(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 226 767 A1

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
08.09.2010 Patentblatt 2010/36

(21) Anmeldenummer: **10001663.3**

(22) Anmeldetag: **18.02.2010**

(51) Int Cl.:
G07C 5/08 *(2006.01)* ***G07C 9/00*** *(2006.01)*
G08B 13/14 *(2006.01)* ***G08B 25/10*** *(2006.01)*

(84) Benannte Vertragsstaaten:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO SE SI SK SM TR
Benannte Erstreckungsstaaten:
AL BA RS

(30) Priorität: **03.03.2009 DE 102009013104**

(71) Anmelder: **Astrium GmbH**
81667 München (DE)

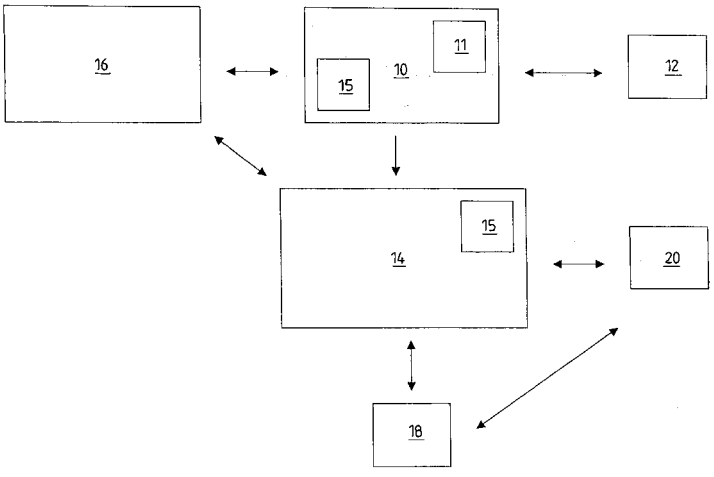
(72) Erfinder:
- **Busch, Wolfgang**
  28832 Achim (DE)
- **Engelke, Horst**
  28816 Stuhr (DE)

(74) Vertreter: **Aulich, Martin et al**
Meissner, Bolte & Partner GbR
Hollerallee 73
28209 Bremen (DE)

(54) Verfahren und System zur Überwachung eines Frachtbehältnisses

(57) Die Erfindung betrifft ein Verfahren und ein System zur Überwachung, insbesondere zur Echtzeitüberwachung, der Integrität eines Frachtbehältnisses, vorzugsweise eines Transportcontainers, wobei das Frachtbehältnis - eine diesem zugeordnete Überwachungseinrichtung (10) aufweist, die über mindestens einen, die Integrität des Frachtbehältnisses überwachenden Überwachungssensor (12) verfügt. Das Verfahren ist gekennzeichnet durch folgende Maßnahmen:
- nach der Erfassung eines die Frachtbehältnisintegrität verletzenden Ereignisses durch den Überwachungssensor (12) werden einem entfernten Analysezentrum (14), insbesondere einer dem Analysezentrum (14) zugeordneten Analyseeinrichtung (18), Ereignisdaten übermittelt, die die Integritätsverletzung repräsentieren,
- in dem Analysezentrum (14), insbesondere in der diesem zugeordneten Analyseeinrichtung (18), werden die übermittelten Ereignisdaten anhand vorbestimmter Kriterien im Hinblick auf eine entweder berechtigte - autorisierte - oder eine unberechtigte - unautorisierte - Integritätsverletzung des Frachtbehältnisses bewertet,
- die Integritätsverletzung, insbesondere ein Öffnen oder Verschließen eines Frachtbehältnisses, wird als berechtigt bzw. autorisiert bewertet, falls dem Analysezentrum (14) - insbesondere im Zeitpunkt des Eintreffens der Ereignisdaten in dem Analysezentrum (14) oder in einer insbesondere vorbestimmten Zeitspanne vor oder nach dem Eintreffen derselben - zu den die Integritätsverletzung repräsentierenden Ereignisdaten ein die Berechtigung der Integritätsverletzung repräsentierender Autorisierungscode vorliegt.

Fig. 1



EP 2 226 767 A1

Beschreibung

[0001] Die vorliegende Erfindung betrifft ein Verfahren zur Überwachung, insbesondere zur Echtzeitüberwachung der Integrität eines Frachtbehältnisses, vorzugsweise eines Transportcontainers, wobei das Frachtbehältnis eine diesem zugeordnete Überwachungseinrichtung aufweist, die über mindestens einen, die Integrität des Behältnisses überwachenden Überwachungssensor verfügt. Die Erfindung betrifft des Weiteren ein System zur Durchführung des Verfahrens.

[0002] National und international steigen im Frachtgeschäft die Anforderungen an die Sicherheit von Frachtbehältnissen, insbesondere von Transportcontainem, wie etwa sogenannten See- oder Landcontainern, immer weiter an. Als besonders groß wird die Gefahr eingestuft, dass einzelne Frachtbehältnisse nach einem Beladevorgang durch autorisiertes Personal auf dem Transportweg von Terroristen geöffnet und mit Sprengsätzen oder dergleichen versehen werden, die am Zielort des Frachtbehältnisses detonieren sollen.

[0003] Um das Risiko derartiger Szenarien zu verringern, gibt es Bestrebungen, sämtliche Frachtbehältnisse auf illegale Waffen oder anderes illegales Frachtgut zu durchleuchten, etwa mit Röntgenverfahren. Derartige Verfahren sind insbesondere in Anbetracht der Vielzahl von weltweit versendeten Frachtbehältnissen äußerst aufwendig.

[0004] Es wurde daher eine Vielzahl von Verfahren entwickelt, mit denen die Integrität von Frachtbehältnissen ausgehend von der Beladung des Behältnisses über dessen Transportweg bis zum Zielort möglichst lückenlos nachverfolgt werden kann. Ein System der eingangs genannten Art ist beispielsweise aus der US 4,750,197 bekannt. Im Inneren eines Transportcontainers ist dort eine Überwachungseinrichtung mit Überwachungssensor angeordnet. Die Überwachungseinrichtung wird von einer berechtigten Person mittels eines geeigneten Schlüssels aktiviert. Nach der Aktivierung erfolgt die Überwachung des Containers. Die Integrität des Containers verletzende Ereignisse werden von dem Sensor erfasst und auf einem lokalen Datenspeicher gespeichert. Weiterhin ist mit der Überwachungseinrichtung ein Alarmsignalgeber gekoppelt. Sobald die Überwachung einen unberechtigten Zugang zu dem Container erfasst, erzeugt der Signalgeber ein Alarmsignal.

[0005] Ein ganz ähnliches System wird in der DE 60 2004 008 248 T2 beschrieben. Auch in dieser Schrift wird einem Transportcontainer eine Überwachungseinrichtung mit Überwachungssensor zugeordnet. Mögliche unberechtigte bzw. unautorisierte Zugänge werden ebenfalls erst erfasst, nachdem eine Aktivierung der Überwachungseinrichtung mittels eines Aktivierungsschlüssels erfolgt ist. Die Überwachungseinrichtung überwacht den Container dann solange, bis sie mittels eines geeigneten Deaktivierungsschlüssels deaktiviert wird, in der Regel am Ende des Transportweges. Etwaige Zugangsvorfälle während des Transportes, beispielsweise ein unerlaubtes Eindringen in den Container auf dem Transportweg, werden wie bei der Lösung der US 4,750,197 erfasst und in einem Speicher der Überwachungseinrichtung gespeichert. Am Ende des Transportweges kann die Überwachungseinrichtung mittels eines geeigneten Deaktivierungsschlüssels deaktiviert, d.h. abgeschaltet werden. Die Überwachung des Containers wird hierdurch beendet. Zugleich werden etwaige gespeicherte Daten über Zugangsvorfälle auf den Deaktivierungsschlüssel übertragen.

[0006] Die dargestellten Überwachungssysteme haben verschiedene Nachteile. Problematisch ist insbesondere, dass nach der autorisierten Öffnung des jeweiligen Containers keinerlei weitere Überwachung desselben mehr stattfindet. Dies kann hochgefährlich sein. Denn Container werden häufig nach dem erstmaligen Beladen am Startort des Containers vor dem Erreichen des eigentlichen Zielorts zwischenbeladen. Dabei wird der Container mit weiterem Frachtgut beladen, das an einem auf dem Transportweg liegenden Ort gelagert ist. Um dieses weitere Frachtgut aufzunehmen, muss die Überwachungseinrichtung im Stand der Technik zunächst autorisiert deaktiviert, also abgeschaltet werden. Erst anschließend ist eine autorisierte Öffnung des Containers und ein (Zwischen-)Beladen des Containers möglich. Nach dem Beladen wird der Container wieder verschlossen und die Überwachungseinrichtung erneut autorisiert aktiviert.

[0007] Im Zeitraum zwischen dem deaktivierten und dem aktivierten Zustand der Überwachungseinrichtung, d.h. zwischen dem Abschalten und erneutem Einschalten derselben, findet dementsprechend keinerlei Überwachung des Containers statt. So kann der Container geraume Zeit in dem geöffneten Zustand verbleiben und beispielsweise unbemerkt von derjenigen Person, die den Container autorisiert geöffnet hatte, von anderen Personen mit illegalem Frachtgut beladen werden. Im Übrigen wäre es auch für die autorisierte Person, die den (Zwischen-)Beladevorgang vornimmt, nach der Deaktivierung der Überwachungseinrichtung problemlos möglich, in dem Container gefährliches Frachtgut zu lagern.

[0008] Ausgehend von diesem Stand der Technik ist es Aufgabe der vorliegenden Erfindung, ein Verfahren und ein System der eingangs genannten Art anzugeben, mit dem die Integrität eines Frachtbehältnisses möglichst lückenlos überwacht werden kann.

[0009] Diese Aufgabe wird gelöst durch ein Verfahren mit den Merkmalen eines Anspruchs 1 sowie durch ein System mit den Merkmalen des Anspruchs 15.

[0010] Danach werden nach der Erfassung eines die Frachtbehältnisintegrität verletzenden Ereignisses durch den Überwachungssensor einem von dem Behältnis entfernt positionierten Analysezentrum Ereignisdaten übermittelt, die die integritätsverletzung repräsentieren. In dem Analysezentrum werden die übermittelten Ereignisdaten anschließend anhand vorbestimmter Kriterien im Hinblick auf eine entweder berechtigte oder unberechtigte Integritätsverletzung des Frachtbehältnisses

bewertet. Abhängig von dem Ergebnis dieser Bewertung können dann geeignete Maßnahmen ergriffen werden, etwa ein Alarmsignal erzeugt werden.

[0011] Das vorgenannte erfindungsgemäße Verfahren läuft durch Verwendung geeigneter, nachfolgend noch näher bezeichneter Systemkomponenten bevorzugt automatisiert oder mindestens teilautomatisiert ab.

[0012] Im Rahmen der Anmeldung wird unter einer Integritätsverletzung allgemein jede berechtigte oder unberechtigte Manipulation innen oder außen am Frachtbehältnis verstanden und/oder jeder physikalischen Zugang zu dem Frachtbehältnis, insbesondere in das Innere desselben.

[0013] Vorzugsweise umfasst eine integritätsverletzung das Öffnen und/oder das Schließen einer oder mehrerer Verschließeinrichtungen, insbesondere Türen, die jeweils mindestens eine Zugangsöffnung zu dem Behältnis verschließen bzw. freigeben können.

[0014] Des Weiteren werden allgemein unter "autorisierte Integritätsverietzungen" berechtigte Integritätsverletzungen verstanden, unberechtigte Verletzungen dagegen werden als "unautorisiert" bezeichnet.

[0015] Das erfindungsgemäße Verfahren ermöglicht es, das Frachtbehältnis bzw. dessen Status während des gesamten Transportweges ununterbrochen zu überwachen.

[0016] In der Regel werden die eine Integritätsverletzung repräsentierenden Ereignisdaten deshalb unmittelbar im Anschluss an deren Erfassung durch den oder die Sensoren automatisch an das Analysezentrum zur anschließenden Bewertung derselben übersandt. Die Übersendung der Daten wird dabei getriggert durch die Erfassung der Integritätsverietzung. In diesem Sinne kann das Analysezentrum den Container im Wesentlichen in Echtzeit überwachen.

[0017] Anders als im Stand der Technik erfolgt die Überwachung im Übrigen auch dann, wenn das Frachtbehältnis, bereits bevor es seinen Zielort erreicht hat, autorisiert geöffnet und mit zusätzlicher Ladung versehen werden sollte. Auch nach einer derartigen autorisierten Zwischenöffnung mit anschließendem erneuten, autorisierten Verschließvorgang bleibt die Überwachungseinrichtung bzw. der mit dieser wirkverbundene Überwachungssensor aktiv. Auf eine Aktivierung und Deaktivierung der Überwachungseinrichtung durch Aktivierungs- bzw. Deaktivierungsschlüssel wird vorteilhafterweise verzichtet. Es erfolgt daher auch in der Zeit nach einer autorisierten (Zwischen-)Öffnung des Behältnisses eine Überwachung desselben. Im Stand der Technik dagegen muss die Überwachungseinrichtung im Sinne einer üblichen Alarmanlage deaktiviert, d.h. abgeschaltet werden, wenn das Behältnis autorisiert geöffnet werden soll.

[0018] Der Überwachungssensor erfasst mögliche Integritätsverletzungen demnach unabhängig davon, ob die jeweilige Integritätsverletzung autorisiert oder unautorisiert erfolgt. Im Stand der Technik dagegen werden letztlich ausschließlich unautorisierte Integritätsverletzungen erfasst. Denn autorisierte Integritätsverletzungen, etwa ein autorisiertes Öffnen, können im Stand der Technik nur in Verbindung mit einem Abschalten der Überwachungseinrichtung erfolgen.

[0019] Erfindungsgemäß kann das Frachtbehältnis dagegen auch im Anschluss an autorisierte Integritätsverletzungen weiter überwacht werden, mindestens bis es seinen Zielort erreicht hat. Wenn die Überwachung beispielsweise mittels Bewegungen innerhalb des Frachtbehältnisses erfassenden Bewegungssensoren erfolgt, werden auch nach einer autorisierten (Zwischen-)Öffnung des Behältnisses auswertbare Überwachungs- bzw. Ereignisdaten erzeugt. Verdächtige Bewegungen, beispielsweise verursacht durch unberechtigte Beladeaktivitäten, können daher auch nach dem autorisierten Öffnen des Behältnisses erfasst und erkannt werden. So ist auch die automatisierte Überwachung des Belade- und/oder Entladevorgangs selbst möglich. Es kann mittels geeigneter Sensorik überwacht und kontrolliert werden, welche Güter verladen und/oder entladen werden.

[0020] Als zu überwachende Frachtbehältnisse kommen sämtliche mobilen Behältnisse in Betracht, in denen Frachtgüter transportiert und/oder gelagert werden können. Die Frachtbehältnisse umgeben oder begrenzen dabei einen in ihrem Inneren angeordneten Fracht- und/oder Laderaum.

[0021] Vorzugsweise verfügen die Frachtbehältnisse jeweils über mindestens eine Verschließeinrichtung, insbesondere eine Tür, Klappe oder dergleichen, die jeweils mindestens eine Beladeöffnung zu dem Frachtbehältnis verschließen und/oder freigeben kann. Über die Beladeöffnung kann das Frachtbehältnis mit Frachtgut beladen werden bzw. Frachtgut aus dem Frachtbehältnis entladen werden.

[0022] In der bevorzugten Anwendung der Erfindung sind die Frachtbehältnisse Transportcontainer, insbesondere See- oder Landcontainer.

[0023] Die Frachtbehältnisse können auch jeweils fest mit Fahrzeugen, wie etwa LKW's oder dergleichen, verbunden sein oder Teil dieser sein.

[0024] Grundsätzlich ist auch denkbar, immobile Fracht- und/oder Lagerräume mit dem erfindungsgemäßen Verfahren zu überwachen.

[0025] Die die Integritätsverletzung repräsentierenden Ereignisdaten, die dem entfernten Analysezentrum zur nachfolgenden Bewertung der erfassten Verletzung als "Autorisiert/Nicht autorisiert" übersandt werden, sind bevorzugt Daten, die unmittelbar den Status bzw. den Zustand des Behältnisses im Sinne "Integrität verletzt ja/nein" kennzeichnen.

[0026] Bei dieser Ausführungsform der Erfindung übernimmt die Überwachungseinrichtung im Vorfeld der vorgenannten Bewertung die Analyse, ob die von dem Sensor gemessenen Messwerte auf eine Integritätsverletzung des Behältnisses hindeuten oder nicht.

[0027] Diese Messwertauswertung erfolgt zweckmäßigerweise im Hinblick auf das Einhalten oder Überschreiten vorgegebener Messwertgrenzwerte. Ergibt die

Auswertung der Überwachungseinrichtung, dass eine Integritätsverletzung vorliegt, kann die Überwachungseinrichtung eine das Vorliegen der Integritätsverletzung repräsentierende Mitteilung an das Analysezentrum senden.

[0028] Etwa bei einem Einsatz eines das Innere des Frachtbehältnisses überwachenden Bewegungssensors würde die Überwachungseinrichtung die Messwerte dann im Hinblick auf das Erreichen oder Überschreiten bestimmter Grenzwerte auswerten. Hierdurch können beispielsweise unkritische (Luft-)Bewegungen, die durch den Transport des Frachtbehältnisses bedingt sind, von kritischen Bewegungen durch Beladeaktivitäten unterscheiden zu können. Die Auswertung der Überwachungseinrichtung ergibt dabei demnach, ob eine Integritätsverletzung vorliegt oder nicht.

[0029] Alternativ oder zusätzlich können aber auch zunächst unmittelbar die unanalysierten Messwerte bzw. die die unanalysierten Messwerte repräsentierenden Daten des Sensors an das Analysezentrum übermittelt werden. In der Folge würde dann erst im Analysezentrum die vorgenannte Analyse im Hinblick auf das Erreichen oder Überschreiten von Grenzwerten erfolgen und damit im Hinblick auf das Vorliegen einer Integritätsverletzung.

[0030] Unabhängig davon, ob die Bewertung der Sensormesswerte im Hinblick auf das Vorliegen einer Integritätsverletzung bereits durch die Überwachungseinrichtung erfolgt oder erst später in dem Analysezentrum, werden erfindungsgemäß die von dem Frachtbehältnis bzw. von der dem Frachtbehältnis zugeordneten Überwachungseinrichtung ausgehenden Ereignisdaten im Analysezentrum später im Hinblick darauf analysiert, ob die erfasste Integritätsverletzung entweder autorisiert oder unautorisiert erfolgte.

[0031] Ein geeignetes Analysezentrum zur Durchführung dieser Aufgaben kann in einfachster Ausführungsform der Erfindung beispielsweise über eine geeignete Computereinrichtung zur Analyse bzw. Bewertung der Ereignisdaten verfügen sowie mindestens über eine Empfangseinrichtung, mit der die von der Überwachungseinrichtung ausgehenden Ereignisdaten empfangen werden können.

[0032] Die Ereignisdaten werden dabei in einer bevorzugten Ausführungsform der Erfindung von einer der Überwachungseinrichtung zugeordneten Sendeeinrichtung per Langstrecken-Datenfernübertragung, insbesondere per Satellitenfunkverbindung, unmittelbar oder mittelbar (ggf. durch Weiterleitung über weitere Zwischensendeeinrichtungen) an das Analysezentrum bzw. an die ihr zugeordnete Empfangseinrichtung übertragen.

[0033] Was die Integritätsverletzungen betrifft, so erfasst die Überwachungseinrichtung - wie oben bereits angedeutet - als Integritätsverletzungen bevorzugt mindestens ein Öffnen und/oder Verschließen des Frachtbehältnisses. Zu diesem Zweck kann die Überwachungseinrichtung einen geeigneten Sensor aufweisen, beispielsweise einen Türsensor. Naturgemäß können auch verschiedene andere Sensoren eingesetzt werden, die geeignet sind, etwaige Integritätsverletzungen zu erfassen. Bevorzugt wird beispielsweise mindestens ein Bewegungssensor eingesetzt, der Bewegungen innerhalb des Frachtbehältnisses und/oder Bewegungen des Frachtbehältnisses selbst überwacht. Weiter ist denkbar, Detektoren einzusetzen, die explosive Sprengstoffe erkennen können und/oder gefährliche Strahlung, insbesondere radioaktive Strahlung.

[0034] Was die Kriterien betrifft, nach denen eine erfasste integritatsverletzung als autorisiert erfolgt oder nicht autorisiert erfolgt bewertet wird, so wird eine derartige Verletzung erfindungsgemäß bevorzugt als autorisiert bewertet, falls dem Analysezentrum jeweils zu den die Integritätsverletzung repräsentierenden Ereignisdaten eine die Berechtigung der Integritätsverletzung repräsentierende Autorisierung vorliegt. Zweckmäßigerweise soll diese Autorisierung insbesondere im Zeitpunkt des Eintreffens der Ereignisdaten in dem Analysezentrum vorliegen oder in einer insbesondere vorbestimmten Zeitspanne vor oder nach dem Eintreffen derselben, beispielsweise innerhalb von einigen Sekunden vor oder nach dem Eintreffen.

[0035] Der Begriff "Autorisierung" umfasst im Rahmen der vorliegenden Anmeldung jeden Vorgang, mit dem eine Integritätsverletzung als berechtigt erfolgt nachgewiesen werden kann. Eine Autorisierung in diesem Sinne kann insbesondere auch einen Vorgang umfassen, bei dem eine behauptete identität der die Autorisierung initiierenden Person oder Institution überprüft wird.

[0036] Erfindungsgemäß werden sämtliche Ereignisdaten, die dem Analysezentrum übersandt werden, daraufhin überprüft, ob zu den jeweiligen Ereignisdaten, d.h. zu den entsprechenden Integritätsverletzungsvorfällen, jeweils eine geeignete Autorisierung vorliegt.

[0037] Wenn beispielsweise ein Versender eines Frachtbehältnisses ein zuvor autorisiert verschlossenes Frachtbehältnis öffnen möchte, ohne dass in letzter Konsequenz möglicherweise ein Alarmzustand ausgelöst wird, kann er dies daher durch eine autorisierte Öffnung desselben erreichen. Der entsprechende, physische Öffnungsvorgang des Versenders wird dabei zunächst als Integritätsverletzungsereignis dem Analysezentrum übersandt. Wenn dem Analysezentrum dann für diesen übermittelten Verletzungsvorgang eine entsprechende Autorisierung vorliegt, wird die Verletzung als berechtigt erfolgt bewertet bzw. als autorisiert erfolgt. Dann wird in der Regel kein Alarmsignal erzeugt.

[0038] Die übermittelte integritätsverletzung, in dem vorgenannten Beispiel das Öffnen des Behältnisses, wird dagegen als unautorisiert bewertet, falls dem Analysezentrum, insbesondere in den vorgenannten Zeitpunkten bzw. Zeitspannen, keine die Berechtigung der Integritätsverletzung repräsentierende Autorisierung vorliegt. Wenn mit anderen Worten der Versender das Behältnis öffnet, ohne dazu autorisiert zu sein, führt die Bewertung der die Öffnung repräsentierenden Ereignisdaten im Analysezentrum zu einer Bewertung der Öffnung als unautorisiert.

[0039] Um Autorisierungen der einzelnen Integritätsverletzungen durchführen zu können, werden bevorzugt elektronische Codes verwendet. Zur Herbeiführung einer Autorisierung einer Integritätsverletzung initiiert vorzugsweise diejenige Person oder Institution, die die Integritätsvertetzung autorisieren möchte, die Übersendung eines die Berechtigung der Integritätsverletzung repräsentierenden, elektronischen Autorisierungscodes an das Analysezentrum. Die autorisierende Person ist dabei in der Regel diejenige Person, die das Frachtbehältnis (berechtigt) zur Beladung mit Frachtgut öffnen oder diesen nach dem Beladen verschließen möchte.

[0040] Vorzugsweise umfassen die elektronischen Autorisierungscodes Daten zum Nachweis der Identität der jeweils die Codes verwendenden Personen oder Institutionen, insbesondere digitale Zertifikate oder Signaturen.

[0041] Die Übermittlung des Codes kann auf vielfältige Weise erfolgen. Beispielsweise können einem für den Transport des Behältnisses verantwortlichem Versender zunächst ein oder mehrere elektronische, zu dem jeweiligen Behältnis und/oder zu der verwendeten Überwachungseinrichtung passende Codes übermittelt werden. Die Codes können dabei beispielsweise auf eine vorzugsweise als Handgerät ausgebildete Autorisierungseinrichtung übertragen werden, etwa auf einen Handheld oder dergleichen einer von dem Versender beauftragen Person.

[0042] Wenn die von dem Versender beauftragte Person anschließend ein Behältnis autorisiert öffnen oder autorisiert verschließen möchte, kann sie dann mithilfe der Autorisierungseinrichtung bei, oder in einer festgelegten Zeitspanne vor oder nach dem Verschließen bzw. Öffnen des Behältnisses einen der zuvor übermittelten, geeigneten Autorisierungscodes an das Analysezentrum übersenden. Dies kann per Datenfernübertragung geschehen, etwa mittels einer Satellitenfunkverbindung oder dergleichen.

[0043] In einer weiteren zweckmäßigen Ausführungsform der Erfindung verfügt die Autorisierungseinrichtung - etwa ein Handheld, ein Mobiltelefon oder dergleichen -, über eine Sendeeinrichtung, mit der die Autorisierungscodes insbesondere per Datenfernübertragung, bevorzugt drahtlos, an das Analysezentrum bzw. an eine dieser zugeordneten Empfangseinrichtung übersendbar sind.

[0044] Die Übermittlung des jeweiligen Autorisierungscodes an das Analysezentrum kann auch mittelbar unter Verwendung der Überwachungseinrichtung bzw. der oben erwähnten, ihr zugeordneten Sende- und/oder Empfangseinrichtung erfolgen. Die Überwachungseinrichtung ist in der oben beschriebenen Weise in der Regel ohnehin über Satellitenkommunikationstechnologie oder andere drahtlose Datenfemübertragungsmittel mit dem Analysezentrum verbunden bzw. verbindbar. Die von dem Versender beauftragte Person kann den jeweiligen Autorisierungscode daher beispielsweise mit der Autonsierungseinrichtung per drahtloser Datenkurzstreckenkommunikation zunächst an die Überwachungseinrichtung bzw. an die dieser zugeordneten Sendeeinrichtung übermitteln. Die Sendeeinrichtung der Überwachungseinrichtung überträgt den Autorisierungscode dann unmittelbar oder mittelbar an das Analysezentrum.

[0045] Es ist auch denkbar, dass die Autorisierungseinrichtung unmittelbarer Bestandteil der Überwachungseinrichtung ist. Sie kann dann beispielsweise über eine mit der Überwachungseinrichtung unmittelbar - mittels geeigneter Leitungen - verbundene Eingabeeinrichtung verfügen, wie etwa eine Tastatur. Über die Eingabeeinrichtung werden dann jeweils die Autorisierungscodes eingeben, die nachfolgend der Überwachungseinrichtung bzw. mittelbar deren Sendeeinrichtung zur Weiterleitung an das Analysezentrum übertragen werden. Vorteilhafterweise weist die Autorisierungseinrichtung und/oder die Überwachungseinrichtung ein Display auf, auf dem, insbesondere während der Eingabe der Autorisierungscodes, geeignete Daten sichtbar gemacht werden können. Dies sind bevorzugt Daten, die zur Anleitung der von dem Versender beauftragten Person während des Autorisierungsvorgangs dienen.

[0046] Die Autorisierungscodes werden vorzugsweise zuvor in dem Analysezentrum generiert, insbesondere in einer oder der diesem zugeordneten Computereinrichtung, bevor sie der Person oder der Institution übermittelt werden, die die geplanten Integritätsverletzungen autorisieren möchte.

[0047] In einer weiteren zweckmäßigen Ausführungsform der Erfindung wird die Gültigkeit des jeweiligen elektronischen Autorisierungscodes nach Verwendung desselben überprüft. Diese Überprüfung kann beispielsweise anhand von hinterlegten Autorisierungsparametem erfolgen, die vorzugsweise in einem dem Analysezentrum, insbesondere der Computereinrichtung desselben, zugeordneten Speicher und/oder einer entsprechenden Datenbank gespeichert sind.

[0048] In einfachster Umsetzung des Prüfverfahrens zur Überprüfung der Gültigkeit der Autorisierungscodes können die zuvor in dem Analysezentrum generierten Codes kopiert und in dem Speicher/der Datenbank hinterlegt werden. Die anschließend von der Autorisierungseinrichtung jeweils an das Analysezentrum unmittelbar oder mittelbar übermittelten Autorisierungscodes werden bei oder nach dem Eintreffen derselben in dem Analysezentrum mit den in dem Speicher hinterlegten Kopien der Codes abgeglichen.

[0049] Naturgemäß gibt es eine Vielzahl von anderen Möglichkeiten, die Gültigkeit bzw. Echtheit der zur jeweiligen Autorisierung verwendeten Autorisierungscodes zu überprüfen.

[0050] Erfindungsgemäß kann weiter vorgesehen sein, zu jedem zu überwachenden Frachtbehältnis und/oder zu jeder zu verwendenden Überwachungseinrichtung einen oder mehrere Autorisierungscodes, insbesondere jeweils einen Satz von Autorisierungscodes, zu erzeugen. Diese Autorisierungscodes können dann nach Generierung derselben beispielsweise dem zuständigen

Versender übermittelt werden. Für jedes Frachtbehältnis und/oder für jede Überwachungseinrichtung sind dann eigene Sätze von Autorisierungscodes vorhanden.

[0051] In einer anderen Ausführungsform der Erfindung ist vorgesehen, Autorisierungscodes bzw. Sätze von Autorisierungscodes jeweils bestimmten Gruppen von Frachtbehältnissen und/oder Gruppen von Überwachungseinrichtungen zuzuordnen.

[0052] Mit den Autorisierungscodes können dann jeweils einzelne Frachtbehältnisse aus diesen Gruppen bzw. einzelne Frachtbehältnisse, die mit Überwachungseinrichtungen aus diesen Gruppen ausgerüstet sind, autorisiert verschlossen oder geöffnet werden.

[0053] Sämtliche der genannten Zuordnungen sind vorteilhafterweise in einem geeigneten Speicher abgelegt, insbesondere in einer geeigneten Datenbank.

[0054] Weitere Merkmale der Erfindung ergeben sich aus den beigefügten Patentansprüchen, der nachfolgenden Beschreibung eines bevorzugten Ausfühmngsbeispiels sowie der beigefügten Zeichnung.

[0055] Darin zeigt:

Fig. 1 ein schematisches Blockschaltbild eines erfindungsgemäßen Systems zum Überwachen der Integrität eines Frachtbehältnis, das gemäß dem erfindungsgemäßen Verfahren betrieben wird.

[0056] Ein wichtiger Bestandteil des erfindungsgemäßen Systems zur Überwachung von Frachtbehältnissen gemäß Fig. 1 ist zum einen eine Überwachungseinrichtung 10.

[0057] Diese Überwachungseinrichtung 10 verfügt über ein oder mehrere Sensoren 12, mit denen ein Frachtbehältnis, im vorliegenden Beispiel ein See-, Land- und/oder Normcontainer, überwacht werden kann.

[0058] Die Überwachungseinrichtung 10 liefert bei einer Verletzung der integrität des Containers Ereignisdaten, die diese Verletzung repräsentieren. Eine Integritätsverletzung umfasst dabei insbesondere das Öffnen und/oder das Schließen einer oder mehrerer Belade- oder Zugangstüren zu dem Container, und zwar unabhängig davon, ob dieses Öffnen/Schließen berechtigt bzw. autorisiert erfolgt oder nicht.

[0059] Der oder die Sensoren 12 stehen mit einer Steuereinheit 11 der Überwachungseinrichtung 10 in Betriebskommunikation. Die Kommunikation zwischen Steuereinheit 11 und Sensor 12 kann drahtgebunden erfolgen, aber auch drahtlos per Funk oder dergleichen.

[0060] Die Überwachungseinrichtung 10 wird bevorzugt mitsamt dem Sensor 12 innerhalb des zu überwachenden Containers positioniert und dort mittels geeigneter Maßnahmen befestigt.

[0061] Mit dem erfindungsgemäßen System wird in der Regel nicht nur ein Container überwacht, sondern eine Vielzahl von Containern. Dabei werden den jeweiligen Containern des Systems jeweils gleichartige Überwachungseinrichtungen 10 zugeordnet. Die Zuordnung der jeweiligen Überwachungseinrichtungen 10 zu den jeweiligen Transportcontainem erfolgt üblicherweise zu Beginn eines Transportes.

[0062] In der Regel wird ein Transport eines Transportcontainers von einem Belade- oder Startort zu einem Zielort durch ein Logistikuntemehmen organisiert. Gegebenfalls beauftragt dieses Logistikuntemehmen einen externen Versender mit der eigentlichen Beladung des Containers und dem eigentlichen Transport desselben.

[0063] Der Versender rüstet den jeweils für einen Transport vorgesehenen Transportcontainer mit der Überwachungseinrichtung 10 aus. Anschließend wird die Überwachungseinrichtung 10 durch Betätigung eines entsprechenden Ein-/Aus-Schalters eingeschaltet. Um sämtliche Funktionen der Überwachungseinrichtung 10 zu gewährleisten, verfügt diese über eine geeignete, autarke Energieversorgung, etwa über entsprechende Batterien oder Akkumulatoren.

[0064] Ab dem Einschaltvorgang beginnt die Überwachungseinrichtung 10 bzw. der oder die Sensoren 12 derselben, den Container zu überwachen.

[0065] In der Regel ist mindestens einer der Sensoren 12 als den Status der Tür des Transportcontainers überwachender Türsensor ausgebildet. Einer der Sensoren 12 kann des Weiteren ein Bewegungssensor sein, der Bewegungen innerhalb des Container und/oder Bewegungen des Containers selbst überwacht. Weiter ist denkbar, Detektoren einzusetzen, die explosive Sprengstoffe erkennen können oder gefährliche Strahlung, insbesondere radioaktive Strahlung. Der oder die Sensoren 12 erzeugen dabei ab dem Einschaltvorgang der Überwachungseinrichtung 10 geeignete Daten.

[0066] Jede Überwachungseinrichtung 10 des erfindungsgemäßen Systems ist durch geeignete drahtlose Datenübertragungstechniken, bevorzugt Kommunikationstechniken unter Einbeziehung von Satelliten (Funk), mit einem Analysezentrum 14 verbunden bzw. verbindbar. Dazu weisen die Überwachungseinrichtungen 10 sowie das Analysezentrum 14 jeweils geeignete Kommunikationsmodule 15 auf, nämlich Sende- und/oder Empfangsmodule, insbesondere funkbasiert. Hierfür geeignete Sende- und/oder Empfangsmodule sind inklusive der dafür notwendigen Antennentechnik im Stand der Technik bekannt und werden hier nicht näher erläutert.

[0067] Bevorzugt im Anschluss an die zuvor bereits beschriebene Installation einer Überwachungseinrichtung 10 in dem jeweiligen Transportcontainer wird dieser mit dem zu befördemden Frachtgut beladen. Grundsätzlich kann das Beladen natürtich auch vor der Installation der Überwachungseinrichtung 10 erfolgen.

[0068] Um sicherheitstechnischen Anforderungen gerecht werden zu können, wird erfindungsgemäß sichergestellt, dass das Beladen und Verschließen des Containers nachweislich von einer dazu berechtigten Person vorgenommen wird:

[0069] Zu diesem Zweck sieht das System die Verwendung von elektronischen Autorisierungscodes vor. Mithilfe der Autorisierungscodes können Verletzungen

der Integrität des Containers autorisiert werden. Insbesondere kann ein Öffnen und/oder ein Verschließen einer Containerzugangstür auf diesem Wege als berechtigt gekennzeichnet werden.

[0070] Die Autorisierungscodes umfassen bei der vorliegenden Ausführungsform insbesondere digitale Zertifikate, mit denen die Identität der den jeweiligen Autorisierungscode übermittelnden, berechtigten Person überprüfbar ist. Weiter umfassen die Autorisierungscodes Daten, die die jeweilige Überwachungseinrichtung 10 und/oder den jeweiligen Container eindeutig kennzeichnen, für die Autorisierungscodes jeweils eingesetzt werden.

[0071] Die Autorisierungscodes sind dabei zuvor von entsprechenden Computereinrichtungen in dem Analysezentrum 14 generiert und der berechtigten Person von dem Analysezentrum 14 übermittelt worden. Die Übermittlung kann dabei etwa über entsprechend gesicherte, elektronische Datentransportwege erfolgen.

[0072] In einer Variante der Erfindung werden die elektronischen Autorisierungscodes von dem Analysezentrum 14 unmittelbar per Datenfernübertragung einer als Handgerät - beispielsweise als Handheld - ausgebildeten Autorisierungseinrichtung 16 übertragen. Beispielsweise ist denkbar, dass sich die berechtigte Person die Autorisierungscodes über eine gesicherte, drahtlose Intemetverbindung von einem entsprechenden Server des Analysezentrums 14 auf die Autorisierungseinrichtung 16 herunterlädt. In der Autorisierungseinrichtung 16 bzw. einem der Autorisierungseinrichtung 16 zugeordneten Speicher werden die Autorisierungscodes anschließend gespeichert.

[0073] Nach dem Beladen des Containers verschließt die dazu berechtigte Person die Tür desselben. Dieser Verschließvorgang führt zu einem Signal des Türsensors 12 der Überwachungseinrichtung 10. Denn in dem installierten und eingeschalteten Zustand der Überwachungseinrichtung 10 führt jede Integritätsverietzung, also in diesem Fall jedes Verschließen und jedes Öffnen der Zugangstür des Containers, zu einem derartigen Türsensorsignal. Das erzeugte Signal bzw. entsprechende Ereignisdaten, die dieses Signal repräsentieren, werden unmittelbar anschließend automatisch über die Kommunikationsmodule 15 per drahtloser Datenfernübertragung an das Analysezentrum 14 übertragen. Das übertragen der Ereignisdaten wird demnach durch die Erfassung des Öffnens der Tür durch den Türsensor 12 ausgelöst bzw. getriggert

[0074] Die berechtigte Person kann den Schließvorgang autorisieren, um zu verhindern, dass das Schließsignal im Analysezentrum 14 einen Alarm auslöst.

[0075] In einer Umsetzung der Erfindung ist zu diesem Zweck vorgesehen, dass die berechtigte Person mittels der Autorisierungseinrichtung 16 die Übertragung eines der zuvor der Autorisierungseinrichtung 16 übermittelten, für die Autorisierung geeigneten Codes an das Analysezentrum 14 initiiert. Dazu positioniert sich die berechtigte Person mit der Autorisierungseinrichtung 16 in der Hand vor dem Container. Durch Betätigung geeigneter Steuerelemente der Autorisierungseinrichtung 16 wird eine Übertragung eines der Codes initiiert, und zwar per drahtloser Kurzstreckendatenübertragung zunächst ausgehend von der Autorisierungseinrichtung 16 hin zu der Überwachungseinrichtung 10. Die Autorisierungseinrichtung 16 und die Überwachungseinrichtung 10 verfügen zu diesem Zweck über für Kurzstreckendatenübertragung geeignete Kommunikationsmodule.

[0076] Die Übertragungseinrichtung 10 leitet den ihr übermittelten Code über die Kommunikationsmodule 15 anschließend an das Analysezentrum 14 weiter. Die übertragenen Autorisierungscodes werden nachfolgend in einem der dem Analysezentrum 14 zugeordneten Speicher abgespeichert.

[0077] In einer dem Analysezentrum 14 zugeordneten Analyseeinrichtung 18 erfolgt die Bewertung des übermittelten Schließsignals im Hinblick darauf, ob der Schließvorgang autorisiert oder unautorisiert erfolgt war. Die Anaiyseeinrichtung 18 kann zu diesem Zweck beispielsweise eine geeignet ausgebildete Steuerungseinrichtung sein und/oder eine mit geeigneter Software ausgebildete Computereinrichtung. Sie überprüft, ob in dem dem Analysezentrum 14 zugeordneten Speicher jeweils zeitgleich zu dem Eintreffen der das Schließen der Tür repräsentierenden Ereignisdaten oder in einer festgelegten Zeitspanne davor oder danach ein passender Autorisierungscode eingetroffen ist. Die Analyseeinrichtung 18 greift hierfür auf den dem Analysezentrum 14 und somit auch ihr zugeordneten Speicher zu.

[0078] Die Analyseeinrichtung 18 überprüft des Weiteren mittels geeigneter Algorithmen insbesondere die Gültigkeit bzw. Echtheit des jeweils übermittelten Autorisierungscodes. Dazu vergleicht sie den übermittelten Autorisierungscode mit in einem oder dem der Analyseeinrichtung 18 bzw. dem Analysezentrum 14 zugeordneten Speicher hinterlegten Autorisierungscodeparametem. Diese Autorisierungscodeparameter müssen in diesem Fall mit dem übermittelten Autorisierungscode übereinstimmen oder in geeigneten Beziehungen zu diesem stehen, damit letzterer als gültig bzw. echt bewertet wird. Bevorzugt sind die Autorisierungscodeparameter in einer in dem Speicher installierten Datenbank abgespeichert.

[0079] Falls demnach die zum Schließvorgang berechtigte Person in der oben beschriebenen Weise in unmittelbarer und festgelegter zeitlicher Nähe zu dem Schließen der Containertür dem Analysezentrum 14 einen geeigneten Autorisierungscode übersendet, wird das Schließen der Tür von der Analyseeinrichtung als autorisiert erfolgt bewertet.

[0080] Daraufhin wird entsprechend im Analysezentrum keine Alarmmeldung erzeugt.

[0081] Etwas anderes gilt allerdings, wenn während des Transportweges nicht berechtigte Personen die Integrität des Containers unberechtigt verletzen sollten, indem sie beispielsweise über die Tür des Containers in

dessen Innenraum eindringen.

[0082] In diesem Fall erzeugt der Türsensor 12 zunächst erneut entsprechende Ereignisdaten, d.h. Daten, die die Integritätsverletzung - in diesem Fall die Türöffnung - repräsentieren.

[0083] Auch diese Ereignisdaten werden automatisch an das Analysezentrum 14 übertragen. In dem vorliegenden Fall des unberechtigten Öffnens des Containers wird allerdings naturgemäß dem Analysezentrum 14 kein geeigneter Autorisierungscode übertragen. In dem dem Analysezentrum 14 zugeordneten Speicher ist entsprechend kein zur Autorisierung des Öffnungsvorgangs geeigneter Autorisierungscode gespeichert.

[0084] Demzufolge liefert die nachfolgende Bewertung der das Öffnungssignal repräsentierenden Ereignisdaten das Ergebnis, dass die Öffnung unautorisiert erfolgt sein muss. Die entsprechende Bewertung führt wiederum die Analyseeinrichtung 18 durch, die zu diesem Zweck in der bereits beschriebenen Weise wiederum den dem Analysezentrum 14 zugeordneten Speicher ausliest. Dabei wird festgestellt, dass dort kein geeigneter Autorisierungscode gespeichert ist.

[0085] In Reaktion auf die Bewertung der Öffnung als unautorisiert können geeignete Maßnahmen eingeleitet werden. Beispielsweise kann mittels eines Signalgebers ein einen Alarmzustand repräsentierendes, insbesondere akustisches oder optisches Alarmsignal erzeugt werden, das verschiedenen privaten und behördlichen Instanzen zugeleitet wird. So können beispielsweise Sicherheitsbehörden benachrichtigt werden, die den betreffenden Container untersuchen. Im einfachsten Fall kann die dem Analysezentrum 14 zugeordnete Analyseeinrichtung 18 die Versendung einer entsprechenden E-Mail oder eine SMS initiieren.

[0086] Insbesondere insofern die Überwachungseinrichtung 10 ein geeignetes Ortungsmodul aufweist, etwa ein GPS-Modul, kann des Weiteren problemlos der genaue Standort des betreffenden Containers geortet werden.

[0087] In einem anderen von der Erfindung erfassten Szenario erfolgt die Öffnung des Containers - anders als in dem vorstehend beschriebenen Fall - autorisiert. Dies kann insbesondere dann sinnvoll sein, wenn der Container auf dem Transportweg vor Erreichen des eigentlichen Endzielortes mit weiterem Frachtgut zwischenbeladen werden soll.

[0088] Erfindungsgemäß kann eine zu der Zwischenbeladung berechtigte Person den Container öffnen, ohne unmittelbar einen Alarm auszulösen. Der Öffnungsvorgang des Containers wird zwar in der oben beschriebenen Weise wiederum von dem entsprechenden Sensor 12 der Überwachungseinrichtung 10 erfasst und entsprechende Ereignisdaten, die diesen Öffnungsvorgang repräsentieren, werden in der Folge dem Analysezentrum 14 übersandt. Wenn die berechtigte Person in analoger Weise wie bei dem weiter oben beschriebenen Verschließvorgang allerdings einen geeigneten Autorisierungscode innerhalb der festgelegten zeitlichen Grenzen an das Analysezentrum 14 versendet, wird dort das Öffnen des Containers in diesem Fall als autorisiert erfolgt bewertet.

[0089] Die überwachungseinrichtung 10 bleibt während des zwischenzeitlichen Beladens des Containers aktiv. Der Container wird daher weiterhin überwacht. Die Überwachungseinrichtung 10 sendet weiterhin Ereignisdaten an das Analysezentrum 14. Wenn etwa einer der Sensoren 12 als Bewegungssensor ausgebildet ist, sendet dieser auch nach dem autorisierten Öffnen des Containers fortlaufend Daten zu Bewegungen innerhalb des Container an das Analysezentrum 14.

[0090] Sobald das Beladen im Rahmen dieses Zwischenbeladevorgangs abgeschlossen ist, kann die berechtigte Person mittels eines weiteren Autorisierungscodes den Container erneut autorisiert verschließen.

[0091] Die Erfindung ermöglicht insgesamt eine lükkenlose Überwachung des Containers ausgehend von einem ersten autorisierten Verschließen über den gesamten Transportweg unter Einschluss möglicher Zwischenbeladungen bis zum Erreichen des Zielortes.

[0092] Wie der Fachmann des Standes der Technik erkennt, existieren naturgemäß verschiedene erfindungsgemäße Alternativen zu dem oben beschriebenen Ausführungsbeispiel. Wie der Fachmann insbesondere erkennt, existieren verschiedene Möglichkeiten, die einzelnen Komponenten des Systems auszubilden und/oder miteinander über geeignete Datenschnittstellen miteinander zu verbinden, um das erfindungsgemäße Verfahren durchzuführen.

Bezugszeichenliste:

[0093]

10	Überwachungseinrichtung
11	Steuereinheit
12	Sensor
14	Analysezentrum
15	Kommunikationsmodul
16	Autorisierungseinheit
18	Computereinrichtung
20	Datenbank

Patentansprüche

1. Verfahren zur Überwachung, insbesondere zur Echtzeitüberwachung, der Integrität eines Frachtbehältnisses, vorzugsweise eines Transportcontainers, wobei das Frachtbehältnis eine diesem zugeordnete Überwachungseinrichtung (10) aufweist, die über mindestens einen, die Integrität des Frachtbehältnisses überwachenden Überwachungssensor (12) verfügt, **gekennzeichnet durch** folgende Maßnahmen:

   - nach der Erfassung eines die Frachtbehältni-

sintegrität verletzenden Ereignisses **durch** den Überwachungssensor (12) werden einem entfernten Analysezentrum (14), insbesondere einer dem Analysezentrum (14) zugeordneten Analyseeinrichtung (18), Ereignisdaten übermittelt, die die Integritätsverletzung repräsentieren,

- in dem Analysezentrum (14), insbesondere in der diesem zugeordneten Analyseeinrichtung (18), werden die übermittelten Ereignisdaten anhand vorbestimmter Kriterien im Hinblick auf eine entweder berechtigte - autorisierte - oder eine unberechtigte - unautorisierte - Integritätsverletzung des Frachtbehältnisses bewertet
- die Integritätsverletzung, insbesondere ein Öffnen oder Verschließen eines Frachtbehältnisses, wird als berechtigt bzw. autorisiert bewertet, falls dem Analysezentrum (14) - insbesondere im Zeitpunkt des Eintreffens der Ereignisdaten in dem Analysezentrum (14) oder in einer insbesondere vorbestimmten Zeitspanne vor oder nach dem Eintreffen derselben - zu den die Integritätsverletzung repräsentierenden Ereignisdaten ein die Berechtigung der Integritätsverletzung repräsentierender Autorisierungscode vorliegt.

2. Verfahren gemäß Anspruch 1, **dadurch gekennzeichnet, dass** die Überwachungseinrichtung (10) mittels eines geeigneten Sensors (12) als Integritätsverletzungen vorzugsweise mindestens ein Öffnen oder Verschließen des Frachtbehältnisses erfasst.

3. Verfahren gemäß Anspruch 2, **dadurch gekennzeichnet, dass** die Überwachungseinrichtung (10) das Frachtbehältnis auch in dem Zeitraum zwischen einem autorisiertem Öffnen des Frachtbehältnisses und einem späteren autorisierten Verschließen des Frachtbehältnisses überwacht, sodass Ereignisdaten, die eine Verletzung der Frachtbehältnisintegrität repräsentieren, dem Analysezentrum (14) auch in diesem Zeitraum übersendet werden.

4. Verfahren gemäß einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** die Überwachungseinrichtung (10) das Frachtbehältnis bis zu ihrem Abschalten unterbrechungslos überwacht.

5. Verfahren gemäß einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** die Integritätsverletzung als unberechtigt bzw. unautorisiert bewertet wird, falls dem Analysezentrum (14) - insbesondere im Zeitpunkt des Eintreffens der Ereignisdaten in dem Analysezentrum (14) oder in einer insbesondere vorbestimmten Zeitspanne vor oder nach dem Eintreffen derselben - keine die Berechtigung der Integritätsverletzung repräsentierende Autorisierung vorliegt.

6. Verfahren gemäß einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** zur Autorisierung von Integritätsverletzungen elektronische Codes verwendet werden, vorzugsweise elektronische Codes, die zuvor in dem Analysezentrum (14) generiert wurden.

7. Verfahren gemäß einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** zur Herbeiführung einer Autorisierung einer Integritätsverletzung dem Analysezentrum (14) im Zeitpunkt des Eintreffens der Ereignisdaten bzw. in der Zeitspanne vor oder nach dem Eintreffen, insbesondere drahtlos, ein die Berechtigung der Integritätsverletzung repräsentierender, elektronischer Autorisierungscode übermittelt wird.

8. Verfahren gemäß einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** die Gültigkeit des elektronischen Autorisierungscodes überprüft wird, insbesondere anhand von vorzugsweise in einer dem Analysezentrum (14) zugeordneten Datenbank hinterlegten Autorisierungsparametern.

9. Verfahren gemäß einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** der übermittelte Autorisierungscode als gültig bewertet wird, insofern der übermittelte Autorisierungscode als ein zuvor generierter Autorisierungscode identifiziert wird und/oder insofern ein oder mehrere der hinterlegten Autorisierungsparameter mit dem Autorisierungscode übereinstimmen.

10. Verfahren gemäß einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** einem oder mehreren zu überwachenden Frachtbehältnissen und/oder einer oder mehreren Gruppen von Frachtbehältnissen mittelbar oder unmittelbar insbesondere jeweils eindeutig ein oder mehrere elektronische, bevorzugt zuvor in dem Analysezentrum (14) generierte, Autorisierungscodes zugeordnet sind.

11. Verfahren gemäß einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** die zugeordneten Autorisierungscodes und/oder Parameter derselben in einer insbesondere dem Analysezentrum (14) zugeordneten Datenbank hinterlegt sind.

12. Verfahren gemäß einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** im Falle einer Bewertung einer Integritätsverletzung als unautorisiert insbesondere mittels eines geeigneten Signalerzeugers ein Signal erzeugt wird,

insbesondere ein einen Alarmzustand repräsentierendes Signal.

13. Verfahren gemäß einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** die Autorisierungscodes jeweils Daten umfassen, die die Überprüfung einer behaupteten Identität der die Autorisierung initiierenden Person oder Institution ermöglichen, insbesondere jeweils mindestens ein digitales Zertifikate oder eine digitale Signatur.

14. Verfahren gemäß einem oder mehreren der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** die die Verletzung der Frachtbehältnisintegrität repräsentierenden Ereignisdaten unmittelbar nach der Erfassung dieser Daten durch den Überwachungssensor (12) per Datenfernübertragung automatisch, insbesondere getriggert bzw. ausgelöst durch diese Erfassung, an das Analysezentrum (14) gesandt werden.

15. System zur Überwachung, insbesondere zur Echtzeitüberwachung, der Integrität eines Frachtbehältnisses, insbesondere eines Transportcontainers, insbesondere zur Durchführung des Verfahrens gemäß einem oder mehreren der vorhergehenden Patentansprüche, mit einem oder mehreren Frachtbehältnissen, wobei jedem Frachtbehältnis jeweils mindestens eine Überwachungseinrichtung (10) zugeordnet ist, die über mindestens einen, die Integrität des Frachtbehältnisses überwachenden Überwachungssensor (12) verfügt, sowie mit einem von dem Frachtbehältnis entfernten Analysezentrum (14), dem nach der Erfassung eines die Frachtbehältnisintegrität verletzenden Ereignisses durch den Überwachungssensor (12) die Integritätsverletzung repräsentierende Ereignisdaten drahtlos übermittelbar sind, wobei in dem Analysezentrum (14) die übermittelten Ereignisdaten mittels einer geeigneten Analyseeinrichtung (18) anhand vorbestimmter Kriterien im Hinblick auf eine entweder berechtigte - autorisierte - oder eine unberechtigte - unautorisierte - Integritätsverletzung des Frachtbehältnisses bewertbar sind.

16. System gemäß Anspruch 15, **dadurch gekennzeichnet, dass** die Analyseeinrichtung zur Bewertung der Integritätsverletzung eine geeignet ausgebildete Steuerungs- und/oder Computereinrichtung (18) ist.

17. System gemäß Anspruch 15 oder 16, **dadurch gekennzeichnet, dass** der Überwachungseinrichtung (10) eine geeignete Sendeeinrichtung (15) zugeordnet ist, vorzugsweise eine Sende- und Empfangseinrichtung, sowie dem Analysezentrum mindestens eine geeignete Empfangeinrichtung (15), vorzugsweise ebenfalls eine Sende- und Empfangseinrichtung, über die die Ereignisdaten drahtlos übermittelbar sind.

18. System gemäß einem oder mehreren der Ansprüche 15 - 17, **gekennzeichnet durch** ein oder mehrere Merkmale der Ansprüche 1-14.

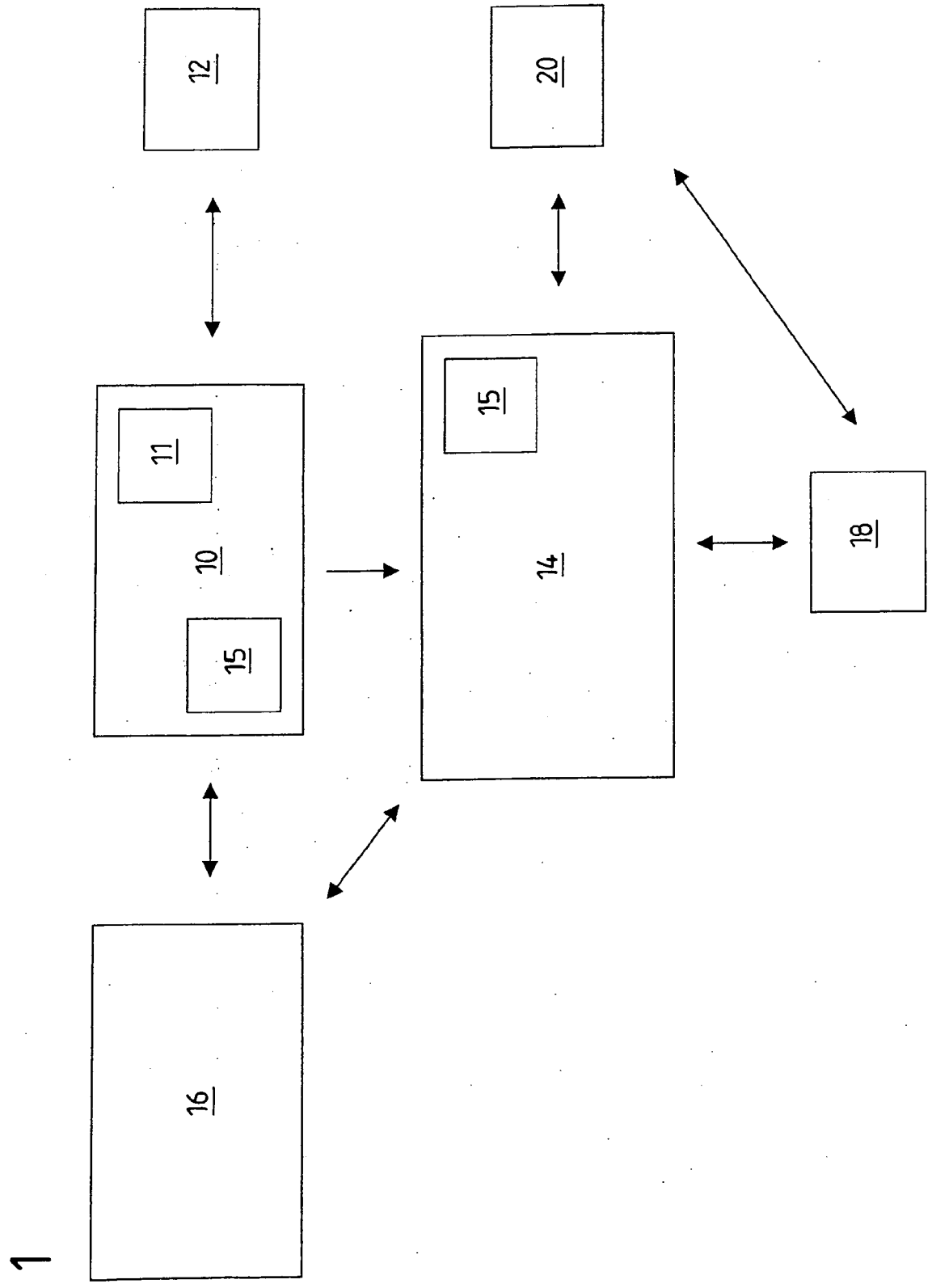


Fig. 1

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 10 00 1663

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (IPC)
X	WO 2006/119123 A2 (ASTRIN ARTHUR W [US]) 9. November 2006 (2006-11-09) * Zusammenfassung * * Seite 7, Zeile 3 - Seite 9, Zeile 23 * * Seite 13, Zeile 17 - Seite 15, Zeile 29 * * Seite 17, Zeile 12 - Seite 19, Zeile 21 * * Abbildung 9 * * Seite 12, Zeile 15 - Zeile 18 * -----	1-18	INV. G07C5/08 G07C9/00 G08B13/14 G08B25/10
X	US 2007/268138 A1 (CHUNG KEVIN K [US] ET AL) 22. November 2007 (2007-11-22) * Absatz [0151] - Absatz [0159] * * Zusammenfassung * * Absatz [0111] - Absatz [0120] * * Absatz [0133] * -----	1-18	
X	US 2008/303663 A1 (SMITH TERRY [US] ET AL) 11. Dezember 2008 (2008-12-11) * Zusammenfassung * * Absatz [0005] * * Absatz [0020] * * Absatz [0023] - Absatz [0032] * * Absatz [0037] - Absatz [0038] * * Absatz [0042] * * Absatz [0047] - Absatz [0049] * * Abbildungen 2, 4 * -----	1-18	RECHERCHIERTE SACHGEBIETE (IPC) G07C G08B

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
München	28. Mai 2010	Stenger, Michael

KATEGORIE DER GENANNTEN DOKUMENTE

X : von besonderer Bedeutung allein betrachtet
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
A : technologischer Hintergrund
O : nichtschriftliche Offenbarung
P : Zwischenliteratur

T : der Erfindung zugrunde liegende Theorien oder Grundsätze
E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
D : in der Anmeldung angeführtes Dokument
L : aus anderen Gründen angeführtes Dokument

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

EPO FORM 1503 03.82 (P04C03)

ANHANG ZUM EUROPÄISCHEN RECHERCHENBERICHT ÜBER DIE EUROPÄISCHE PATENTANMELDUNG NR. EP 10 00 1663

In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten europäischen Recherchenbericht angeführten Patentdokumente angegeben.
Die Angaben über die Familienmitglieder entsprechen dem Stand der Datei des Europäischen Patentamts am
Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

28-05-2010

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 2006119123 A2	09-11-2006	US 2006250235 A1	09-11-2006
US 2007268138 A1	22-11-2007	KEINE	
US 2008303663 A1	11-12-2008	KEINE	

EPO FORM P0461

Für nähere Einzelheiten zu diesem Anhang : siehe Amtsblatt des Europäischen Patentamts, Nr.12/82

IN DER BESCHREIBUNG AUFGEFÜHRTE DOKUMENTE

Diese Liste der vom Anmelder aufgeführten Dokumente wurde ausschließlich zur Information des Lesers aufgenommen und ist nicht Bestandteil des europäischen Patentdokumentes. Sie wurde mit größter Sorgfalt zusammengestellt; das EPA übernimmt jedoch keinerlei Haftung für etwaige Fehler oder Auslassungen.

In der Beschreibung aufgeführte Patentdokumente

- US 4750197 A **[0004] [0005]**
- DE 602004008248 T2 **[0005]**