(19) Deutsches Patent- und Markenamt

(10) **DE 10 2023 131 634 A1** 2025.05.15

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2023 131 634.6**
(22) Anmeldetag: **14.11.2023**
(43) Offenlegungstag: **15.05.2025**

(51) Int Cl.: ***G06F 11/30*** (2006.01)

(71) Anmelder:
Dräger Safety AG & Co. KGaA, 23560 Lübeck, DE

(72) Erfinder:
Schröder, Tino, 23558 Lübeck, DE; Draack, Sebastian, 23558 Lübeck, DE; Harneid, Justus, 23558 Lübeck, DE; Zickmantel, Till, 23558 Lübeck, DE; Kulling, Kim, 23558 Lübeck, DE

(56) Ermittelter Stand der Technik:

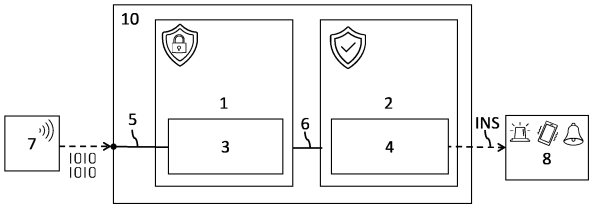
DE	**10 2019 219 870**	**A1**
DE	**10 2022 109 700**	**A1**

Rechercheantrag gemäß § 43 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **Vorrichtung und Verfahren zur Ausführung von Cybersecurity-Funktionen und von Safety-Funktionen**

(57) Zusammenfassung: Die Erfindung betrifft eine Vorrichtung (10) zur Ausführung von Cybersecurity-Funktionen im Sinne der Informationssicherheit und von Safety-Funktionen im Sinne der Betriebssicherheit mit einer ersten Recheneinheit (1) zur Ausführung zumindest einer der Cybersecurity-Funktionen und mit einer zweiten Recheneinheit (2) zur Ausführung zumindest einer der Safety-Funktionen, wobei die erste Recheneinheit (1) ein Kommunikationsmodul (3) umfasst, welches eine erste Schnittstelle (5) aufweist und eingerichtet ist, eingehende Daten zu prüfen, wobei die zweiten Recheneinheit (2) ein Alarmmodul (4) umfasst, welches eingerichtet ist, ein Informationssignal (INS) zu erzeugen, und wobei die erste Recheneinheit (1) und die zweite Recheneinheit (2) über eine zweite Schnittstelle (6) zum Datenaustausch miteinander verbunden sind. Ferner betrifft die Erfindung ein Verfahren zur Ausführung von Cybersecurity-Funktionen und von Safety-Funktionen auf einer solchen Vorrichtung (10) sowie ein Gasmessgerät (20) und ein Beatmungs- oder Anästhesiegerät (30) mit einer solchen Vorrichtung (10).



Beschreibung

[0001] Die vorliegende Erfindung betrifft eine Vorrichtung sowie ein Verfahren zur Ausführung von Cybersecurity-Funktionen und von Safety-Funktionen. Ferner betrifft die Erfindung ein Gasmessgerät und ein Beatmungs- oder Anästhesiegerät mit einer solchen Vorrichtung.

[0002] Cybersecurity und Cybersecurity-Funktionen gewinnen mehr und mehr an Bedeutung, insbesondere im Zeitalter der Digitalisierung und der immer umfangreicheren Vernetzung von Geräten mit internetbasierten Plattformen. Cybersecurity, gleichbedeutend mit IT-Security, soll die Informationssicherheit von Systemen und Geräten gewährleisten. Dabei soll die Verfügbarkeit, Vertraulichkeit und Integrität von Informationen sichergestellt werden. Ein wesentlicher Aspekt dabei ist der Schutz vor Angriffen, mit denen Informationen gezielt manipuliert werden und somit großer Schaden angerichtet werden kann. In erster Linie handelt es sich bei Cybersecurity-Funktionen um Maßnahmen, die den Schutz von Geräten oder Systemen vor solchen Angriffen ermöglichen.

[0003] Im Gegensatz dazu handelt es sich bei Safety-Funktionen insbesondere um den Schutz von Lebewesen und der Umwelt vor möglichen Gefahren. Safety-Funktionen, auch funktionale Sicherheit genannt, soll die Betriebssicherheit gewährleisten. Dabei sollen Gefahren möglichst verhindert oder, falls dies nicht möglich ist, zumindest darauf hingewiesen werden, so dass Gegenmaßnahmen eingeleitet werden können. Aufgrund der großen Bedeutung von Safety-Funktionen sind diese, insbesondere im industriellen und medizinischen Umfeld, speziellen Regularien, wie Normen und Standards, unterlegen. Häufig wird dabei zwischen verschiedenen Gefahrenbereichen unterschieden, wobei in Bereichen, in denen eine Gefahr für Leib und Leben herrscht, hohe Anforderungen an die Safety-Funktionen gestellt werden. Regularien bezüglich Cybersecurity-Funktionen gibt es dagegen, je nach Anwendungsbereich, zum aktuellen Zeitpunkt nur wenige. Jedoch ist davon auszugehen, dass sich dies in Zukunft aufgrund der immer größer werdenden Relevanz ändert. Umso wichtiger ist es das Zusammenwirken von Security- und Safety-Funktionen zu berücksichtigen.

[0004] Eine Einhaltung der jeweiligen Regularien bezogen auf Safety-Funktionen wird üblicherweise von einer darauf spezialisierten Zulassungsstelle überprüft. Dies ist häufig, insbesondere in der Gasmesstechnik und der Medizintechnik, mit erhöhtem Aufwand verbunden, da die einwandfreie Funktionsweise sichergestellt und geprüft werden muss. Dementsprechend benötigt der Prozess der Zulassung eines Gerätes oder Systems bezüglich einer Norm seitens des Herstellers und der Zulassungsstelle üblicherweise viel Zeit. Dabei sind Zeiten von einigen Wochen bis hin zu einigen Monaten üblich.

[0005] Diesem hohen zeitlichen Aufwand steht die Notwendigkeit entgegen, auftretende Probleme im Hinblick auf Cybersecurity und des technischen Fortschritts, insbesondere bei bereits im Markt befindlichen Geräten oder Systemen, möglichst schnell zu beheben. Dabei ist es das Ziel, einen zumeist wirtschaftlichen Schaden zu verhindern oder zumindest zu begrenzen. Ferner ist es erforderlich, Cybersecurity-Funktionen auf dem neuesten Stand zu halten, also beispielsweise regelmäßig Software-Updates für Geräte und Systeme bereitzustellen, um der technischen Weiterentwicklung und somit auch möglichen neuen Problemen im Hinblick auf Cybersecurity, wie beispielsweise neuartige Angriffsmöglichkeiten, zu begegnen.

[0006] Der Erfindung liegt also die Aufgabe zu Grunde, eine Vorrichtung sowie ein Verfahren zur Ausführung von Cybersecurity-Funktionen und Safety-Funktionen bereitzustellen, wobei die Cybersecurity-Funktionen, insbesondere von im Markt befindlichen Geräten oder Systemen, in kurzer Zeit änderbar sein sollen, beispielsweise in Form eines Software-Updates. Dabei soll es möglich sein diese Änderungen unabhängig von den Safety-Funktionen durchzuführen, so dass die Safety-Funktionen von den Änderungen der Cybersecurity-Funktionen nicht beeinflusst werden. Hierdurch soll gewährleistet sein, dass die Safety-Funktionen weiterhin den von der Zulassungsstelle geprüften Regularien entsprechen, bestenfalls also keine erneute Zulassung erfolgen muss, und eine Änderung der Cybersecurity-Funktionen, beispielsweise in Form eines Software-Updates eines im Markt befindlichen Gerätes oder Systems, schnellstmöglich umsetzbar ist. Dabei soll sich eine Verbesserung der Verfügbarkeit eines Gerätes mit aktuellen Cybersecurity-Funktionen und zulassungskonformen Safety-Funktionen ergeben.

[0007] Die voranstehende Aufgabe wird durch eine Vorrichtung zur Ausführung von Cybersecurity-Funktionen und von Safety-Funktionen mit den Merkmalen des Anspruchs 1, einem Verfahren zur Ausführung von Cybersecurity-Funktionen und von Safety-Funktionen gemäß Anspruch 10, einem Gasmessgerät gemäß Anspruch 8, und einem Beatmungs- oder Anästhesiegerät gemäß Anspruch 9 gelöst. Weitere Details der Erfindung ergeben sich aus den abhängigen Ansprüchen, der Beschreibung und den Zeichnungen. Dabei gelten Merkmale und Details, die im Zusammenhang mit der erfindungsgemäßen Vorrichtung beschrieben sind, auch im Zusammenhang mit dem erfindungsgemäßen Verfahren, Gasmessgerät und Beatmungs- oder Anästhesiegerät, sodass bezüglich der Offenbarung zu den einzelnen Erfin-

dungsaspekten stets wechselseitig Bezug genommen wird oder vielmehr genommen werden kann.

[0008] Die erfindungsgemäße Vorrichtung zur Ausführung von Cybersecurity-Funktionen im Sinne der Informationssicherheit und von Safety-Funktionen im Sinne der Betriebssicherheit weist eine erste Recheneinheit zur Ausführung zumindest einer der Cybersecurity-Funktionen und eine zweite Recheneinheit zur Ausführung zumindest einer der Safety-Funktionen auf. Die erste Recheneinheit umfasst ein Kommunikationsmodul, das eine erste Schnittstelle aufweist und eingerichtet ist, eingehende Daten zu prüfen. Die zweite Recheneinheit umfasst ein Alarmmodul, welches eingerichtet ist, ein Informationssignal zu erzeugen. Zudem sind die erste Recheneinheit und die zweite Recheneinheit über eine Schnittstelle zum Datenaustausch miteinander verbunden.

[0009] Cybersecurity ist als Form der Informationssicherheit zu verstehen, wohingegen Safety als Form der Betriebssicherheit zu verstehen ist.

[0010] Dementsprechend umfassen Cybersecurity-Funktionen Maßnahmen zum Schutz von Informationen, insbesondere elektronischen Daten, vor Modifikation oder Einsichtnahme von Unbefugten. Solche Maßnahmen sind beispielsweise das Verschlüsseln von Daten oder die Authentifizierung von Kommunikationspartnern.

[0011] Safety-Funktionen umfassen Maßnahmen zum direkten oder indirekten Schutz von Lebewesen oder Objekten vor möglichen Gefahren, wie zum Beispiel giftige oder brennbare Gase, eine unzureichende Versorgung eines Patienten bei der Beatmung oder auch andere Gefahren, die zu Verletzungen oder Beschädigungen führen können. Dabei bedeutet ein direkter Schutz die Vermeidung von Gefahren, wobei eine Aktion ausgeführt wird, die die Gefahr unschädlich macht. Ein indirekter Schutz hingegen bedeutet das Hinweisen auf eine drohende Gefahr und/oder das Warnen vor einer drohenden Gefahr, wobei eine Information ausgegeben wird, die eine Gefahr anzeigt. Beispiele für Safety-Funktionen sind das Aktivieren einer Lüftungsanlage bei einer gefährlichen Gaskonzentration in einer Produktionshalle oder das Alarmieren in einem solchen Fall, das Aktivieren einer Notfall-Gasversorgung bei Ausfall der primären Gasversorgung eines Beatmungs- oder Anästhesiegeräts, oder das Alarmieren bei Beatmungsparametern in einem unerlaubten oder für den Patienten gefährlichen Bereich.

[0012] Unter einer Recheneinheit ist eine Einheit zum Ausführen eines Computerprogramms oder zum Ausführen von Software zu verstehen. Eine Recheneinheit kann als Prozessor, Mikroprozessor, zentrale Verarbeitungseinheit (Central Processing Unit, CPU) oder Prozessorkern ausgebildet sein. Weitere programmierbare Rechenwerke als Form der Recheneinheit, insbesondere Field Programmable Gate Arrays (FPGA) oder Application-Specific Integrated Circuits (ASIC), sind denkbar. Erfindungswesentlich an der Recheneinheit ist die Fähigkeit ein Computerprogramm oder eine Software unabhängig auszuführen, insbesondere unabhängig von weiteren Recheneinheiten.

[0013] Die erste Recheneinheit und die zweite Recheneinheit sind bevorzugt zwei Mikroprozessoren, die über die zweite Schnittstelle miteinander verbunden sind. Ferner ist denkbar, dass die erste und zweite Recheneinheit als erster und zweiter Prozessorkern auf einem Prozessor oder Mikroprozessor ausgebildet sind. Weitere Varianten, in denen beispielsweise die erste Recheneinheit als Mikroprozessor und die zweite Recheneinheit als FPGA ausgebildet sind oder die erste Recheneinheit als ASIC und die zweite Recheneinheit als Prozessorkern eines Mikroprozessors ausgebildet sind, sind ebenfalls denkbar. Wesentlich dabei ist, dass die erste und zweite Recheneinheit bezogen auf die Hardware voneinander getrennt sind. Daraus ergibt sich der besondere Vorteil, dass Computerprogrammprodukte oder Software zur Ausführung der Cybersecurity- oder Safety-Funktionen aufgrund der hardwareseitigen Trennung der ersten und zweiten Recheneinheit im Wesentlichen unabhängig voneinander sind. Dabei können sie getrennt voneinander entwickelt und/oder geändert werden sowie unabhängig voneinander lauffähig sein. Die zweite Schnittstelle, die die erste und zweite Recheneinheit zum Datenaustausch miteinander verbindet, ermöglicht dabei, dass sich die Computerprogramme der ersten und zweiten Recheneinheit gegenseitig beeinflussen können. Eine solche Beeinflussung ist aber nur in einem, während der Entwicklung der Computerprogramme, vorhergesehenen Maße möglich und somit vorgegeben, so dass sich spätere Änderungen des jeweiligen Computerprogramms an die vorgegebenen Schnittstelleneigenschaften und Schnittstellenfunktionen richten müssen. Daraus ergibt sich ebenfalls der Vorteil, dass die Computerprogramme, welche die Cybersecurity- und Safety-Funktionen implementieren, der ersten und zweiten Recheneinheit getrennt voneinander änderbar sind. Es ist also möglich, ein erstes Computerprogramm der ersten Recheneinheit zu ändern, ohne dabei ein zweites, bereits bestehendes Computerprogramm der zweiten Recheneinheit ändern zu müssen. Auf vorteilhafte Weise sind also zeitlich verschiedene Änderungszyklen eines jeweiligen Computerprogramms der ersten und zweiten Recheneinheit möglich und beispielsweise ein erstes Computerprogramm der ersten Recheneinheit wöchentlich änderbar und ein zweites Computerprogramm der zweiten Recheneinheit jährlich änderbar. Diese ver-

schiedenen Änderungszyklen sind deshalb vorteilhaft, da in der Praxis ein häufiges und schnelles Ändern von Cybersecurity-Funktionen notwendig ist, wohingegen Safety-Funktionen aufgrund der sich kaum ändernden Anforderungen üblicherweise nur selten geändert werden. Sofern Safety-Funktionen geändert werden, erfordert dies in der Regel eine neue Zulassung des mit den geänderten Safety-Funktionen ausgestatteten Geräts.

[0014] Die erste Recheneinheit umfasst das Kommunikationsmodul, welches eine sichere Kommunikation der erfindungsgemäßen Vorrichtung mit externen Kommunikationspartnern mittels Cybersecurity-Funktionen bereitstellt. Dabei umfasst das Kommunikationsmodul eine erste Schnittstelle, die geeignet ist, eingehende Daten von einem externen Kommunikationspartner zu empfangen. Ferner ist denkbar, dass die erste Schnittstelle eingerichtet ist, Daten an externe Kommunikationspartner zu senden. Die eingehenden Daten werden von dem Kommunikationsmodul geprüft. Wie zuvor erwähnt, kann eine solche Prüfung eine Authentifizierung des Kommunikationspartners umfassen und/oder die Prüfung der Daten, wobei beispielsweise auch eine Entschlüsselung von verschlüsselten Daten stattfinden kann. Weitere Maßnahmen zur Prüfung der Daten im Sinne der Informationssicherheit sind denkbar.

[0015] Die zweite Recheneinheit umfasst ein Alarmmodul, welches eine Safety-Funktion ausführt und eine Gefahrensituation bewertet. Eine Gefahrensituation ist beispielsweise eine Verletzung eines Grenzwertes für eine Gaskonzentration oder einen Beatmungsparameter. Unter einem Modul ist im Falle des Alarmmoduls und auch in den weiteren genannten Modulen, wie Sensormodul, Kommunikationsmodul, Nutzerinteraktionsmodul oder Speichermodul vorzugsweise ein Computerprogrammprodukt zu verstehen, welches eine Cybersecurity-Funktion, Safety-Funktion oder eine erweiterte Funktion auf einer Recheneinheit umsetzt. Dabei erzeugt das Alarmmodul ein Informationssignal, das anzeigt, ob eine Gefahrensituation vorliegt. Ein solches Informationssignal kann als analoges und/oder digitales Informationssignal ausgebildet sein. Beispielsweise steuert ein analoges Informationssignal eine optische, akustische und/oder haptische Alarmierungseinheit in Form einer LED, einer Hupe und/oder eines Vibrationsmotors. Ein digitales Informationssignal steuert beispielsweise eine Anzeigeeinheit in Form eines Displays und/oder wird über eine digitale Schnittstelle an einen externen Kommunikationspartner zur weiteren Verarbeitung übertragen.

[0016] Die zuvor beschriebene zweite Schnittstelle verbindet die erste und zweite Recheneinheit, so dass diese Daten miteinander austauschen können. Der Datenaustausch findet dabei zumindest von der ersten Recheneinheit zur zweiten Recheneinheit statt. Somit ist es möglich, dass eingehende Daten, die zuvor von der Kommunikationseinheit der ersten Recheneinheit geprüft wurden, an die zweite Recheneinheit und somit an das Alarmmodul weiterzuleiten, welches ein Informationssignal erzeugt. Auf vorteilhafte Weise sind beispielsweise Parameter des Alarmmoduls änderbar, die Einfluss auf das Informationssignal haben. Solche Parameter können beispielsweise geänderte Alarmschwellen beinhalten oder das Alarmverhalten des Alarmmoduls beeinflussen. Ferner ist denkbar, dass die eingehenden Daten das Alarmmodul dazu veranlassen ein Informationssignal unter Berücksichtigung dieser Daten zu erzeugen. Beispielsweise ist es denkbar, dass ein Alarmsignal an die erfindungsgemäße Vorrichtung gesendet wird, welches zunächst im Sinne der Informationssicherheit von der ersten Recheneinheit geprüft und anschließend von der zweiten Recheneinheit und dem Alarmmodul im Sinne der Betriebssicherheit ausgegeben wird, also zum Beispiel, wie zuvor beschrieben, eine optische, akustische und/oder haptische Alarmierungseinheit angesteuert wird.

[0017] Die zweite Schnittstelle ist derart eingerichtet, dass ausschließlich Daten von der ersten zur zweiten Recheneinheit und/oder von der zweiten zur ersten Recheneinheit übertragbar sind, die für eine Datenübertragung vorgesehen wurden. Es handelt sich also um eine definierte Schnittstelle, wobei die möglichen Daten während der Entwicklung festgelegt wurden. Daraus ergibt sich eine Entkopplung der ersten und zweiten Recheneinheit sowie des Kommunikationsmoduls und des Alarmmoduls, wobei eine Beeinflussung lediglich durch einen definierten Datenaustausch über die zweite Schnittstelle möglich ist. Auf vorteilhafte Weise ist beispielsweise eine eigenständige Lauffähigkeit der ersten und zweiten Recheneinheit umsetzbar, so dass, wie zuvor beschrieben, eine Änderung der Funktionalität der ersten Recheneinheit, insbesondere der Funktionalität des Kommunikationsmoduls, unabhängig von der Funktionalität der zweiten Recheneinheit, insbesondere der Funktionalität des Alarmmoduls, und umgekehrt änderbar ist.

[0018] Der besondere Vorteil der erfindungsgemäßen Vorrichtung ist, dass die Vorrichtung geeignet ist, Cybersecurity- und Safety-Funktionen auszuführen, wobei die Ausführung der Cybersecurity- und Safety-Funktionen aufgrund der hardwareseitigen Trennung der ersten und zweiten Recheneinheit derart voneinander unabhängig sind, dass sie getrennt voneinander änderbar sind. Daraus ergibt sich beispielsweise die Möglichkeit die Cybersecurity-Funktionen zu ändern, ohne dabei die Safety-Funktionen zu beeinflussen, so dass eine Änderung der Safety-Funktion aufgrund einer Änderung der Cybersecurity-Funktionen nicht erforderlich ist. Auf Vorteilhafte Weise sind die Cybersecurity-Funktionen der ersten

Recheneinheit kurzfristig änderbar, ohne beispielsweise einen erneuten, oft langwierigen Zulassungsprozess der Safety-Funktionen der zweiten Recheneinheit durchführen zu müssen.

[0019] In einer bevorzugten Ausführungsform der Vorrichtung ist die erste Recheneinheit konfiguriert auf einen ersten Datenspeicher zuzugreifen und die zweite Recheneinheit konfiguriert auf einen zweiten Datenspeicher zuzugreifen. Dabei beinhaltet das Zugreifen auf den jeweiligen Datenspeicher das Lesen und/oder Schreiben von Daten.

[0020] Ein Datenspeicher bezeichnet einen Speicherbereich zur Speicherung von digitalen Daten auf einem oder mehreren Speichermedien oder Datenträgern. Der erste und zweite Datenspeicher sind bevorzugt als Halbleiterspeicher ausgestaltet. Ein solcher Halbleiterspeicher ist beispielsweise ein flüchtiger oder bevorzugt ein nicht-flüchtiger Speicher. Der erste Datenspeicher umfasst einen Halbleiterspeicher und der zweite Datenspeicher umfasst einen davon separaten Halbleiterspeicher. Ferner ist denkbar, dass der erste und zweite Datenspeicher einen gemeinsamen Halbleiterspeicher umfassen oder der jeweilige Datenspeicher mehrere Halbleiterspeicher umfasst.

[0021] Die erste Recheneinheit ist eingerichtet, Daten vom ersten Datenspeicher zu lesen und/oder Daten auf den ersten Datenspeicher zu schreiben. Beispielsweise handelt es sich bei den Daten des ersten Datenspeichers um Daten, die über die erste Schnittstelle empfangen wurden und/oder Computerprogrammdaten zur Ausführung der Cybersecurity-Funktionen. Die zweite Recheneinheit ist eingerichtet, Daten vom zweiten Datenspeicher zu lesen und/oder Daten auf den zweiten Datenspeicher zu schreiben. Beispielsweise handelt es sich bei den Daten des zweiten Datenspeichers um Computerprogrammdaten zur Ausführung der Safety-Funktionen und/oder Parameter zur Bewertung einer Alarmsituation.

[0022] Gemäß einer bevorzugten Ausführungsform der Vorrichtung sind der erste Datenspeicher und der zweite Datenspeicher nichtüberlappend. Dabei ist der Speicherbereich des ersten Datenspeichers vom Speicherbereich des zweiten Datenspeichers getrennt. Demzufolge sind Daten des ersten Datenspeichers ausschließlich von der ersten Recheneinheit zugreifbar und Daten des zweiten Datenspeichers ausschließlich von der zweiten Recheneinheit zugreifbar. Auf vorteilhafte Weise ist durch die Trennung der Daten des ersten und zweiten Datenspeichers gewährleistet, dass die jeweilige Recheneinheit lediglich Zugriff auf einen für sie bestimmten Speicherbereich hat und somit auch nur diese Daten lesen und/oder schreiben kann. Eine gegenseitige Beeinflussung der Recheneinheiten, und somit auch der Ausführung der Safety- und Cybersecurity-Funktionen, durch den direkten Zugriff auf Daten des jeweiligen, anderen Datenspeichers ist folglich ausgeschlossen.

[0023] Es ist denkbar, dass die Vorrichtung zusätzlich eine Speicherschutzeinheit (Memory Protection Unit, MPU) umfasst, welche den ersten und/oder den zweiten Datenspeicher vor unerlaubtem Zugriff schützt. Dabei wäre ein unerlaubter Zugriff beispielsweise das Lesen von Daten der ersten Recheneinheit aus dem zweiten Datenspeicher oder das Schreiben der ersten Recheneinheit auf den ersten Datenspeicher.

[0024] In einer bevorzugten Ausführungsform der Vorrichtung ist die erste Recheneinheit eingerichtet, die zumindest eine Cybersecurity-Funktion unabhängig von der zweiten Recheneinheit auszuführen und die zweite Recheneinheit ist eingerichtet, die zumindest eine Safety-Funktion unabhängig von der ersten Recheneinheit auszuführen. Eine solche Entkopplung der Ausführung der Funktionen der ersten und der zweiten Recheneinheit gewährleistet, dass die zumindest eine Cybersecurity-Funktion und die zumindest eine Safety-Funktion wie vorgesehen ausführbar sind. Eine Störung oder Unterbrechung der Ausführung der zumindest einen Cybersecurity-Funktion durch die zweite Recheneinheit und/oder der Ausführung der zumindest einen Safety-Funktionen durch die erste Recheneinheit ist dementsprechend ausgeschlossen. Der besondere Vorteil dabei ist die erhöhte Zuverlässigkeit der Ausführung der jeweiligen Funktion, wobei die zumindest eine Safety-Funktion beispielsweise selbst in dem Fall ausführbar ist, in dem die erste Recheneinheit und/oder dessen Funktion eine Störung aufweist oder ausgefallen ist. Dabei ist vorzugsweise sichergestellt, dass eine Datenübertragung zwischen der ersten und zweiten Recheneinheit zumindest seitens der zweiten Recheneinheit unterbunden ist, beispielsweise indem die zweite Recheneinheit die Störung der ersten Recheneinheit und/oder dessen Funktion feststellt und eine Datenübertragung blockiert. Ferner ist die zumindest eine Cybersecurity-Funktion auch in solchen Fällen ausführbar, in denen die zweite Recheneinheit und/oder dessen Funktion gestört oder ausgefallen ist. Im letztgenannten Fall liegt ein weiterer Vorteil darin, dass die Störung oder der Ausfall der zweiten Recheneinheit und/oder dessen Funktion vorzugsweise von der ersten Recheneinheit detektierbar ist, welche diese Information anschließend durch das Kommunikationsmodul über die erste Schnittstelle an externe Kommunikationspartner weiterleiten kann. Eine derartige Informationsweiterleitung sorgt auf vorteilhafte Weise für eine erhöhte Betriebssicherheit, da auf die Störung oder den Ausfall reagiert und beispielsweise eine Reparatur der Vorrichtung beauftragt oder ein Verlassen eines vermeintlichen Gefahren-

bereichs angeordnet werden kann. In jedem Fall ist die bestimmungsgemäße Ausführung der zumindest einen Cybersecurity-Funktion der ersten Recheneinheit und der Safety-Funktion der zweiten Recheneinheit nicht durch eine Störung oder den Ausfall der jeweils anderen Recheneinheit und/oder deren Funktion beeinflussbar.

[0025] Gemäß einer bevorzugten Ausführungsform der Vorrichtung umfasst die zweite Recheneinheit ein Sensormodul zur Erfassung von Sensordaten. Zur Bewertung von unmittelbaren Gefahrensituationen ist es notwendig, Informationen über aktuelle Gegebenheiten zu ermitteln. Das Sensormodul zur Erfassung von Sensordaten dient, wie das Alarmmodul zur Erzeugung eines Informationssignals, ebenfalls der Betriebssicherheit. Dabei werden Messungen von einem oder mehreren Sensoren durchgeführt und die Messdaten vom Sensormodul zur weiteren Verarbeitung erfasst. Ein häufiges Anwendungsbeispiel ist dabei die Bewertung einer Alarmsituation mittels der erfassten Messdaten und die Ausgabe des Ergebnisses der Bewertung. Das Sensormodul ist dabei an den jeweiligen Sensor angepasst. Beispielsweise ist das Sensormodul eingerichtet Sensordaten bezüglich einer Gaskonzentration, einer Temperatur, einer Atemfrequenz und/oder eines Tidalvolumens zu erfassen. Das Sensormodul ist bevorzugt Bestandteil eines Mikroprozessors der zweiten Recheneinheit, der das Alarmmodul umfasst. Es ist denkbar, dass das Sensormodul und das Alarmmodul Bestandteile separater Einheiten, beispielsweise zweier Mikroprozessoren oder zweier Prozessorkerne, der zweiten Recheneinheit sind. Ferner ist denkbar, dass die zweite Recheneinheit mehrere Sensormodule umfasst, so dass die Sensordaten verschiedener Sensoren erfassbar sind. Das Sensormodul ermöglicht durch die Erfassung von Sensordaten auf vorteilhafte Weise die Bewertung einer direkten Gefahrenlage, beispielsweise in der unmittelbaren Umgebung der Vorrichtung.

[0026] In einer bevorzugten Ausführungsform der Vorrichtung umfasst die erste Recheneinheit und/oder die zweite Recheneinheit ein Speichermodul zur Verwaltung von Daten auf einem Speichermedium. Dabei ist das jeweilige Speichermodul auf die Art des Speichermediums angepasst. Es sind Speichermedien zu unterscheiden, auf die lediglich von einer Recheneinheit der Vorrichtung zugreifbar ist, beispielsweise der RAM (Random-Access Memory) eines Mikroprozessors der ersten Recheneinheit, und Speichermedien, auf die zusätzlich von weiteren, nicht zur Vorrichtung gehörenden, Recheneinheiten zugreifbar ist, beispielsweise eine Speicherkarte (SD-Karte), die aus der Vorrichtung entfernbar ist. Im ersten Fall ist das Speichermodul Bestandteil der ersten und/oder zweiten Recheneinheit. Im zweiten Fall ist das Speichermodul Bestandteil der ersten Recheneinheit, da in diesem Fall beispielsweise eine Manipulation der Daten durch eine nicht zur Vorrichtung gehörenden Recheneinheit möglich ist und entsprechende Cybersecurity-Funktionen notwendig sind, um eine solche Manipulation zu verhindern oder zumindest zu erkennen. Eine geeignete Cybersecurity-Funktion ist beispielsweise das Verschlüsseln der Daten auf dem Speichermedium, sodass sichergestellt ist, dass nur befugte Anwender mit einem entsprechendem Sicherheitsschlüssel diese Daten lesen und/oder ändern können. Auf vorteilhafte Weise ist das Speichermodul demzufolge an unterschiedliche Arten von Speichermedien anpassbar und entsprechend des jeweiligen Speichermediums Bestandteil der geeigneten Recheneinheit der Vorrichtung.

[0027] Gemäß einer bevorzugten Ausführungsform weist die Vorrichtung eine dritte Recheneinheit auf, welche ein Nutzerinteraktionsmodul zur Eingabe und/oder Ausgabe von Informationen umfasst. Ferner ist die dritte Recheneinheit zum Datenaustausch mit der ersten und/oder zweiten Recheneinheit verbindbar oder verbunden. Das Nutzerinteraktionsmodul umfasst dabei Funktionen, die der komfortablen Bedienung und Anwendung der Vorrichtung dienen und weder direkten Einfluss auf die Informationssicherheit noch auf die Betriebssicherheit haben.

[0028] Die Eingabe von Informationen ist dabei derart beschränkt, dass eine Manipulation der ersten und zweiten Recheneinheit und deren Cybersecurity- und Safety-Funktionen nicht möglich ist. Demzufolge sind die erste und zweite Recheneinheit unabhängig von der dritten Recheneinheit und die Informationssicherheit der Vorrichtung weiterhin gewährleistet. Die Ausgabe von Informationen durch die dritte Recheneinheit umfasst lediglich solche Informationen, die für die Betriebssicherheit unwesentlich sind und/oder bei denen es sich um wenigstens eine zusätzlich angezeigte Information handelt. Beispielsweise ist es denkbar, dass eine Information über eine erkannte Gefahrensituation , beispielsweise die Verletzung eines Grenzwerts für wenigstens eine Gaskonzentration oder einen Beatmungsparameter, von dem Alarmmodul der zweiten Recheneinheit erzeugt wird, welches vorzugsweise eine optische, akustische und/oder haptische Alarmierungseinheit in Form einer LED, einer Hupe und/oder eines Vibrationsmotors ansteuert und zusätzlich die Information über die erkannte Gefahrensituation der dritten Recheneinheit zur Verfügung stellt. Die dritte Recheneinheit ist beispielsweise eingerichtet ein Display anzusteuern und die Information über erkannte Gefahrensituation auf dem Display anzeigen zu lassen. Eine solche Ausgabe der Information durch die dritte Recheneinheit stellt eine zusätzliche Informationsanzeige dar, die im Sinne der Betriebssicherheit als optional angesehen werden kann, da sie redundant gegenüber der Ansteuerung der

Alarmierungseinheit durch das Alarmmodul ist und somit nicht als Safety-Funktion angesehen werden muss. In diesem Beispiel ist die Safety-Funktion im Sinne der Betriebssicherheit, hier das Warnen vor oder in einer Gefahrensituation, durch das Alarmmodul der zweiten Recheneinheit und das Ansteuern der optischen, akustischen und/oder haptischen Alarmierungseinheit gewährleistet.

[0029] Auf vorteilhafte Weise bietet die dritte Recheneinheit eine Erweiterung des Funktionsumfanges der Vorrichtung, ohne dabei Einfluss auf die erste und zweite Recheneinheit sowie die Cybersecurity- und Safety-Funktion zu nehmen. Demzufolge ist eine Änderung der Cybersecurity-Funktion und der Safety-Funktion unabhängig von der dritten Recheneinheit und deren erweiterten Funktionen durchführbar.

[0030] Ferner betrifft die Erfindung ein Verfahren zur Ausführung von Cybersecurity-Funktionen im Sinne der Informationssicherheit und von Safety-Funktionen im Sinne der Betriebssicherheit auf einer Vorrichtung mit einer ersten Recheneinheit und mit einer zweiten Recheneinheit. Das Verfahren weist folgende Schritte auf:

- Empfangen und Prüfen von Daten mit einem Kommunikationsmodul der ersten Recheneinheit,

- Speichern der Daten in einem ersten Datenspeicher und/oder Übertragen der Daten an eine zweite Recheneinheit,

- Auswerten der Daten bezüglich einer Alarmsituation mit einem Alarmmodul der zweiten Recheneinheit, und

- Erzeugen eines Informationssignals durch das Alarmmodul

[0031] Das Verfahren ist geeignet von der zuvor beschriebenen, erfindungsgemäßen, oder einer der zuvor beschriebenen Ausführungsformen weitergebildeten Vorrichtung ausgeführt zu werden. Dabei führt die erste Recheneinheit zumindest eine Cybersecurity-Funktion und die zweite Recheneinheit zumindest eine Safety-Funktion aus. Zum Schutz der Informationssicherheit werden vom Kommunikationsmodul empfangene Daten geprüft, wobei beispielsweise festgestellt wird, ob die Daten von einem zur Kommunikation berechtigten Absender geschickt worden sind oder ob die Integrität der Daten gewährleistet ist, also ob die Daten korrekt, vollständig und konsistent sind. Ferner ist denkbar, dass die Daten verschlüsselt empfangen worden sind und das Kommunikationsmodul die Daten entschlüsselt.

[0032] In einem weiteren Verfahrensschritt werden die Daten, deren Informationssicherheit geprüft wurde, abgespeichert und/oder an die zweite Recheneinheit übertragen. Zur Übertragung weist die Vorrichtung eine zweite Schnittstelle auf, die die erste Recheneinheit mit der zweiten Recheneinheit zum Datenaustausch verbindet. Die Daten können also in dem Datenspeicher, auf den lediglich die erste Recheneinheit Zugriff hat, gespeichert werden und beispielsweise zu einem späteren Zeitpunkt oder direkt an die zweite Recheneinheit weitergeleitet werden. Die Daten können dabei beispielsweise Informationen über eine erkannte Gefahrensituation enthalten, die eine externe Leitwarte oder ein externe Überwachungseinrichtung an die Vorrichtung gesendet hat.

[0033] In einem weiteren Verfahrensschritt werden die geprüften und übertragenen Daten von dem Alarmmodul der zweiten Recheneinheit ausgewertet. Wie zuvor erwähnt kann es sich bei den Daten beispielsweise um Informationen über eine Gefahrensituation handeln. Ferner sind andere Informationen denkbar, beispielsweise eine Information zur Konfiguration des Alarmmoduls, wie Grenzwerte oder Alarmierungsverhalten, sowie andere Einstellungen oder Informationen bzgl. einer Safety-Funktion.

[0034] In einem nächsten Schritt erzeugt das Alarmmodul auf Basis der Auswertung ein Informationssignal. Dieses Informationssignal kann zur Ansteuerung einer akustischen und/oder optischen Alarmierungseinheit dienen, oder ein digitales Signal sein, welches beispielsweise über das Kommunikationsmodul an eine Leitwarte gesendet wird.

[0035] Auf vorteilhafte Weise ist das Verfahren geeignet eine Cybersecurity-Funktion und eine Safety-Funktion auszuführen, wobei diese auf unterschiedlichen Recheneinheiten ausgeführt werden und unabhängig voneinander sind, so dass insbesondere die Cybersecurity-Funktion geändert werden kann, ohne dass dabei die Safety-Funktion geändert werden muss.

[0036] In einer bevorzugten Ausführungsform des Verfahrens wird ein Sensormesswert mit einem Sensormodul der zweiten Recheneinheit ermittelt. Dieser Sensormesswert wird vorzugsweise mit den Rohdaten eines zur Vorrichtung gehörenden oder mit ihr verbundenen Sensors ermittelt. Denkbar ist auch, dass der Sensormesswert mit Daten von einem externen Kommunikationspartner ermittelt wird, der diese Daten an die Vorrichtung gesendet hat. Ferner findet eine Auswertung des Sensormesswertes bezüglich einer Alarmsituation durch das Alarmmodul statt. Dabei führt das Sensormodul eine Safety-Funktion im Sinne der Betriebssicherheit aus und ermittelt beispielsweise einen Sensormesswert einer Gaskonzentration oder einer Atemfrequenz. Der Sensormesswert wird anschließend durch das Alarmmodul beispielsweise mit einem Grenzwert

verglichen, um festzustellen, ob eine Alarmsituation vorliegt. Eine Alarmsituation kann beispielsweise vorliegen, wenn ein Sensormesswert den Grenzwert verletzt. Das Verfahren bietet den besonderen Vorteil, dass die Safety-Funktionen, hier das Ermitteln und Auswerten eines Sensormesswertes, gemeinsam auf einer zweiten Recheneinheit ausgeführt werden, sodass sie von einer ersten Recheneinheit, welche zumindest eine Cybersecurity-Funktion ausführt, unabhängig ist.

[0037] In einer bevorzugten Ausführungsform des Verfahrens werden Informationen der zweiten Recheneinheit in einem zweiten Datenspeicher gespeichert, wobei der zweite Datenspeicher und der erste Datenspeicher nichtüberlappend sind. Wie zuvor beschrieben bezeichnet ein Datenspeicher einen gewissen Speicherbereich eines oder mehrerer Speichermedien, beispielsweise Halbleiterspeicher. Der erste und zweite Datenspeicher werden derart konfiguriert, dass sie keine gemeinsamen Dateninhalte besitzen. Das heißt, dass Daten entweder im ersten oder im zweiten Datenspeicher abgespeichert werden. Daraus folgt, dass die erste Recheneinheit nicht auf die Daten des zweiten Datenspeichers zugreifen kann und die zweite Recheneinheit nicht auf die Daten des ersten Datenspeichers zugreifen kann. Auf vorteilhafte Weise sind die Daten also derart voneinander getrennt, dass nur eine der beiden Recheneinheiten darauf Zugriff hat. Diese Zugriffsbeschränkung trägt zur Entkopplung der ersten und zweiten Recheneinheit und somit der Cybersecurity- und Safety-Funktionen bei.

[0038] Es ist denkbar, dass der erste und zweite Datenspeicher durch eine Speicherschutzeinheit (Memory Protection Unit, MPU) vor unerlaubtem Zugriff geschützt werden. Dabei wäre ein unerlaubter Zugriff beispielsweise das Lesen von Daten der ersten Recheneinheit aus dem zweiten Datenspeicher oder das Schreiben der ersten Recheneinheit auf den ersten Datenspeicher.

[0039] Gemäß einer bevorzugten Ausführungsform des Verfahrens findet ein Empfangen und/oder Ausgeben von Informationen mit einem Nutzerinteraktionsmodul einer dritten Recheneinheit der Vorrichtung statt, wobei vorzugsweise eine Datenübertragung zwischen der zweiten und dritten Recheneinheit stattfindet. Das Nutzerinteraktionsmodul umfasst dabei vorzugsweise Funktionen, die der komfortablen Bedienung und Anwendung der Vorrichtung dienen und weder direkten Einfluss auf die Informationssicherheit noch auf die Betriebssicherheit haben. Wie zuvor beschrieben sind die erste und zweite Recheneinheit unabhängig von der dritten Recheneinheit, so dass die bestimmungsgemäße Ausführung der Cybersecurity-Funktionen und der Safety-Funktionen durch die erste und zweite Recheneinheit nicht durch die dritte Recheneinheit gestört werden kann. Ferner sind die Cybersecurity-Funktionen und die Safety-Funktionen unabhängig von den Funktionen der dritten Recheneinheit änderbar sowie die Funktionen der dritten Recheneinheit unabhängig von den Funktionen der ersten (Cybersecurity-Funktionen) und zweiten Recheneinheit (Safety-Funktionen) änderbar. Auf vorteilhafte Weise bietet die dritte Recheneinheit eine Erweiterung des Funktionsumfanges der Vorrichtung, ohne dabei Einfluss auf die erste und zweite Recheneinheit zu nehmen. Demzufolge ist eine Änderung der Cybersecurity-Funktion unabhängig von der dritten Recheneinheit und deren erweiterten Funktionen durchführbar.

[0040] Weitere Merkmale, Aufgaben und Wirkungen der Erfindung ergeben sich aus der folgenden Beschreibung spezieller Ausführungsbeispiele und den beigefügten Figuren. Es werden Ausführungsbeispiele der Erfindung beschrieben, ohne den allgemeinen Erfindungsgedanken zu beschränken.

[0041] Ferner betrifft die Erfindung ein Gasmessgerät mit einer Vorrichtung, die gemäß einer der zuvor beschriebenen Ausführungsformen gestaltet ist und/oder das ein Verfahren gemäß wenigstens einer der zuvor beschriebenen Ausgestaltungen ausführen kann.

[0042] Das vorgeschlagene Gasmessgerät kann als ein mobiles oder ein stationäres, also ortsunveränderliches, Gasmessgerät ausgestaltet sein und umfasst die Vorrichtung sowie vorzugsweise eine Alarmierungseinheit und einen oder mehrere Sensoren, wobei die Alarmierungseinheit und die Sensoren mit der zweiten Recheneinheit der Vorrichtung zum Informationsaustausch verbunden sind. Die Alarmierungseinheit kann einen akustischen und/oder optischen Signalgeber aufweisen. Die Sensoren können in der Lage sein, verschiedene giftige oder brennbare Gase zu messen.

[0043] Auf vorteilhafte Weise ist das Gasmessgerät in Bezug auf die Informationssicherheit und in Bezug auf die Betriebssicherheit zuverlässig einsetzbar, wobei Cybersecurity-Funktionen und Safety-Funktionen unabhängig voneinander ausführbar sind. Durch die Trennung dieser Funktionalitäten ist ein zuverlässiger Betrieb und eine effiziente Wartung des Gasmessgerätes gewährleitstet. Dabei ist unter Wartung insbesondere die Notwendigkeit einer Änderung und Anpassung der Cybersecurity-Funktionen an neue Anforderungen sowie neue Technologien zu verstehen. Auf besonders vorteilhafte Weise ist also eine Änderung der Cybersecurity-Funktionen, beispielsweise eine Anpassung an neuere Security-Standards, durchführbar, ohne dabei die Safety-Funktionen zu beeinflussen, wobei eine erneute Zulassungsprüfung der Safety-Funktionen entfallen

kann und die Änderungen der Cybersecurity-Funktionen nach deren Umsetzung verfügbar sind.

[0044] Ferner betrifft die Erfindung ein Beatmungs- oder Anästhesiegerät mit einer Vorrichtung, die gemäß einer der zuvor beschriebenen Ausführungsformen gestaltet ist und/oder das ein Verfahren gemäß wenigstens einer der zuvor beschriebenen Ausgestaltungen ausführen kann.

[0045] Das vorgeschlagene Beatmungs- oder Anästhesiegerät umfasst die Vorrichtung sowie vorzugsweise eine Alarmierungseinheit und einen oder mehrere Sensoren, wobei die Alarmierungseinheit und die Sensoren mit der zweiten Recheneinheit der Vorrichtung zum Informationsaustausch verbunden sind. Die Alarmierungseinheit kann einen akustischen und/oder optischen Signalgeber aufweisen. Die Sensoren können in der Lage sein, verschiedene Beatmungsparameter zu erfassen.

[0046] Auf vorteilhafte Weise ist das Beatmungs- oder Anästhesiegerät in Bezug auf die Informationssicherheit und in Bezug auf die Betriebssicherheit zuverlässig einsetzbar, wobei Cybersecurity-Funktionen und Safety-Funktionen unabhängig voneinander ausführbar sind. Durch die Trennung dieser Funktionalitäten ist ein zuverlässiger Betrieb und eine effiziente Wartung des Beatmungs- oder Anästhesiegerät gewährleitstet. Dabei ist unter Wartung insbesondere die Notwendigkeit einer Änderung und Anpassung der Cybersecurity-Funktionen an neue Anforderungen sowie neue Technologien zu verstehen. Auf besonders vorteilhafte Weise ist also eine Änderung der Cybersecurity-Funktionen, beispielsweise eine Anpassung an neuere Security-Standards, durchführbar, ohne dabei die Safety-Funktionen zu beeinflussen, wobei eine erneute Zulassungsprüfung der Safety-Funktionen entfallen kann und die Änderungen der Cybersecurity-Funktionen nach deren Umsetzung verfügbar sind.

[0047] In den Figuren zeigt:

Fig. 1: eine schematische Darstellung einer Ausführungsform der erfindungsgemäßen Vorrichtung,

Fig. 2: eine schematische Darstellung einer Ausführungsform des erfindungsgemäßen Gasmessgerätes, und

Fig. 3: eine schematische Darstellung einer Ausführungsform des erfindungsgemäßen Beatmungs- oder Anästhesiegerätes.

[0048] Nachstehend werden Ausführungsbeispiele der Erfindung anhand der beigefügten Figuren im Einzelnen beschrieben. Dabei sind gleichartige Bauteile in mehreren Figuren jeweils mit den gleichen Bezugszeichen versehen.

[0049] **Fig.** 1 zeigt ein bevorzugtes Ausführungsbeispiel der erfindungsgemäßen Vorrichtung 10 anhand einer schematischen Darstellung mit einer ersten Recheneinheit 1 und einer zweiten Recheneinheit 2, die über eine zweite Schnittstelle 6 zum Datenaustausch miteinander verbunden sind. Die erste Recheneinheit 1 ist eingerichtet, eine Cybersecurity-Funktion auszuführen und umfasst ein Kommunikationsmodul 3, welches eine erste Schnittstelle 5 aufweist. Die erste Schnittstelle 5 ist eingerichtet, Daten von einem externen Kommunikationspartner 7, in diesem Fall drahtlos übertragene Daten, wie mit dem gestrichelten Pfeil angedeutet, zu empfangen. Das Kommunikationsmodul 3 ist eingerichtet, eingehenden Daten zu prüfen. Die zweite Recheneinheit 2 ist eingerichtet, eine Safety-Funktion auszuführen und umfasst ein Alarmmodul, welches eingerichtet ist, ein Informationssignal INS zu erzeugen. Das Alarmmodul 4 ist zum Datenaustausch, wie mit dem gestrichelten Pfeil angedeutet, mit einer Alarmierungseinheit 8 verbunden, wobei die Alarmierungseinheit 8 ausgebildet ist, einen akustischen, haptischen und/oder optischen Alarm zu erzeugen.

[0050] Die erste und zweite Recheneinheit 1,2 sind jeweils als Mikroprozessor ausgebildet und über die zweite Schnittstelle 6 in Form einer UART-Schnittstelle (Universal Asynchronous Receiver Transmitter - Schnittstelle) zum Datenaustausch miteinander verbunden. Über die erste Schnittstelle 5 sind Daten eines externen Kommunikationspartners 7, beispielsweise in Form einer Leitwarte, empfangbar. Die Daten des externen Kommunikationspartners 7 können beispielsweise Alarminformationen beinhalten, also Informationen, ob eine Gefahrensituation vorliegt oder nicht. Das Kommunikationsmodul 3 ist eingerichtet, die Daten des externen Kommunikationspartners 7 zu prüfen. Dabei findet eine Authentifizierung des externen Kommunikationspartners 7 und eine Integritätsprüfung der Daten statt.

[0051] Sofern der externe Kommunikationspartner 7 eine Alarminformation gesendet hat, empfängt das Kommunikationsmodul 3 diese Alarminformation und prüft sie im Sinne der Informationssicherheit. Hat die Prüfung ergeben, dass der externe Kommunikationspartner vertrauenswürdig und/oder bekannt ist und der Inhalt der Daten, also die Alarminformationen, korrekt im Sinne der Datenintegrität sind, so leitet die erste Recheneinheit 1 die Alarminformation an die zweite Recheneinheit 2 über die zweite Schnittstelle 6 weiter. Das Alarmmodul 4 der zweiten Recheneinheit 2 übernimmt die Alarminformation, wertet diese aus und steuert die Alarmierungseinheit 8 entsprechend der Alarminformation an. Hat die Prüfung hingegen ergeben, dass der externe Kommunikationspartner 7 nicht vertrauenswürdig und/oder bekannt ist, so wird die Alarminformation verworfen und nicht an die zweite Recheneinheit weitergeleitet.

[0052] Dabei ist die erste Recheneinheit 1 mit einem ersten Datenspeicher 11 und die zweite Recheneinheit 2 mit einem zweiten Datenspeicher 12 verbunden. Die Datenspeicher 11, 12 sind jeweils als eigenständiger Halbleiterspeicher ausgebildet.

[0053] Im Fall, dass der externe Kommunikationspartner 7, eine Informationen bezogen auf eine Änderung der Funktionsweise des Kommunikationsmoduls 3 gesendet hat, wobei es sich um ein Software-Update handelt, und die Authentifizierung erfolgreich von dem Kommunikationsmodul 3 durchgeführt wurde, speichert das Kommunikationsmodul 3 diese Informationen im ersten Datenspeicher 11 ab und die erste Recheneinheit 1 führt anschließend ein Software-Update des Kommunikationsmoduls 3 durch, wobei die Funktionsweise des Alarmmoduls 4 nicht beeinflusst wird.

[0054] **Fig.** 2 zeigt ein bevorzugtes Ausführungsbeispiel des erfindungsgemäßen Gasmessgerätes mit einer Ausführungsform der erfindungsgemäßen Vorrichtung 10, einem Gassensor 25 und einer Alarmierungseinheit 8. Die Vorrichtung 10 entspricht im Wesentlichen der Vorrichtung 10, wie sie in **Fig.** 1 dargestellt und zuvor beschrieben ist. Zusätzlich umfasst die Vorrichtung 10 einen Halbleiterspeicher 23 mit einem ersten Datenspeicher 21 und einem zweiten Datenspeicher 22, wobei der erste Datenspeicher 21 von der ersten Recheneinheit 1 und der zweite Datenspeicher von der zweiten Recheneinheit 2 zugreifbar ist, dargestellt mittels gestrichelter Linien. Die Datenspeicher 21, 22 bilden zwei separate Speicherbereiche des Halbleiterspeichers 23, die sich nicht überlappen, also voneinander getrennt sind. Ferner umfasst die zweite Recheneinheit 2 der Vorrichtung 10 ein Sensormodul 24 zur Erfassung von Sensordaten des Gassensors 25. Dabei ist das Sensormodul 24 mit dem Sensor 25 zum Empfangen eines Sensorsignals verbunden, dargestellt mittels der gestrichelten Linie. Es ist denkbar, jedoch in **Fig.** 2 nicht dargestellt, dass das Sensormodul 24 oder mehrere Sensormodule mehrere Sensorsignale von mehreren Gassensoren erfassen.

[0055] Wie zuvor beschrieben ist das Kommunikationsmodul 3 der ersten Recheneinheit 1 eingerichtet, eingehende Daten eines externen Kommunikationspartners 7 zu prüfen, wobei die Daten über eine erste Schnittstelle 5 empfangen werden. Der externe Kommunikationspartner 7 ist beispielsweise eine externe Leitwarte zur Überwachung und Steuerung von Gasmessgeräten. Die Daten können dabei beispielsweise Alarminformationen oder Alarmparameter zur Konfiguration des Alarmmoduls 4 der zweiten Recheneinheit 2 sein. Die erste und die zweite Recheneinheit sind über die zweite Schnittstelle zum Datenaustausch miteinander verbunden, so dass die zuvor genannten Alarminformationen oder Alarmparameter an die zweite Recheneinheit 2 und somit an das Alarmmodul 4 übertragbar sind. Vor einer solchen Übertragung findet, wie in der Beschreibung zu **Fig.** 1, eine Prüfung der eingehenden Daten, also der Alarminformationen und der Alarmparameter, von dem Kommunikationsmodul 3 der ersten Recheneinheit 1 im Sinne der Cybersecurity statt. Dabei sind Informationen, die zur Prüfung benötigt werden, auf dem ersten Datenspeicher 21 gespeichert und von der ersten Recheneinheit zugreifbar. Solche Informationen umfassen beispielsweise einen Sicherheitsschlüssel zur Prüfung eingehender, verschlüsselter Daten.

[0056] Im Falle, dass es sich bei den eingehenden Daten um eine Alarminformation handelt, also beispielsweise eine Information, dass eine Gefahrensituation vorliegt, so wird diese über die zweite Schnittstelle 6 an die zweite Recheneinheit 2 und das Alarmmodul 4 übertragen. Die zweite Recheneinheit 2 und das Alarmmodul 4 führen eine Safety-Funktion im Sinne der Betriebssicherheit aus, wobei es sich um das Erzeugen des Informationssignals INS handelt, welches einen nicht dargestellten Anwender des Gasmessgerätes 20 vor einer Gefahrensituation warnt. In diesem Fall wird also aufgrund der Alarminformation ein Informationssignal INS erzeugt und an die Alarmierungseinheit 8 übertragen, die eine LED, einen Vibrationsmotor und eine Hupe umfasst und einen akustischen, haptischen und/oder optischen Alarm zu erzeugen. Dabei sind die Parameter, wie das Informationssignal INS erzeugt wird, im zweiten Datenspeicher 22 gespeichert. Diese Parameter umfassen beispielsweise Signalmuster für einen Alarm und/oder Grenzwerte für Gaskonzentrationen und sind lediglich von der zweiten Recheneinheit zugreifbar. Somit ist sichergestellt, dass die erste Recheneinheit 1 keinen direkten Einfluss auf diese Parameter und somit auf die Safety-Funktionen der zweiten Recheneinheit 2 hat. Das Signalmuster legt fest, wie ein Alarm von der Alarmierungseinheit 8 des Gasmessgerätes 20 ausgegeben wird, also auf welche Art und Weise die LED, der Vibrationsmotor und/oder die Hupe das Informationssignal INS signalisieren.

[0057] Alternativ oder zusätzlich ist die zweite Recheneinheit 2 eingerichtet ein Informationssignal INS auf Grundlage von Sensordaten des Gassensors 25 zu erzeugen. Dabei erfasst das Sensormodul 24 die Sensordaten des Gassensors 25 und erzeugt einen Sensormesswert, in diesem Fall einen Gaskonzentrationswert. Dieser Gaskonzentrationswert wird von dem Alarmmodul 4 ausgewertet, indem er mit einem Grenzwert verglichen wird. Auf Grundlage dieser Auswertung erzeugt das Alarmmodul ein Informationssignal INS. Der Grenzwert für die Gaskonzentration ist, wie zuvor beschrieben, ein Parameter, der im zweiten Datenspeicher 22 gespeichert und lediglich von der zweiten Recheneinheit 2 zugreifbar ist.

[0058] **Fig.** 3 zeigt ein bevorzugtes Ausführungsbeispiel des erfindungsgemäßen Beatmungs- oder Anästhesiegerätes mit einer Ausführungsform der erfindungsgemäßen Vorrichtung 10, einem Einlass 35 zur Einleitung eines Atemgases, einer Beatmungseinheit 36, einem Volumenstromsensor 37, einem Auslass 38 zur Bereitstellung eines Atemgasstroms zur Beatmung eines Patienten 39 sowie einer Alarmierungseinheit 8, einem Monitor 40 und einem Speichermedium in Form einer SD-Karte 31. Die Vorrichtung 10 entspricht im Wesentlichen der Vorrichtung 10, wie sie in **Fig.** 2 dargestellt und zuvor beschrieben ist. Zusätzlich umfasst die erste Recheneinheit 1 der Vorrichtung 10 ein Speichermodul 32 zur Verwaltung der Daten auf der SD-Karte 31 sowie eine dritte Recheneinheit 33 mit einem Nutzerinteraktionsmodul 34 zur Eingabe und/oder Ausgabe von Informationen. Diese Informationen werden von dem Monitor 40 in Form eines berührungsempfindlichen Bildschirms entgegengenommen und/oder darüber angezeigt.

[0059] Der Funktionsumfang der Vorrichtung 10 entspricht im Wesentlichen dem Funktionsumfang der Vorrichtung 10, wie sie in **Fig.** 2 dargestellt und zuvor beschrieben ist. Das Sensormodul 24 ist jedoch eingerichtet die Sensordaten des Volumenstromsensors 37 zu erfassen und einen Volumenstromwert zu erzeugen. Auf Grundlage des Volumenstromwertes wird ein Informationssignal INS mittels Vergleich mit einem entsprechenden Grenzwert von dem Alarmmodul erzeugt und an die Alarmierungseinheit 8, die eine LED und eine Hupe umfasst, zur Signalisierung des Informationssignals übertragen.

[0060] Der externe Kommunikationspartner 7 in **Fig.** 3 ist beispielsweise eine Überwachungsstation in einem Krankenhauses, welche eingerichtet ist mit dem Beatmungs- oder Anästhesiegerät zu kommunizieren.

[0061] Zusätzlich zu der in **Fig.** 2 dargestellten und beschriebenen Vorrichtung 10 ist die Vorrichtung 10 in **Fig.** 3 eingerichtet, mittels der dritten Recheneinheit 33 und dem Nutzerinteraktionsmodul 34 Informationen mit dem Monitor 40 des Beatmungs- oder Anästhesiegerätes 30 auszutauschen. Dabei ist die dritte Recheneinheit 33 jeweils über eine Schnittstelle mit der ersten und zweiten Recheneinheit 1, 2 zum Datenaustausch verbunden. Somit ist gewährleistet, dass die Cybersecurity-Funktionen der ersten Recheneinheit 1 und die Safety-Funktionen der zweiten Recheneinheit 2 unabhängig von der Funktionalität der dritten Recheneinheit 33 sind. Beispielsweise können die Volumenstrommesswerte des Sensormoduls 24 von der zweiten Recheneinheit 2 an die dritte Recheneinheit 33 übertragen, von dem Nutzerinteraktionsmodul 34 für die Anzeige aufbereitet und auf dem Monitor 40 angezeigt werden. Ferner können Informationen über eine Eingabe eines nicht dargestellten Anwenders über den Monitor 40 an die erste und/oder zweite Recheneinheit 1, 2 weitergeleitet werden, wobei es sich beispielsweise um die Abfrage von Informationen handeln kann, welche anschließend auf dem Monitor angezeigt werden.

[0062] Zusätzlich zu der in **Fig.** 2 dargestellten und beschriebenen Vorrichtung 10 ist die Vorrichtung 10 in **Fig.** 3 eingerichtet, Daten eines Speichermediums in Form einer SD-Karte 31 mittels des Speichermoduls 32 der ersten Recheneinheit 1 zu verwalten. Da es sich bei der SD-Karte 31 um ein Speichermedium, welches aus dem Beatmungs- oder Anästhesiegerät 30 entfernt werden kann und deren Daten potenziell von Unberechtigten manipuliert werden können, werden die Daten der SD-Karte 31 von der ersten Recheneinheit 1 im Sinne der Cybersecurity geprüft. Dabei wird beispielsweise die Datenintegrität beim Lesen der Daten von der SD-Karte durch die erste Recheneinheit 1 geprüft. Somit wird die Informationssicherheit beim Einsatz der SD-Karte 31 als Speichermedium gewährleistet.

Bezugszeichenliste

1	erste Recheneinheit
2	zweite Recheneinheit
3	Kommunikationsmodul
4	Alarmmodul
5	erste Schnittstelle
6	zweite Schnittstelle
7	externer Kommunikationspartner
8	Alarmierungseinheit
INS	Informationssignal
20	Gasmessgerät
21	erster Datenspeicher
22	zweiter Datenspeicher
23	Halbleiterspeicher
24	Sensormodul
25	Gassensor
30	Beatmungs- oder Anästhesiegerät
31	SD-Karte
32	Speichermodul
33	dritte Recheneinheit
34	Nutzerinteraktionsmodul
35	Einlass
36	Beatmungseinheit
37	Volumenstromsensor

38 Auslass

39 Patient

40 Monitor

Patentansprüche

1. Vorrichtung (10) zur Ausführung von Cybersecurity-Funktionen im Sinne der Informationssicherheit und von Safety-Funktionen im Sinne der Betriebssicherheit mit einer ersten Recheneinheit (1) zur Ausführung zumindest einer der Cybersecurity-Funktionen und mit einer zweiten Recheneinheit (2) zur Ausführung zumindest einer der Safety-Funktionen, wobei die erste Recheneinheit (1) ein Kommunikationsmodul (3) umfasst, welches eine erste Schnittstelle (5) aufweist und eingerichtet ist eingehende Daten zu prüfen, wobei die zweiten Recheneinheit (2) ein Alarmmodul (4) umfasst, welches eingerichtet ist ein Informationssignal (INS) zu erzeugen, und wobei die erste Recheneinheit (1) und die zweite Recheneinheit (2) über eine zweite Schnittstelle (6) zum Datenaustausch miteinander verbunden sind.

2. Vorrichtung (10) nach Anspruch 1, **dadurch gekennzeichnet**, dass die erste Recheneinheit (1) konfiguriert ist, auf einen ersten Datenspeicher (21) zuzugreifen und die zweite Recheneinheit (2) konfiguriert ist, auf einen zweiten Datenspeicher (22) zuzugreifen.

3. Vorrichtung (10) nach Anspruch 2, **dadurch gekennzeichnet**, dass der erste Datenspeicher (21) und der zweite Datenspeicher (22) nichtüberlappend sind.

4. Vorrichtung (10) nach einem der vorherigen Ansprüche, **dadurch gekennzeichnet**, dass die erste Recheneinheit (1) eingerichtet ist, die zumindest eine Cybersecurity-Funktion unabhängig von der zweiten Recheneinheit (2) auszuführen und die zweite Recheneinheit (2) eingerichtet ist, die zumindest eine Safety-Funktion unabhängig von der ersten Recheneinheit (1) auszuführen.

5. Vorrichtung (10) nach einem der vorherigen Ansprüche, **dadurch gekennzeichnet**, dass die zweite Recheneinheit (2) ein Sensormodul (24) zur Erfassung von Sensordaten umfasst.

6. Vorrichtung (10) nach einem der vorherigen Ansprüche, **dadurch gekennzeichnet**, dass die erste Recheneinheit (1) und/oder die zweite Recheneinheit (2) ein Speichermodul (32) zur Verwaltung von Daten auf einem Speichermedium (31) umfasst.

7. Vorrichtung (10) nach einem der vorherigen Ansprüche, **dadurch gekennzeichnet**, dass die Vorrichtung (10) eine dritte Recheneinheit (33) aufweist und die dritte Recheneinheit (33) ein Nutzerinteraktionsmodul (34) zur Eingabe und/oder Ausgabe von Informationen umfasst.

8. Vorrichtung (10) nach Anspruch 6, **dadurch gekennzeichnet**, dass die dritte Recheneinheit (33) zum Datenaustausch mit der ersten Recheneinheit (1) und/oder zweiten Recheneinheit (2) verbunden ist.

9. Verfahren (10) zur Ausführung von Cybersecurity-Funktionen im Sinne der Informationssicherheit und von Safety-Funktionen im Sinne der Betriebssicherheit auf einer Vorrichtung (10) mit einer ersten Recheneinheit (1) und mit einer zweiten Recheneinheit (2), aufweisend folgende Schritte:
- Empfangen und Prüfen von Daten mit einem Kommunikationsmodul (3) der ersten Recheneinheit (1),
- Speichern der Daten in einem ersten Datenspeicher (21) und/oder Übertragen der Daten an eine zweite Recheneinheit (2),
- Auswerten der Daten bezüglich einer Alarmsituation mit einem Alarmmodul (4) der zweiten Recheneinheit (2), und
- Erzeugen eines Informationssignals (INS) durch das Alarmmodul (4)

10. Verfahren (10) nach Anspruch 9, ferner aufweisend folgende Schritte:
- Ermitteln eines Sensormesswertes mit einem Sensormodul (24) der zweiten Recheneinheit (2)
- Auswerten des Sensormesswertes bezüglich einer Alarmsituation durch das Alarmmodul (4)

11. Verfahren (10) nach Anspruch 9 oder 10, ferner aufweisend folgenden Schritt:
- Speichern von Informationen der zweiten Recheneinheit (2) in einem zweiten Datenspeicher (22), wobei der zweite Datenspeicher (22) und der erste Datenspeicher (21) nichtüberlappend sind

12. Verfahren (10) nach einem der Ansprüche 9 bis 11, ferner aufweisend folgenden Schritt:
- Empfangen und/oder Ausgeben von Informationen mit einem Nutzerinteraktionsmodul einer dritten Recheneinheit der Vorrichtung (10)

13. Gasmessgerät (20) mit einer Vorrichtung (10) nach einem der Ansprüche 1 bis 8.

14. Beatmungs- oder Anästhesiegerät (30) mit einer Vorrichtung (10) nach einem der Ansprüche 1 bis 8.

Es folgen 3 Seiten Zeichnungen

Anhängende Zeichnungen

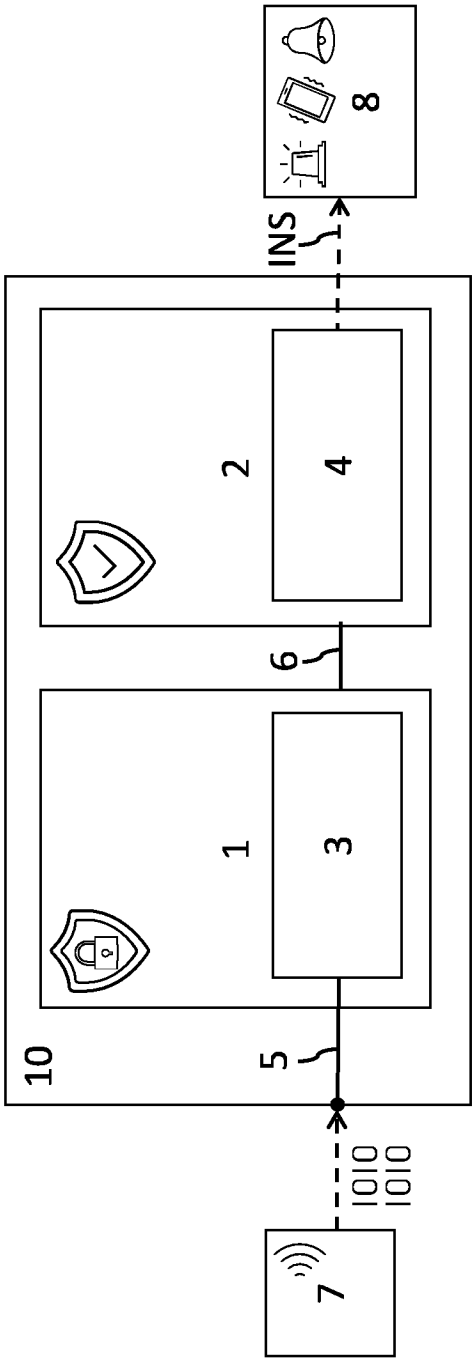


Fig. 1

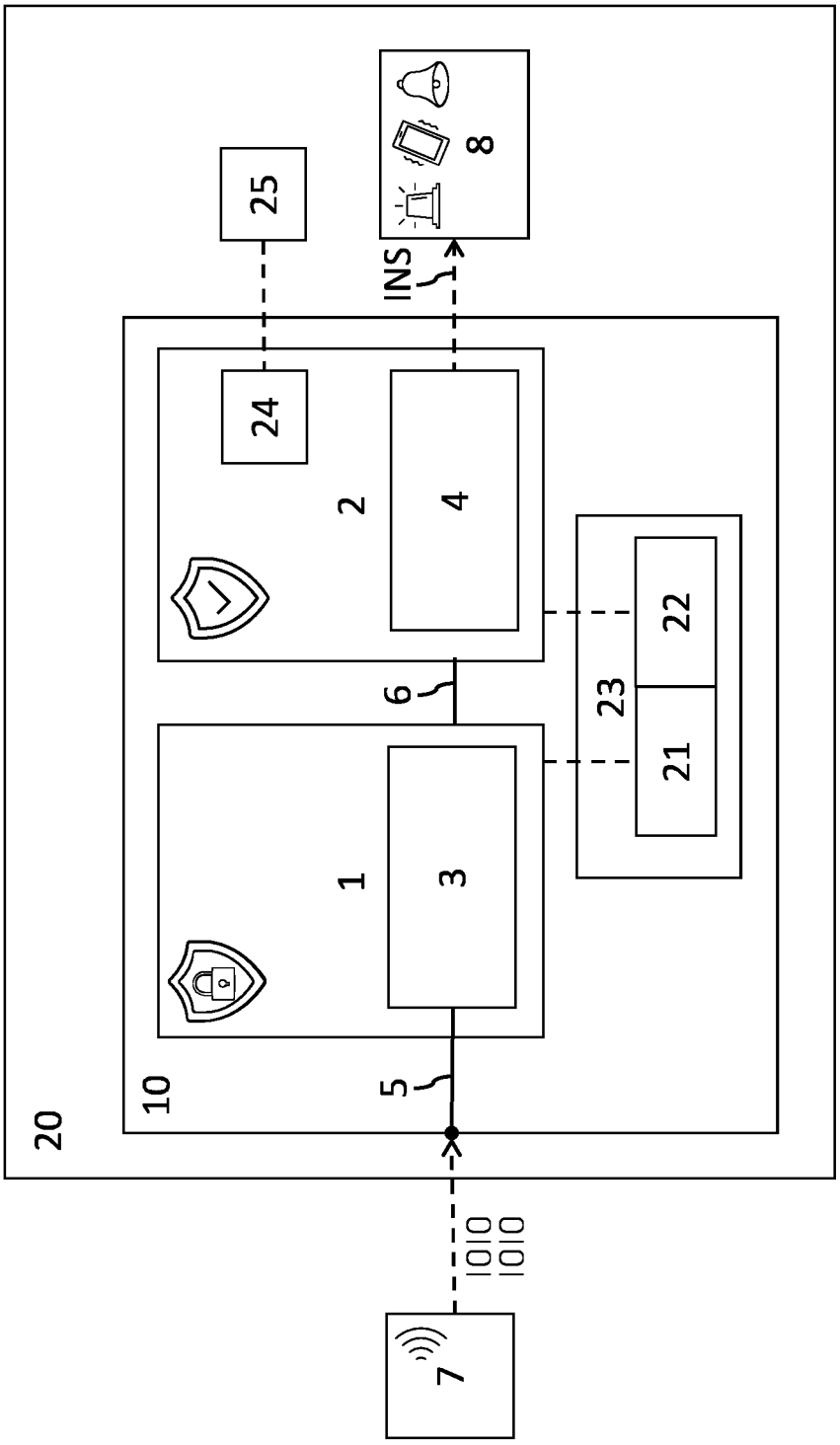


Fig. 2

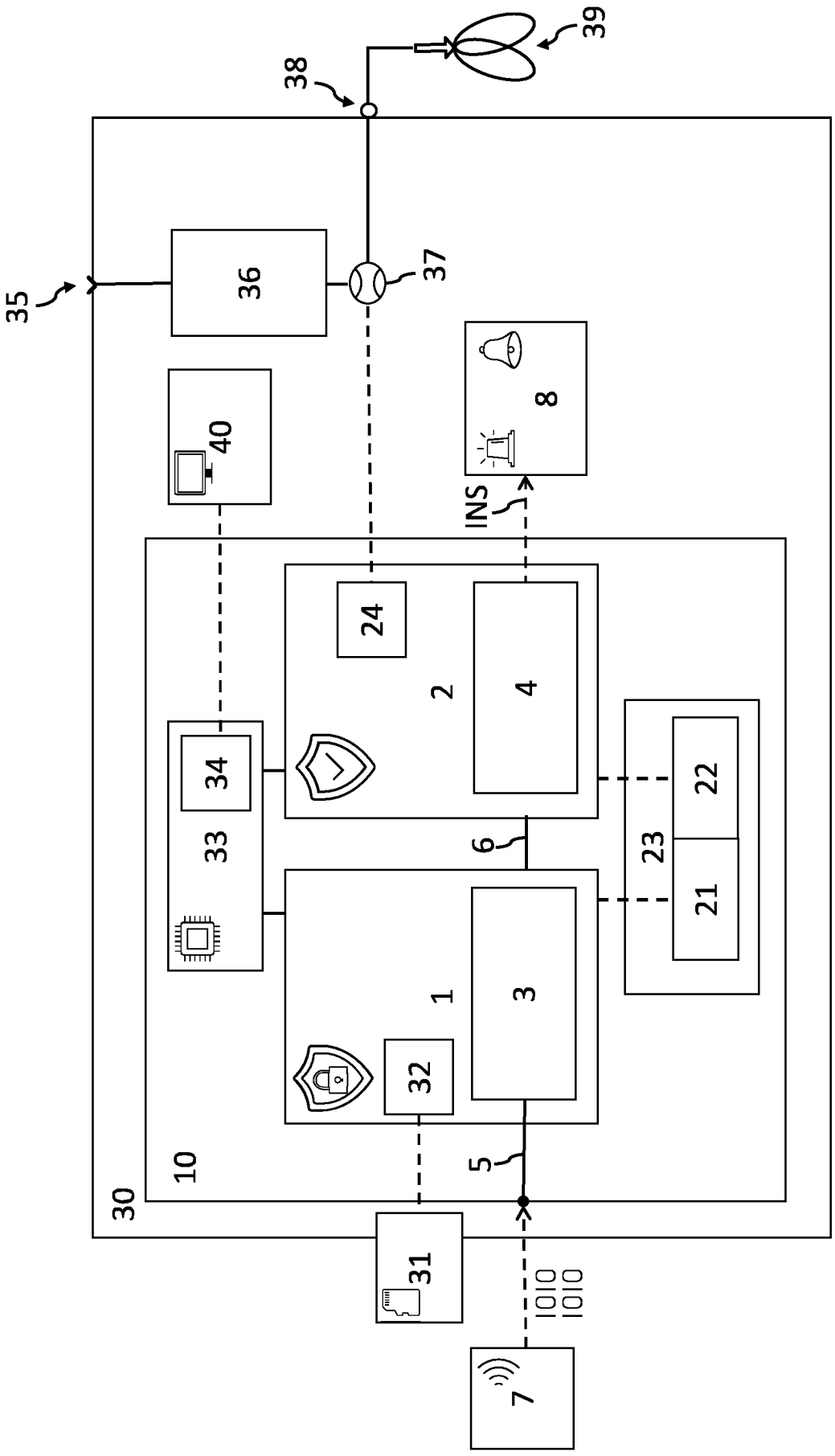


Fig. 3

