. aus den von dem Feldgerät erzeugten Daten erkannt werden.

[0033] Aus diesem Grund ist ein weiterer Teilnehmer TN des Kommunikationsnetzwerks KN, beispielsweise in Gestalt eines passiven Geräts (bspw. ein Switch mit Zusatzelektronik), vorgesehen, welcher physikalisch zwischen Feldgerät FG1 und Bedieneinheit BE angeordnet ist. Es kann alternativ vorgesehen sein, dass die Bedieneinheit BE oder das Feldgerät FG1 selbst die nachfolgend beschriebenen Funktionalitäten des weiteren Teilnehmers TN des Kommunikationsnetzwerk KN durchführt.

[0034] Der weitere Teilnehmer TN erfasst für ein vorbestimmtes Zeitintervall die Datentelegramme DT des Feldgeräts FG1.

[0035] In **Fig.** 2 ist in dem oberen Diagramm eine Abfolge von drei Datentelegrammen DT abgebildet, welche über das vorbestimmte Zeitintervall aufgezeichnet wurden. Das Diagramm zeigt auf der Abszisse den Zeitverlauf t und auf der Ordinate einen Stromwert I in mA. Im HART-Protokoll sind Datentelegramme derart ausgestaltet, dass diese auf einen Basisstromwert (4-20 mA-Standard), welcher die aktuelle Größe der durch das Feldgerät FG1 erfasste primäre Prozessvariable anzeigt, aufmoduliert. Eine digitale „1“ wird mit der Frequenz 1,2 kHz (1200 Hz) und eine „0“ wird mit der Frequenz 2,2 kHz (2200 Hz) dargestellt. Im vorliegenden Diagramm sind in dieser Darstellung keine Fehlfunktionen erkennbar.

[0036] Der weitere Teilnehmer TN führt anschließend eine Fourier-Transformation der in dem vorbestimmten Zeitintervall erfassten Datentelegramme durch. Hier führt er einen Fast-Fourier-Transformation(FFT)-Algorithmus oder einen ähnlich gut geeigneten Algorithmus durch. Dadurch werden die aufgezeichneten Datentelegramme DT vom zeitlichen Raum in den Frequenzraum überführt. **Fig.** 2 zeigt im unteren Diagramm das spezifische Frequenzspektrum FS der Fourier-transformierten Datentelegramme DT. Die Ordinate stellt ein Frequenzband f dar, die Abszisse zeigt den Betrag einer Größe der Fourier-transformierten Datentelegramme.

[0037] Das spezifische Frequenzspektrum FS ist eindeutig für das Feldgerät FG1 und wird dadurch auch als „Fingerprint“ bezeichnet. Führt man eine solche Fourier-Transformation an einem digitalen Signal eines elektrischen Gerätes mit einer Abtastrate durch, die deutlich höher als die Kommunikationsfrequenz selbst ist, so kann man Signifikanzen im Frequenzspektrum erkennen, die einzigartig für die Elektronik sind. Jede Elektronik hat sozusagen ihren eigenen Fingerprint.

[0038] Das spezifische Frequenzspektrum FS wird anschließend an eine cloudbasierte Plattform übermittelt. Auf dieser wird eine Applikation ausgeführt, die einen KI- oder Machine Learning-Algorithmus ausführt. Dieser KI- oder Machine Learning-Algorithmus vergleicht das spezifische Frequenzspektrum mit einem vorbestimmten Frequenzspektrum auf Abweichungen.

[0039] Dabei muss berücksichtigt werden, dass ein Fingerabdruck nicht nur vom Feldgerät FG1 selbst, sondern auch von der Gesamtimpedanz des Kommunikationsnetzwerks KN abhängt. Auch ist es möglich, dass sich der Fingerabdruck in Abhängigkeit geräteinterner Vorgänge verändern kann. Beispielsweise könnte eine Sensorik des Feldgeräts FG1 in

der Grenzlast Auswirkungen auf den Fingerabdruck haben. Der Fingerabdruck weist deshalb eine gewisse Dynamik auf, die erst erlernt werden muss. KI- oder Machine Learning-Algorithmus ist daher mit einer Vielzahl von Frequenzspektren vorab auf diese Dynamik eingelernt, bzw. wird während des Betriebs stets weiter eingelernt (bspw. mittels Rückmeldungen des Benutzers) und kann daher nach einiger Zeit sehr präzise Aussagen treffen, ob eine Änderung tatsächlich stattgefunden hat, oder nicht.

[0040] Im vorliegenden Fall detektiert die KI-Abweichungen im oberen Frequenzbereich des spezifischen Frequenzspektrums. Das Frequenzspektrum FS zeigt typische Spikes im Bereich von 1200 Hz und 2200 Hz, welche die aufmodulierten „1“- und „0“-Signale des HART-Telegramms zeigen. Der Frequenzanteil unterhalb von 1200 Hz zeigt die langsamere Änderung der 4-20 mA-Prozessvariable. Der Frequenzanteil oberhalb von 2200 Hz zeigt allerdings, verglichen mit dem Referenzspektrum, einen untypischen Verlauf. Der KI- oder Machine Learning-Algorithmus detektiert diesen als Abweichung und detektiert (durch einen Vergleich mit weiteren Referenzspektren, die typische Fehlerbilder zeigen) eine schleichende, altersbedingte Veränderung der Elektronik des Feldgeräts FG1. Dies wird dem Benutzer mittels einer Notifikation mitgeteilt.

[0041] Anstatt der cloudbasierten Plattform können auch das Bediengerät BG, der weitere Teilnehmer TN oder das Feldgerät FG den Schritt des Vergleichens durchführen. Voraussetzung hierfür ist, dass diese Instanzen über ausreichende Ressourcen zum Ausführen und Trainieren des KI- oder Machine Learning-Algorithmus verfügen.

[0042] In **Fig.** 3 ist eine weitere Anwendung des Verfahrens gezeigt. Abgebildet ist hier ein Kommunikationsnetzwerk KN, welches aus mehreren Feldgeräten FG1, FG2, FG3, FG4, einer Steuereinheit SE, mehreren Workstation-PCs PC1, PC2 und einem weiteren Teilnehmer TN in Gestalt eines Edge Devices oder Gateways besteht. Das Kommunikationsnetzwerk KN verwendet ein modernes Feldbusprotokoll (beispielsweise Foundation Fieldbus® oder Profibus®) oder ist ethernetbasiert ausgestaltet.

[0043] Der weitere Teilnehmer TN zeichnet hier Datentelegramme von einem oder mehreren der Feldgeräte FG1, FG2, FG3, FG4 auf und wandelt die in spezifischen Zeitintervallen aufgezeichneten Datentelegramme per Fourier-Transformation in spezifische Frequenzspektren um. Der auf der cloudbasierten Plattform CP implementierte KI- oder Machine Learning-Algorithmus untersucht diese spezifischen Frequenzspektren auf Abweichungen. Nicht nur können (hardwarebedingte) Fehler der Feldgeräte detektiert werden - aufgrund der Einzigartigkeit der Frequenzspektren kann detektiert werden, ob ein Datentelegramm tatsächlich von dem im Telegramm enthaltenen Adressaten stammt, oder ob eine Manipulation durch einen Dritten vorliegt (bspw. durch einen Austausch von Feldgeräten FG1, FG2, FG3, FG4 oder Leitungen, oder aber auch mittels Einbringens von Datentelegrammen durch ein Fremdgerät). Auch die Datentelegramme der Steuereinheit SE können auf diese Art und Weise überprüft werden.

Bezugszeichenliste

BE	Bedieneinheit
CP	cloudbasierte Plattform
DT	Datentelegramme
FG1, FG2, FG3, FG4	Feldgeräte
FS	Frequenzspektrum
KI	KI- oder Machine Learning-Algorithmus
KN	Kommunikationsnetzwerk
PC1, PC2	Workstation-PCs
SE	Steuereinheit
TN	weiterer Teilnehmer des Kommunikationsnetzwerks

Patentansprüche

1. Verfahren zum Überprüfen eines Feldgeräts (FG1, FG2, FG3, FG4) der Automatisierungstechnik, wobei das Feldgerät (FG1, FG2, FG3, FG4) an ein Kommunikationsnetzwerk (KN) angeschlossen ist, wobei das Feldgerät (FG1, FG2, FG3, FG4) über das Kommunikationsnetzwerk (KN) Datentelegramme (DT) empfängt und aussendet, wobei das Feldgerät (FG1, FG2, FG3, FG4) die Datentelegrame (DT) in einem vorbestimmten Kommunikationsfrequenzband aussendet, umfassend:
- Erfassen der von dem Feldgerät (FG1, FG2, FG3, FG4) ausgesendeten Datentelegramme (DT) über zumindest einen vorbestimmten Zeitraum;
- Durchführen einer Fourier-Transformation an den über den vorbestimmten Zeitraum erfassten Datentelegrammen (DT) zum Erlangen eines spezifischen Frequenzspektrums (FS), wobei die Fourier-Transformation mit einer Abtastrate durchgeführt wird, welche höher ist als die maximale Frequenz des Kommunikationsfrequenzbands;
- Vergleichen des spezifischen Frequenzspektrums (FS) mit mindestens einem vorbestimmten Frequenzspektrum; und
- Erstellen einer Notifikation im Falle einer Abweichung des spezifischen Frequenzspektrums (FS)

von dem mindestens einen vorbestimmten Frequenzspektrum.

2. Verfahren nach Anspruch 1, wobei für den Schritt des Vergleichens des spezifischen Frequenzspektrums (FS) mit dem vorbestimmten Frequenzspektrum ein KI- oder Machine Learning-Algorithmus (KI) verwendet wird.

3. Verfahren nach Anspruch 2, wobei der KI- oder Machine Learning-Algorithmus mit einer Vielzahl von Frequenzspektren des Feldgeräts (FG1, FG2, FG3, FG4) eingelernt wird und daraus das vorbestimmte Frequenzspektrum erstellt.

4. Verfahren nach Anspruch 3, wobei ein Benutzer nach dem Erstellen einer Notifikation eine Rückmeldung gibt, ob eine unerwünschte Abweichung aufgetreten ist.

5. Verfahren nach Anspruch 3, wobei der KI- oder Machine Learning-Algorithmus bestimmt, ob eine unerwünschte Änderung aufgetreten ist und dies als Rückmeldung an sich selbst zurückführt.

6. Verfahren nach Anspruch 4 oder 5, wobei der der KI- oder Machine Learning-Algorithmus das vorbestimmte Frequenzspektrum basierend auf der Rückmeldung anpasst.

7. Verfahren nach einem oder mehreren der vorherigen Ansprüche, wobei das Feldgerät (FG1, FG2, FG3, FG4) selbst den Schritt des Erfassens der ausgesendeten Datentelegramme (DT) durchführt.

8. Verfahren nach einem oder mehreren der vorherigen Ansprüche, wobei ein weiterer Teilnehmer (TN) des Kommunikationsnetzwerks (KN), insbesondere ein weiteres Feldgerät (FG1, FG2, FG3, FG4) oder ein Netzwerkgerät, den Schritt des Erfassens der ausgesendeten Datentelegramme (DT) durchführt.

9. Verfahren nach Anspruch 7 oder 8, wobei die Schritte des Durchführens der Fourier-Transformation und/oder des Vergleichens von einem weiteren Teilnehmer (TN) des Kommunikationsnetzwerks (KN), insbesondere ein weiteres Feldgerät oder ein lokaler PC, durchgeführt werden, wobei die erfassten Daten über das Kommunikationsnetzwerk (KN) an den weiteren Netzwerkteilnehmer übermittelt werden.

10. Verfahren nach Anspruch 7 oder 8, Cloud, wobei die Schritte des Durchführens der Fourier-Transformation und/oder des Vergleichens von einer cloudbasierten Plattform (CP) durchgeführt werden, wobei die erfassten Daten über das Internet an die cloudbasierte Plattform (CP) übermittelt werden.

11. Verfahren nach einem oder mehreren der vorherigen Ansprüche, wobei das Feldgerät (FG1, FG2, FG3, FG4) physikalische Messgrößen eines verfahrenstechnischen Prozesses und/oder und Diagnosedaten als Datentelegramme (DT) aussendet.

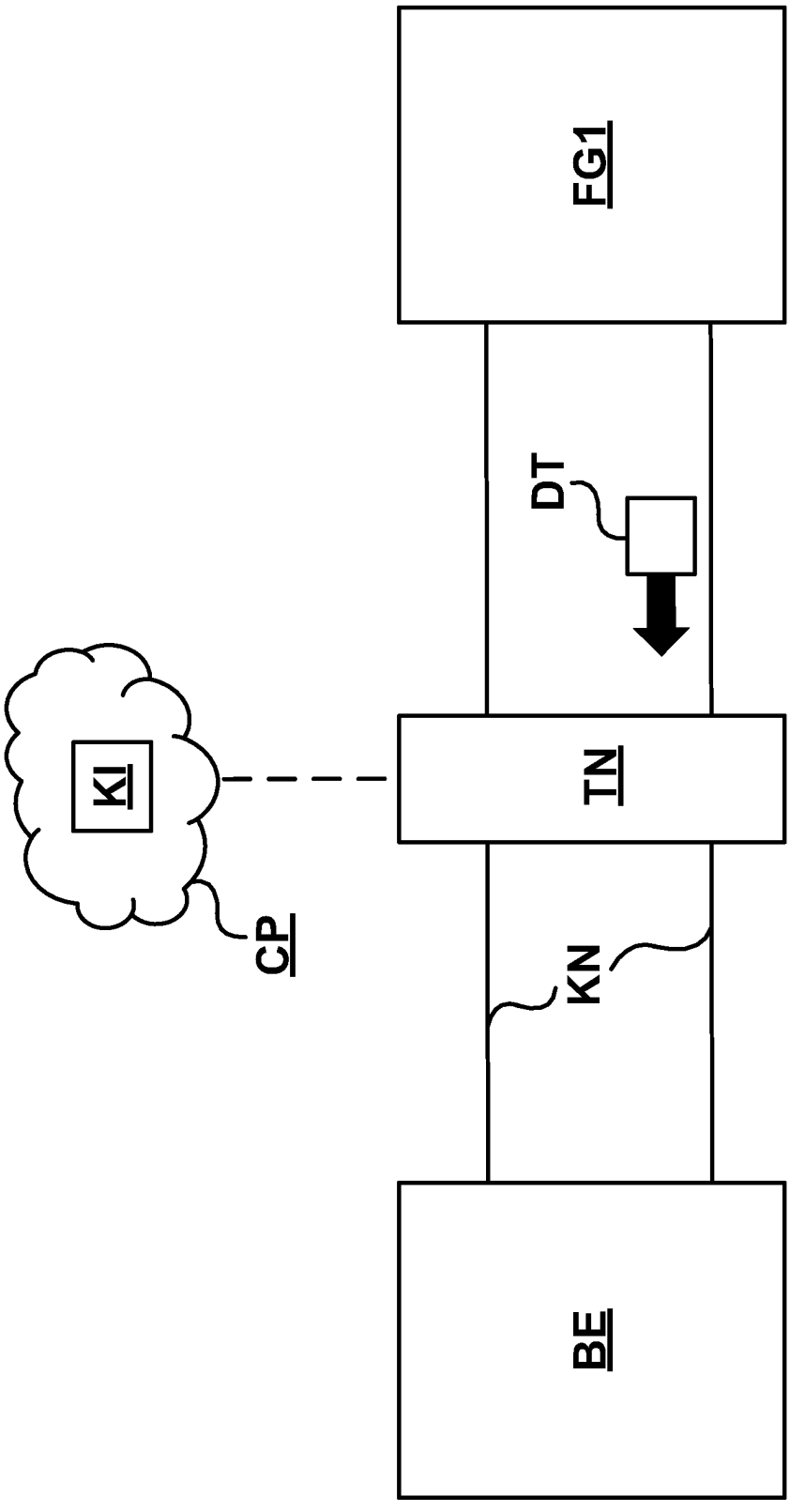
12. Verfahren nach einem oder mehreren der vorherigen Ansprüche, wobei als Kommunikationsnetzwerk (KN) ein Feldbus der Automatisierungstechnik verwendet wird.

13. Verfahren nach einem oder mehreren der vorherigen Ansprüche, wobei als Kommunikationsnetzwerk (KN) ein ethernetbasiertes Netzwerk verwendet wird.

Es folgen 3 Seiten Zeichnungen

Anhängende Zeichnungen

Fig. 1



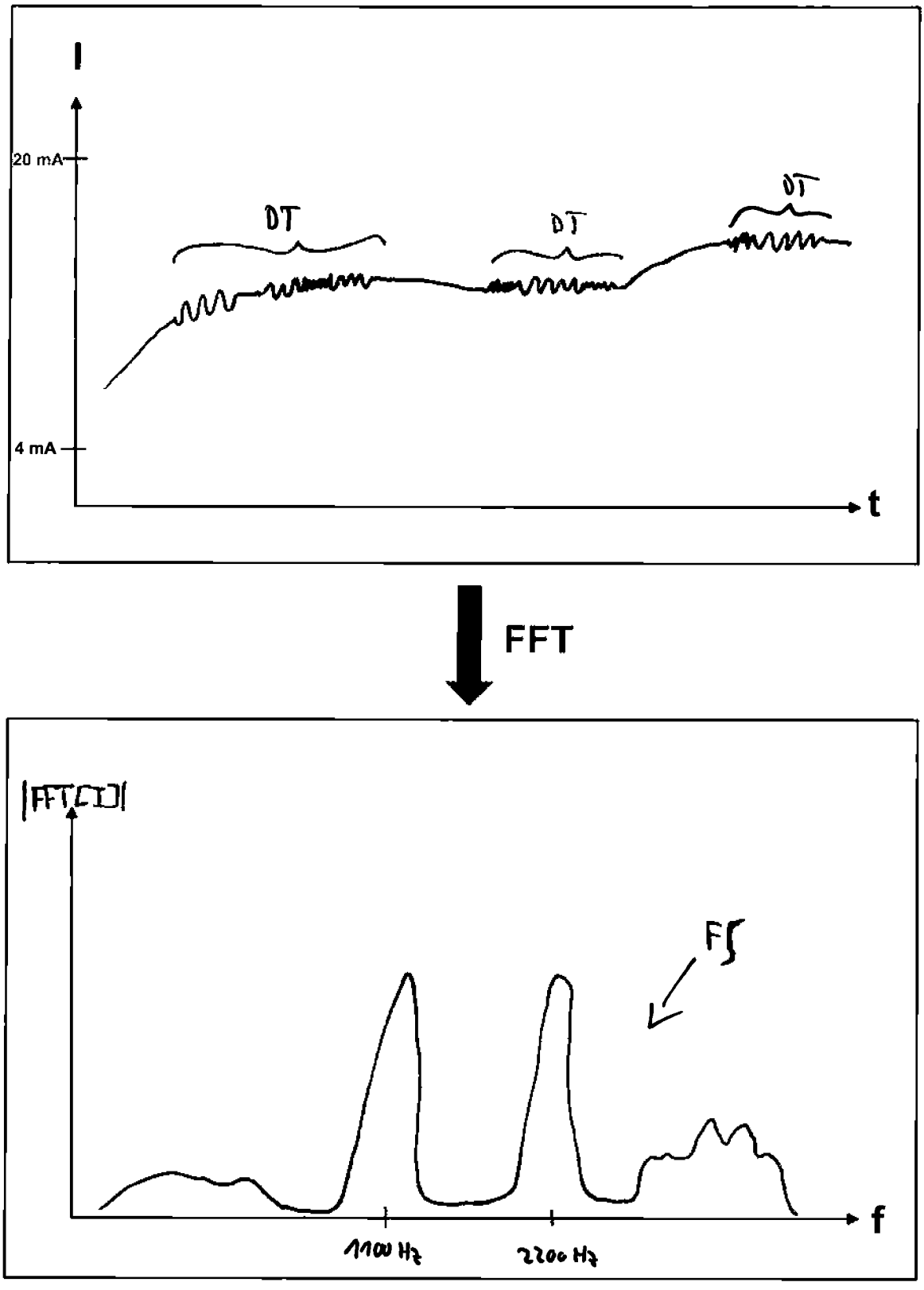


Fig. 2

Fig. 3