(19) LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Économie

(11) N° de publication : **LU501035**

(12) **BREVET D'INVENTION** **B1**

(21) N° de dépôt: LU501035

(22) Date de dépôt: 17/12/2021

(51) Int. Cl.:
H04L 12/46, H04L 45/243, H04L 45/247, H04L 45/00, H04L 45/28, H04L 9/40

(30) Priorité:

(43) Date de mise à disposition du public: 20/06/2023

(47) Date de délivrance: 20/06/2023

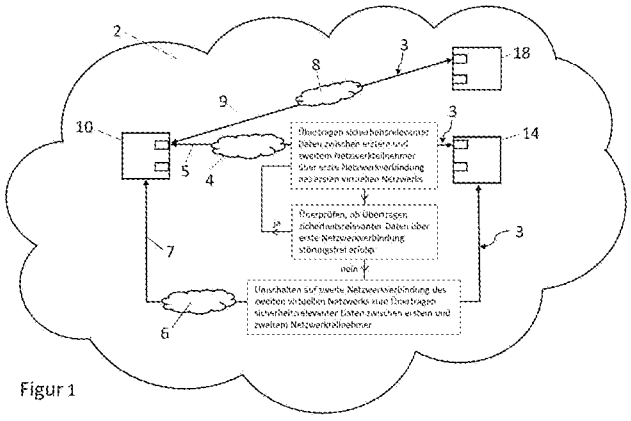
(73) Titulaire(s):
PHOENIX CONTACT GMBH & CO. KG –
32825 Blomberg (Allemagne)

(72) Inventeur(s):
OSTER Viktor – Allemagne, HELLMANN Klas – Allemagne

(74) Mandataire(s):
PHOENIX CONTACT GMBH & CO. KG –
32825 Blomberg (Allemagne)

(54) **Verfahren und System zum Absichern des Austausches von Daten in einem Netzwerksystem für industrielle Steuerungen.**

(57) Die vorliegende Erfindung betrifft ein Verfahren zum Übertragen von Daten über ein physikalisches Netzwerk für industrielle Steuerungen, aufweisend eine Mehrzahl von Netzwerkteilnehmern. Für den Fall, dass sicherheitsrelevante Daten zwischen wenigstens einem ersten und zweiten Netzwerkteilnehmer aus der Mehrzahl von Netzwerkteilnehmern übertragen werden sollen, umfasst das Verfahren folgende Schritte: - Übertragen dieser sicherheitsrelevanten Daten zwischen dem ersten und zweiten Netzwerkteilnehmer zumindest über eine erste Netzwerkverbindung eines ersten virtuellen Netzwerks in dem physikalischen Netzwerk, - Überprüfen, ob das Übertragen der sicherheitsrelevanten Daten über die erste Netzwerkverbindung störungsfrei erfolgt, - im Falle eines Feststellens eines nicht störungsfreien Übertragens über die erste Netzwerkverbindung Umschalten auf eine zweite, von der ersten verschiedenen Netzwerkverbindung eines zweiten virtuellen Netzwerks in dem physikalischen Netzwerk zum Übertragen dieser sicherheitsrelevanten Daten zwischen dem ersten und zweiten Netzwerkteilnehmer. Ferner betrifft die vorliegende Erfindung ein System, welches zum Durchführen dieser Verfahrensschritte eingerichtet ist und eine Diagnoseeinheit zum Überprüfen eines störungsfreien Übertragens umfasst.



Figur 1

Verfahren und System zum Absichern des Austausches von Daten in einem Netzwerksystem für industrielle Steuerungen

Die vorliegende Erfindung betrifft ein Verfahren zum Übertragen von Daten über ein physikalisches Netzwerk für industrielle Steuerungen, welches eine Mehrzahl von Netzwerkteilnehmern umfasst, wobei sicherheitsrelevante Daten zwischen wenigstens einem ersten und zweiten Netzwerkteilnehmer aus der Mehrzahl von Netzwerkteilnehmern übertragen werden sollen, und ferner ein System zum Durchführen des Verfahrens.

Bekanntermaßen kommen bei dem Austausch von Daten, insbesondere von sicherheitsrelevanten Daten, über Standard-Netzwerke spezielle Verfahren zum Einsatz, welche dem Erkennen von Fehlern, insbesondere dem Erkennen von einer Datenmanipulation, bei der Übertragung und/oder Speicherung dieser Daten dienen. Ein Beispiel für ein solches Verfahren ist die sog. zyklische Redundanzprüfung (cyclic redundancy check, CRC), bei welcher jedem Datenblock der Nutzdaten, d.h. der zu übertragendenden oder zu speichernden Daten, ein berechneter Prüfwert hinzugefügt wird, mit dessen Hilfe Fehler bei der Datenübertragung und Datenspeicherung erkannt werden können. Alle diese Verfahren sind grundsätzlich so konzipiert, dass sie den Anforderungen gemäß dem für die Prüfung von Bussystemen für die Übertragung sicherheitsbezogener Nachrichten an Maschinen geltenden Grundsatz GS ET 26 genügen und somit die darin bezeichneten Fehlermodelle abdecken. Da es immer häufiger zu unberechtigten Zugriffen wie Hacker-Angriffe und Manipulationen bei der Übertragung von sicherheitsrelevanten Daten kommt, werden die Standard-Netzwerke u.a. im Hinblick auf diese Gefahr weiterentwickelt zu sicheren Netzwerken im Sinne von Security, d.h. im Sinne des Schutzes von Daten.

Eine solche Weiterentwicklung der Standard-Netzwerke ist insbesondere vor dem Hintergrund des Zukunftsprojekts Industrie 4.0 zur umfassenden Digitalisierung von Prozessen, Verfahrensabläufen usw. in der Industrie und Wirtschaft und dem damit verbundenen Ausbau von Netzwerken und Netzwerkinfrastrukturen, beispielsweise unter Verwendung von Cloud Technologien, zwingend erforderlich. Die Verwendung von sog. „safety guards“, d.h. Schutz- bzw. Sicherheitsvorrichtungen zum

automatischen Erkennen von Fehlern, insbesondere zum automatischen Erkennen einer Datenmanipulation, bei der Übertragung und/oder Speicherung von sicherheitsrelevanten Daten ist meist jedoch mit hohen Kosten und auch mit starken Einschränkungen verbunden. Eine Einschränkung kann beispielsweise sein, dass alle Hardware- und Software- bzw. Firmware-Einheiten in der Sicherheitskette entsprechend dem jeweiligen Sicherheitsstandard der safety guards entwickelt und qualifiziert sein müssen. Darunter leidet jedoch insbesondere die oftmals gewünschte Flexibilität, z.B. bei modularen Maschinen bzw. Anwendungen.

Auch kommen im Hinblick auf den Sicherheitsaspekt z.B. redundante Systeme bzw. redundante Bauteile u.a. innerhalb einer Baugruppe zum Einsatz. Redundante Systeme haben aber in der Regel den Nachteil, dass Veränderungen in diesen Systemen meist sehr aufwändig sind.

Die Sicherstellung einer verfälschungsfreien Übertragung von sicherheitsrelevanten Daten erfolgt meist durch eine Reihe von Zusatzinformationen, beispielsweise einem den zu übertragenden Daten zugefügten berechneten Prüfwert (CRC-Wert). Über diese Zusatzinformationen lässt sich eine Manipulation der zu übertragenden oder übertragenen Daten sicher erkennen. Somit ist das zugrundeliegende Sicherheitssystem in der Lage, gültige Daten von fehlerhaften, insbesondere manipulierten Daten zu unterscheiden und entsprechend zu reagieren. Wird beispielsweise eine fehlerhafte Datenübertragung erkannt, so wird das Sicherheitssystem in der Regel als Sicherheitsreaktion in einen sicheren Zustand überführt. Dies hat jedoch in den meisten Fällen eine Reduzierung der Verfügbarkeit des Sicherheitssystems zur Folge. In Maschinen führt dieses Verhalten meist zu einem unerwünschten Maschinenstillstand, wobei in einem solchen Fall die Überführung in einen sicheren Zustand einem NOT-AUS als Sicherheitsreaktion entspricht. Eine schlechtere Verfügbarkeit von Maschinen und Anlagen kann teils dazu führen, dass deren Bediener die von den Maschinen oder Anlagen ausgehenden Sicherheitssignale überbrücken, damit Störungen kein Abschalten der Maschine oder Anlage bewirken. Die von einer manipulierten Maschine oder Anlage ausgehende Gefahr kann in einem solchen Fall jedoch größer als eine von einer Maschine oder Anlage ohne Sicherheitseinrichtungen ausgehende Gefahr sein. In der Regel verlässt sich der Bediener einer Maschine oder Anlage auf die darin

installierten Sicherheitseinrichtungen und kann nicht immer erkennen, dass die Maschine oder Anlage manipuliert wurde bzw. Sicherheitssignale überbrückt wurden, da solche Manipulationen oft nur für eine kurze Zeit, z.B. für eine Schicht, vorgenommen wurden.

Vor diesem Hintergrund ist es zumindest eine Aufgabe der vorliegenden Erfindung, ein Verfahren zu entwickeln sowie ein System zum Durchführen dieses Verfahrens bereitzustellen, welches die zuvor genannten Nachteile überwindet und mit welchem im Falle des Erkennens von Fehlern, insbesondere Manipulationen, bei der Übertragung von sicherheitsrelevanten Daten weiterhin eine sichere Datenübertragung ermöglicht wird und gleichzeitig die Verfügbarkeit des zugrundeliegenden Systems zumindest für eine begrenzte Zeit aufrecht erhalten wird.

Die Lösung der vorliegenden Erfindung ist durch ein Verfahren mit den Merkmalen nach dem unabhängigen Anspruch 1 und durch ein System zum Durchführen dieses Verfahrens mit den Merkmalen nach dem unabhängigen Anspruch 10 gegeben. Vorteilhafte Ausgestaltungen und Weiterentwicklungen sind Gegenstand der weiteren Merkmale der Unteransprüche.

Dementsprechend geht die Lösung gemäß der Erfindung von einem Verfahren zum Übertragen von Daten über ein physikalisches Netzwerk für industrielle Steuerungen aus, welches eine Mehrzahl von Netzwerkteilnehmern umfasst. Für den Fall, dass sicherheitsrelevante Daten zwischen wenigstens einem ersten und zweiten Netzwerkteilnehmer aus der Mehrzahl von Netzwerkteilnehmern übertragen werden sollen, weist das Verfahren folgende Schritte auf:

- Übertragen dieser sicherheitsrelevanten Daten zwischen dem ersten und dem zweiten Netzwerkteilnehmer zumindest über eine erste Netzwerkverbindung eines ersten virtuellen Netzwerks in dem physikalischen Netzwerk,
- Überprüfen, ob das Übertragen der sicherheitsrelevanten Daten über die erste Netzwerkverbindung störungsfrei erfolgt,
- im Falle eines Feststellens eines nicht störungsfreien Übertragens über die erste Netzwerkverbindung Umschalten auf eine zweite, von der ersten verschiedenen Netzwerkverbindung eines zweiten virtuellen Netzwerks in dem physikalischen

Netzwerk zum Übertragen dieser sicherheitsrelevanten Daten zwischen dem ersten und zweiten Netzwerkteilnehmer.

Das zuvor beschriebene Verfahren ermöglicht durch den Schritt des Umschaltens auf eine zweite, von der ersten verschiedenen Netzwerkverbindung eines zweiten virtuellen Netzwerks in dem physikalischen Netzwerk, dass das Übertragen der sicherheitsrelevanten Daten zwischen dem ersten und zweiten Netzwerkteilnehmer auch weiterhin erfolgen kann, obwohl bei der Übertragung der sicherheitsrelevanten Daten zumindest über die erste Netzwerkverbindung eine nicht störungsfreie Übertragung, beispielsweise bei der Übertragung aufgetretene Fehler, erkannt wurde. Dies wird dadurch erreicht, dass nach dem Erkennen, insbesondere unmittelbar nach dem Erkennen, einer nicht störungsfreien Übertragung über die erste virtuelle Netzwerkverbindung auf eine zweite virtuelle Netzwerkverbindung, die von der ersten virtuellen Netzwerkverbindung verschieden ist, umgeschaltet wird, um die sicherheitsrelevanten Daten zwischen dem ersten und zweiten Netzwerkteilnehmer nicht mehr über die erste virtuelle Netzwerkverbindung, sondern über diese zweite virtuelle Netzwerkverbindung zu übertragen. Dabei erfolgt das Übertragen der sicherheitsrelevanten Daten über die zumindest erste Netzwerkverbindung des ersten virtuellen Netzwerks und im Störungsfall über die zweite Netzwerkverbindung des zweiten virtuellen Netzwerks stets innerhalb desselben physikalischen Netzwerks, welches ein privates Netz, aber auch ein öffentliches Netz wie beispielsweise das Internet sein kann.

Unter einem Umschalten auf die zweite Netzwerkverbindung des zweiten virtuellen Netzwerks ist im Rahmen der vorliegenden Erfindung zu verstehen, dass entweder zumindest von der ersten Netzwerkverbindung auf die zweite Netzwerkverbindung umgeschaltet wird oder dass zumindest von der ersten und zweiten Netzwerkverbindung auf die zweite Netzwerkverbindung umgeschaltet wird. D.h. es ist nicht grundsätzlich ausgeschlossen, dass ein Übertragen der sicherheitsrelevanten Daten zwischen dem ersten und zweiten Netzwerkteilnehmer beispielsweise zusätzlich noch über eine dritte Netzwerkverbindung erfolgen kann. Demzufolge gibt es zumindest drei Schaltzustände hinsichtlich der zur Datenübertragung aufzubauenden bzw. aufgebauten virtuellen Netzwerkverbindungen, wobei ein erster Schaltzustand einer Übertragung der

sicherheitsrelevanten Daten ausschließlich über die erste Netzwerkverbindung des ersten virtuellen Netzwerks entspricht, ein zweiter Schaltzustand einer redundanten Übertragung der sicherheitsrelevanten Daten über die erste und zweite Netzwerkverbindung des ersten bzw. zweiten virtuellen Netzwerks entspricht und ein dritter Schaltzustand einer Übertragung der sicherheitsrelevanten Daten ausschließlich über die zweite Netzwerkverbindung des zweiten virtuellen Netzwerks entspricht. Der erste oder zweite Schaltzustand kann vor dem Schritt des Umschaltens auf die zweite Netzwerkverbindung eingenommen werden, während der dritte Schaltzustand stets nach dem Schritt des Umschaltens auf die zweite Netzwerkverbindung eingenommen wird. Weitere Schaltzustände können sich beispielsweise dadurch ergeben, dass zusätzlich zu den vorbeschriebenen Schaltzuständen noch ein Übertragen der sicherheitsrelevanten Daten über zumindest eine dritte Netzwerkverbindung eines dritten virtuellen Netzwerks stattfinden kann.

Das im Falle einer nicht störungsfreien Übertragung von sicherheitsrelevanten Daten über die erste Netzwerkverbindung erfolgende erfindungsgemäße Umschalten auf die zweite Netzwerkverbindung zum Übertragen der sicherheitsrelevanten Daten zwischen dem ersten und zweiten Netzwerkteilnehmer hat den großen Vorteil, dass ein System, welches zumindest eine Mehrzahl von Netzwerkteilnehmern einschließlich des ersten und zweiten Netzwerkteilnehmers umfasst, weiterhin zumindest für begrenzte Zeit Kommunikationsverbindungen zwischen dem ersten und zweiten Netzwerkteilnehmer aufrecht erhalten kann. Dies führt zu einer deutlichen Verbesserung bzw. Erhöhung der Verfügbarkeit des Systems. Ein Überführen des Systems in einen sicheren Zustand, wie ein NOT-AUS kann somit zumindest zeitlich verzögert, wenn nicht sogar vollständig vermieden werden, was u.a. die laufenden Betriebskosten des Systems reduziert und den dem System zugrundeliegenden Prozess zumindest nicht unmittelbar unterbricht. Während der Übertragung der sicherheitsrelevanten Daten über die zweite Netzwerkverbindung kann zudem versucht werden, die beim Übertragen der sicherheitsrelevanten Daten vorliegende Störung zu beseitigen und die erste Netzwerkverbindung zwischen dem ersten und zweiten Netzwerkteilnehmer wieder störungsfrei herzustellen, ohne dass das System dafür abgeschaltet werden muss.

Zweckmäßigerweise wird gemäß dem erfindungsgemäßen Verfahren für das Übertragen dieser sicherheitsrelevanten Daten zwischen dem wenigstens ersten und zweiten Netzwerkteilnehmer ausschließlich den für dieses Übertragen vorgesehenen Netzwerkteilnehmern eine Zugriffsberechtigung für das jeweilige virtuelle Netzwerk erteilt. Eine Erteilung der Zugriffsberechtigung kann dabei insbesondere durch eine Kontrollinstanz, insbesondere eine Kontrollinstanz des zugrundeliegenden Systems, oder durch einen dieser wenigstens ersten und zweiten Netzwerkteilnehmer erfolgen. Dadurch wird gewährleistet, dass ausschließlich die Netzwerkteilnehmer, die für den Austausch der sicherheitsrelevanten Daten autorisiert bzw. berechtigt sind, an dem Übertragen dieser sicherheitsrelevanten Daten teilnehmen können.

Zudem wird gemäß einer Weiterentwicklung des erfindungsgemäßen Verfahrens zumindest das erste virtuelle Netzwerk lediglich für den Fall eingerichtet, dass sicherheitsrelevante Daten zwischen dem wenigstens ersten und zweiten Netzwerkteilnehmer aus der Mehrzahl von Netzwerkteilnehmern übertragen werden sollen. Somit sind Störungen und Fehler innerhalb des ersten virtuellen Netzwerks und/oder Angriffe, insbesondere manipulativer Natur, auf das erste virtuelle Netzwerk auf die Zeitdauer der tatsächlichen Übertagung von sicherheitsrelevanten Daten beschränkt.

Das erfindungsgemäße Verfahren kann vorzugsweise zusätzlich zu dem Schritt des Übertragens der sicherheitsrelevanten Daten zwischen dem ersten und dem zweiten Netzwerkteilnehmer über die erste Netzwerkverbindung des ersten virtuellen Netzwerks auch den Schritt eines Übertragens dieser sicherheitsrelevanten Daten zwischen dem ersten und dem zweiten Netzwerkteilnehmer über die zweite Netzwerkverbindung des zweiten virtuellen Netzwerks in dem physikalischen Netzwerk umfassen. Dies ist insbesondere dann von Vorteil, wenn ein schnelles Umschalten auf die zweite Netzwerkverbindung erfolgen soll, beispielsweise um die Kommunikationsverbindung zwischen dem ersten und zweiten Netzwerkteilnehmer nahezu unterbrechungsfrei, d.h. nahezu ohne zeitliche Verzögerungen beim Umschalten auf die zweite Netzwerkverbindung zum Übertragen der sicherheitsrelevanten Daten, aufrecht zu erhalten. In Anwendungsfällen, in welchen ein unterbrechungsfreies Aufrechterhalten der Kommunikationsverbindung zwischen erstem und zweitem Netzwerkteilnehmer

und somit eine hohe Verfügbarkeit des zugrundeliegenden Systems höchste Priorität hat, sind die erste Netzwerkverbindung des ersten virtuellen Netzwerks und die zweite Netzwerkverbindung des zweiten virtuellen Netzwerks daher zweckmäßig redundant ausgeführt. In dem vorbeschriebenen Fall ist es vorteilhaft, wenn das zweite virtuelle Netzwerk lediglich für den Fall eingerichtet wird, dass sicherheitsrelevante Daten zwischen dem wenigstens ersten und zweiten Netzwerkteilnehmer aus der Mehrzahl von Netzwerkteilnehmern übertragen werden sollen, wie bereits im Hinblick auf das erste virtuelle Netzwerk beschrieben.

Alternativ zu dem vorbeschriebenen Fall kann gemäß dem erfindungsgemäßen Verfahren jedoch auch vorgesehen sein, dass die zweite Netzwerkverbindung erst im Falle des Feststellens eines nicht störungsfreien Übertragens der sicherheitsrelevanten Daten über die erste Netzwerkverbindung aufgebaut wird. In diesem Fall sind die erste Netzwerkverbindung des ersten virtuellen Netzwerks und die zweite Netzwerkverbindung des zweiten virtuellen Netzwerks somit nicht redundant ausgeführt. Vielmehr erfolgt der Aufbau der zweiten Netzwerkverbindung zwischen dem ersten und zweiten Netzwerkteilnehmer erst möglichst unmittelbar nach dem Feststellen einer Störung bei dem Übertragen der sicherheitsrelevanten Daten über die erste Netzwerkverbindung. Dies ist insbesondere dann von Vorteil, wenn eine möglichst geringe Kapazitätsauslastung der jeweiligen virtuellen Netzwerkverbindungen in dem physikalischen Netzwerk erwünscht ist und dieser Aspekt höher priorisiert ist als ein schnelles Umschalten auf die zweite Netzwerkverbindung bzw. als ein nahezu unterbrechungsfreies Übertragen der sicherheitsrelevanten Daten zwischen dem ersten und zweiten Netzwerkteilnehmer. Sollen beispielsweise sehr große Datenmengen von sicherheitsrelevanten Daten zwischen dem ersten und dem zweiten Netzwerkteilnehmer übertragen werden, kann es sich als vorteilhaft erweisen, wenn ein Übertragen dieser sehr großen Datenmengen an sicherheitsrelevanten Daten nicht gleichzeitig über sowohl die erste Netzwerkverbindung als auch in redundanter Weise über die zweite Netzwerkverbindung erfolgt. Auch wenn die zweite Netzwerkverbindung zwischen erstem und zweitem Netzwerkteilnehmer noch nicht aufgebaut ist, kann das zweite virtuelle Netzwerk dennoch bereits eingerichtet worden sein, damit für den Fall einer festgestellten Störung der Datenübertragung über die erste Netzwerkverbindung möglichst unterbrechungsfrei die zweite Netzwerkverbindung aufgebaut werden kann.

Unabhängig davon, wann die zweite Netzwerkverbindung des zweiten virtuellen Netzwerks zwischen dem ersten und dem zweiten Netzwerkteilnehmer letztendlich aufgebaut wird, wird nach dem Umschalten auf die zweite Netzwerkverbindung das Übertragen der sicherheitsrelevanten Daten über die zweite Netzwerkverbindung fortgesetzt, vorzugsweise indem mit neuen sicherheitsrelevanten Daten gestartet wird oder zunächst eine bestimmte, insbesondere vorgebbare Anzahl von über die erste Netzwerkverbindung bereits übertragenen Daten erneut über die zweite Netzwerkverbindung übertragen wird.

Ferner kann gemäß dem erfindungsgemäßen Verfahren vorgesehen sein, dass im Falle des Feststellens eines nicht störungsfreien Übertragens der sicherheitsrelevanten Daten ein Reaktionssignal an eine mit dem physikalischen Netzwerk verbundene zentrale Einheit ausgesandt wird. Die zentrale Einheit kann beispielsweise basierend auf dem Reaktionssignal eine Ferndiagnose der jeweils vorliegenden Störung und/oder eine Fernwartung durchführen. Ferner kann die zentrale Einheit beispielsweise Aktualisierungen innerhalb des ersten und/oder zweiten Netzwerkteilnehmers durchführen oder auch einen erneuten Aufbau der ersten Netzwerkverbindung zwischen dem ersten und dem zweiten Netzwerkteilnehmer veranlassen. Von der zentralen Einheit empfangene oder erfasste Diagnosedaten bzgl. der vorliegenden Störung bei dem Übertragen der sicherheitsrelevanten Daten können z.B. in einer Cloud gesammelt werden, wobei u.a. bei Verletzung einer vorab festgelegten Ausfallstatistik z.B. ein außer-Betrieb-Setzen des ersten und/oder zweiten Netzwerkteilnehmers erfolgen kann.

Gemäß einer Weiterentwicklung des Verfahrens kann vorgesehen sein, dass das Überprüfen in Bezug auf das störungsfreie Übertragen der sicherheitsrelevanten Daten von wenigstens einem der bei diesem Übertragen beteiligten Netzwerkteilnehmer durchgeführt wird, wobei im Falle des Feststellens eines nicht störungsfreien Übertragens der sicherheitsrelevanten Daten das Umschalten auf die zweite Netzwerkverbindung von dem feststellenden, insbesondere von dem zuerst feststellenden, Netzwerkteilnehmer initiiert wird. Zweckmäßig erfolgt ein solches Überprüfen von dem jeweils die sicherheitsrelevanten Daten empfangenden bzw. für

den Empfang der sicherheitsrelevanten Daten vorgesehenen Netzwerkteilnehmer, sodass dieser das Umschalten auf die zweite Netzwerkverbindung einleitet.

Für das erste virtuelle Netzwerk und für das zweite virtuelle Netzwerk kann dasselbe virtuelle Netzwerk verwendet werden oder es können zwei unterschiedliche virtuelle Netzwerke verwendet werden.

Zudem kann das erfindungsgemäße Verfahren den Schritt umfassen, dass parallel zum Übertragen der sicherheitsrelevanten Daten über die erste und/oder zweite Netzwerkverbindung diese oder auch weitere sicherheitsrelevante Daten zwischen einem der ersten und zweiten Netzwerkteilnehmer und einem dritten Netzwerkteilnehmer über eine weitere Netzwerkverbindung eines virtuellen Netzwerks in dem physikalischen Netzwerk übertragen werden. Grundsätzlich kann ein Netzwerkteilnehmer somit mehrere Verbindungen in gleichen oder auch unterschiedlichen virtuellen Netzwerken nutzen.

Für die weitere Netzwerkverbindung des virtuellen Netzwerks in dem physikalischen Netzwerk kann insbesondere das erste virtuelle Netzwerk oder das zweite virtuelle Netzwerk oder ein weiteres virtuelles Netzwerk verwendet werden.

Neben dem zuvor beschriebenen Verfahren umfasst die vorliegende Erfindung ferner ein System zum Durchführen dieses Verfahrens. Das System weist ein physikalisches Netzwerk für industrielle Steuerungen mit einer Mehrzahl von Netzwerkteilnehmern auf, wobei wenigstens ein erster und zweiter Netzwerkteilnehmer aus der Mehrzahl von Netzwerkteilnehmern eingerichtet sind, sicherheitsrelevante Daten zu übertragen. Das System ist zum Übertragen dieser sicherheitsrelevanten Daten zwischen dem ersten und zweiten Netzwerkteilnehmer zumindest über eine erste Netzwerkverbindung eines ersten virtuellen Netzwerks in dem physikalischen Netzwerk eingerichtet. Ferner besitzt das System eine Diagnoseeinheit, und zwar zum Überprüfen, ob das Übertragen dieser sicherheitsrelevanten Daten über die erste Netzwerkverbindung störungsfrei erfolgt. Weiterhin ist das System eingerichtet, im Falle eines Feststellens eines nicht störungsfreien Übertragens über die erste Netzwerkverbindung auf eine zweite, von der

ersten verschiedenen Netzwerkverbindung eines zweiten virtuellen Netzwerks in dem physikalischen Netzwerk umzuschalten.

Weitere Vorteile, Merkmale und Anwendungsmöglichkeiten der vorliegenden Erfindung werden anhand der folgenden Beschreibung von Ausführungsformen davon sowie der dazugehörigen Figuren deutlich. Es zeigen:

Figur 1: eine schematische Ablaufskizze des erfindungsgemäßen Verfahrens gemäß einer ersten Ausführungsform,

Figur 2: eine erste Ausführungsform eines erfindungsgemäßen Systems zum Durchführen des erfindungsgemäßen Verfahrens,

Figur 3: eine zweite Ausführungsform eines erfindungsgemäßen Systems zum Durchführen des erfindungsgemäßen Verfahrens.

Figur 1 veranschaulicht den Ablauf des erfindungsgemäßen Verfahrens zum Übertragen von Daten über ein physikalisches Netzwerk 2 für industrielle Steuerungen anhand eines ersten Ausführungsbeispiels. Das in Figur 1 beispielhaft dargestellte physikalische Netzwerk 2, welches ein privates oder ein öffentliches Netz wie z.B. das Internet sein kann, umfasst eine Mehrzahl von Netzwerkteilnehmern, wobei der Übersichtlichkeit halber lediglich die Netzwerkteilnehmer 10, 14, 18 gezeigt sind, zwischen welchen sicherheitsrelevante Daten 3 übertragen werden sollen. Weitere vom physikalischen Netzwerk 2 umfasste Netzwerkteilnehmer sind beispielsweise mit Bezugszeichen 12 und 16 in den Ausführungsformen eines erfindungsgemäßen Systems gemäß Figuren 2 und 3 zu sehen, wobei zwischen den Netzwerkteilnehmern 12 und 16 zwar auch Daten, aber keine sicherheitsrelevanten Daten ausgetauscht werden. Im Rahmen des erfindungsgemäßen Verfahrens ist vorgesehen, dass zumindest zwischen einem ersten Netzwerkteilnehmer 10 und einem zweiten Netzwerkteilnehmer 14 aus der vom physikalischen Netzwerk 2 umfassten Mehrzahl von Netzwerkteilnehmern 10, 12, 14, 16, 18 sicherheitsrelevante Daten 3 übertragen werden sollen, wie in Figuren 1-3 gezeigt.

Gemäß dem Blockdiagramm in Figur 1 umfasst das Verfahren den Schritt des Übertragens dieser sicherheitsrelevanten Daten 3 zwischen dem ersten Netzwerkteilnehmer 10 und dem zweiten Netzwerkteilnehmer 14 zumindest über eine erste Netzwerkverbindung 5 eines ersten virtuellen Netzwerks 4 in dem physikalischen Netzwerk 2. Im dargestellten Fall erfolgt beispielhaft zusätzlich zu diesem Übertragen der sicherheitsrelevanten Daten 3 über die erste Netzwerkverbindung 5 des ersten virtuellen Netzwerks 4 auch ein Übertragen dieser sicherheitsrelevanten Daten 3 zwischen dem ersten und dem zweiten Netzwerkteilnehmer 10, 14 über eine zweite Netzwerkverbindung 7 eines zweiten virtuellen Netzwerks 6 in dem physikalischen Netzwerk 2. Diese zweite Netzwerkverbindung 7 ist eine von der ersten Netzwerkverbindung 5 verschiedene Netzwerkverbindung. Die erste und zweite Netzwerkverbindung 5, 7 sind folglich im dargestellten Beispiel redundant ausgeführt. Ebenso werden für das erste virtuelle Netzwerk 4 und für das zweite virtuelle Netzwerk 6 beispielhaft zwei unterschiedliche virtuelle Netzwerke verwendet. In einer weiteren Ausführungsform der vorliegenden Erfindung könnte für das erste virtuelle Netzwerk 4 und für das zweite virtuelle Netzwerk 6 jedoch auch dasselbe virtuelle Netzwerk verwendet werden.

Ferner können diese oder auch weitere sicherheitsrelevanten Daten 3 parallel zum Übertragen der sicherheitsrelevanten Daten 3 über die erste und zweite Netzwerkverbindung 5, 7 auch beispielsweise zwischen dem ersten Netzwerkteilnehmer 10 und einem dritten Netzwerkteilnehmer 18 übertragen werden, und zwar über eine weitere, dritte Netzwerkverbindung 9 eines dritten virtuellen Netzwerks 8 in dem physikalischen Netzwerk, wie in Figur 1 zu sehen. Dies kann insbesondere dadurch erfolgen, dass jede einzelne Netzwerkverbindung 5, 7, 9 über jeweils eine IP-Adresse aufgebaut wird. So können beispielsweise dem ersten Netzwerkteilnehmer 10 drei verschiedene IP-Adressen zugeordnet werden, um über die erste, zweite und dritte Netzwerkverbindung 5, 7, 9 jeweils Daten austauschen zu können. Alternativ ist jedoch auch möglich, jedem einzelnen Netzwerkteilnehmer jeweils eine IP-Adresse zuzuordnen.

Auch wenn in Figur 1 nicht gezeigt, ist im Rahmen des erfindungsgemäßen Verfahrens vorgesehen, dass für das Übertragen der sicherheitsrelevanten Daten 3 zwischen dem

wenigstens ersten und zweiten Netzwerkteilnehmer 10, 14, insbesondere auch dem ersten und dritten Netzwerkteilnehmer 10, 18, ausschließlich den für dieses Übertragen vorgesehenen Netzwerkteilnehmern 10, 14, 18 eine Zugriffsberechtigung für das jeweilige virtuelle Netzwerk 4, 6, 8 erteilt wird. Eine solche Zugriffsberechtigung kann beispielsweise durch eine Kontrollinstanz (nicht in Figur 1 gezeigt) oder durch insbesondere einen der ersten und zweiten Netzwerkteilnehmer 10, 14, aber auch durch den dritten Netzwerkteilnehmer 18 erteilt werden. Dies hat den Vorteil, dass ausschließlich die Netzwerkteilnehmer, die für den Austausch der sicherheitsrelevanten Daten 3 autorisiert bzw. berechtigt sind, an dem Übertragen dieser sicherheitsrelevanten Daten 3 teilnehmen können.

Auch wenn aus Figur 1 nicht ersichtlich, so wird zumindest das erste virtuelle Netzwerk 4, und vorzugsweise auch das zweite virtuelle Netzwerk 6 und/oder das dritte virtuelle Netzwerk 8, lediglich für den Fall eingerichtet, dass sicherheitsrelevante Daten 3 zwischen dem wenigstens ersten und zweiten Netzwerkteilnehmer 10, 14, im gezeigten Beispiel der Figur 1 insbesondere auch zwischen dem ersten und dritten Netzwerkteilnehmer 10, 18, übertragen werden sollen. Dadurch können Störungen bzw. Fehler innerhalb des ersten, zweiten und dritten virtuellen Netzwerks 4, 6, 8 und/oder Angriffe, insbesondere manipulativer Natur, auf das erste, zweite und dritte virtuelle Netzwerk 4, 6, 8 auf die Zeitdauer des tatsächlichen Übertragens von sicherheitsrelevanten Daten 3 beschränkt werden.

Weiterhin umfasst das Verfahren gemäß Figur 1 den Schritt des Überprüfens, ob das Übertragen der sicherheitsrelevanten Daten 3 über die erste Netzwerkverbindung 5 störungsfrei erfolgt. Hierzu können verschiedene Maßnahmen gemäß dem Stand der Technik zur Erkennung von Störungen bzw. Fehlern, insbesondere von Manipulationen, bei der Übertragung von Daten, insbesondere von sicherheitsrelevanten Daten, durchgeführt werden. Beispiele für solche Maßnahmen sind u.a. zyklische Redundanzprüfungen (CRCs) oder auch eine versteckte CRCs für Teilbereiche der zu übertragenden Daten, eine Datenkennzeichnung mit Sende- und Empfangsadresse, eine Kennzeichnung der Datenabfolge mittels Zähler, eine Übertragung von Taktsignalen einer Systemuhr (Clock (CLK)-Signale) und eine Übertragung von Befehlen, die die Verwendung der Daten bestimmen, z.B. spezielle Systemnachrichten. Gemäß Figur 1

kann u.a. vorgesehen sein, die von einem der Netzwerkteilnehmer 10, 14 sowohl über die erste Netzwerkverbindung 5 als auch über die zweite Netzwerkverbindung 7 empfangenen sicherheitsrelevanten Daten 3 auf deren Übereinstimmung miteinander zu überprüfen, wobei infolge einer nicht störungsfreien Übertragung der sicherheitsrelevanten Daten 3 eine fehlende Überstimmung der jeweils über die erste und zweite Netzwerkverbindung 5, 7 empfangenen sicherheitsrelevanten Daten 3 vorliegt. Bei einer redundanten Übertragung von sicherheitsrelevanten Daten 3 zwischen dem ersten und zweiten Netzwerkteilnehmer 10, 14 sowohl über die erste als auch über die zweite Netzwerkverbindung 5,7 können dabei auftretende Störungen bzw. Fehler vorteilhafterweise schnell und sehr gut erkannt werden.

Wird bei dem Überprüfen festgestellt, dass das Übertragen der sicherheitsrelevanten Daten 3 zwischen dem ersten und zweiten Netzwerkteilnehmer 10, 14 über die erste Netzwerkverbindung 5 störungsfrei erfolgt, so wird keinerlei Maßnahme ergriffen, sodass dieses Übertragen ununterbrochen fortgeführt wird. Wird hingegen während des Überprüfens festgestellt, dass das Übertragen der sicherheitsrelevanten Daten 3 zwischen dem ersten und zweiten Netzwerkteilnehmer 10, 14 über die erste Netzwerkverbindung 5 nicht störungsfrei erfolgt, so wird im Rahmen des erfindungsgemäßen Verfahrens der Schritt des Umschaltens auf die zweite Netzwerkverbindung 7 des zweiten virtuellen Netzwerks 6 in dem physikalischen Netzwerk 2 zum Übertragen dieser sicherheitsrelevanten Daten 3 zwischen dem ersten und zweiten Netzwerkteilnehmer 10, 14 durchgeführt. Dies hat den großen Vorteil, dass eine Kommunikations- bzw. Datenverbindung insbesondere zwischen dem ersten und zweiten Netzwerkteilnehmer 10, 14 zumindest für begrenzte Zeit trotz der festgestellten gestörten Datenübertragung über die erste Netzwerkverbindung 5 weiter aufrechterhalten werden kann. Eine Kommunikation bzw. Übertragung von sicherheitsrelevanten Daten 3 insbesondere zwischen dem ersten und zweiten Netzwerteilnehmer 10, 14 muss folglich nicht unterbrochen werden, was zu einer deutlichen Verbesserung bzw. Erhöhung der Verfügbarkeit des entsprechenden zugrundeliegenden Systems führt.

Der Begriff des Umschaltens bedeutet im vorliegenden Beispiel der Figur 1, dass von einem Schaltzustand, in welchem eine redundante Übertragung der

sicherheitsrelevanten Daten 3 zwischen dem ersten und zweiten Netzwerkteilnehmer 10, 14 sowohl über die erste als auch über die zweite Netzwerkverbindung 5, 7 erfolgt, in einen Schaltzustand umgeschaltet wird, in welchem eine Übertragung der sicherheitsrelevanten Daten 3 zwischen dem ersten und zweiten Netzwerkteilnehmer 10, 14 über die zweite Netzwerkverbindung 7, und somit nicht mehr über die erste Netzwerkverbindung 5, erfolgt. Dabei ist jedoch nicht ausgeschlossen, dass diese oder auch weitere sicherheitsrelevanten Daten 3 beispielsweise zwischen dem ersten und dem dritten Netzwerkteilnehmer 10, 18 über eine dritte Netzwerkverbindung 9 eines weiteren, dritten virtuellen Netzwerks 8, wie in Figur 1 gezeigt, oder sogar über eine vierte Netzwerkverbindung (nicht dargestellt) zwischen dem ersten und zweiten Netzwerkteilnehmer 10, 14 übertragen werden. Auch wäre es im Rahmen der Erfindung denkbar, dass ein Übertragen der sicherheitsrelevanten Daten 3 zwischen dem ersten und zweiten Netzwerkteilnehmer 10, 14 zusätzlich noch über eine weitere Netzwerkverbindung eines weiteren virtuellen Netzwerks erfolgt, und zwar vor und/oder nach dem Umschalten auf die zweite Netzwerkverbindung.

Eine gemäß Figur 1 gezeigte redundante Ausführung der ersten und zweiten Netzwerkverbindung 5, 7 ist insbesondere dann von Vorteil, wenn ein schnelles Umschalten auf die zweite Netzwerkverbindung 7 erfolgen soll, beispielsweise um die Kommunikations- bzw. Datenverbindung zwischen dem ersten und zweiten Netzwerkteilnehmer 10, 14 nahezu unterbrechungsfrei, d.h. nahezu ohne zeitliche Verzögerungen beim Umschalten, aufrecht zu erhalten. In solchen Anwendungsfällen wird in der Regel oberste Priorität auf eine hohe Verfügbarkeit des zugrundeliegenden Systems gelegt.

Während des Übertragens der sicherheitsrelevanten Daten 3 über die zweite Netzwerkverbindung 7 kann zudem zweckmäßigerweise versucht werden, die beim Übertragen der sicherheitsrelevanten Daten 3 über die erste Netzwerkverbindung 5 vorliegende Störung zu beseitigen und die erste Netzwerkverbindung 5 zwischen dem ersten und zweiten Netzwerkteilnehmer 10, 14 wieder störungsfrei herzustellen, ohne dass dafür sämtliche Kommunikationsverbindungen zwischen den Netzwerkteilnehmern 10 14, 18, insbesondere dem ersten und zweiten

Netzwerkteilnehmer 10, 14, unterbrochen werden müssen bzw. das entsprechende zugrundeliegende System dafür abgeschaltet werden muss.

Ferner kann im Rahmen des erfindungsgemäßen Verfahrens vorgesehen sein, dass das Überprüfen in Bezug auf das störungsfreie Übertragen der sicherheitsrelevanten Daten 3 zwischen dem ersten und zweiten Netzwerkteilnehmer 10, 14 von wenigstens einem der bei diesem Übertragen beteiligten Netzwerkteilnehmer 10, 14 durchgeführt wird. Im Falle des Feststellens eines nicht störungsfreien Übertragens der sicherheitsrelevanten Daten 3 kann das Umschalten auf die zweite Netzwerkverbindung 7 von dem feststellenden, insbesondere von dem zuerst feststellenden, Netzwerkteilnehmer der ersten und zweiten Netzwerkteilnehmer 10, 14 initiiert werden. Zweckmäßigerweise wird diese Überprüfung von dem jeweils für den Empfang der sicherheitsrelevanten Daten 3 vorgesehenen Netzwerkteilnehmer durchgeführt. In Figuren 2 und 3 ist dies beispielweise der zweite Netzwerkteilnehmer 14, welcher dafür eine Diagnoseeinheit 20 umfasst. Stellt die Diagnoseeinheit 20 ein nicht störungsfreies Übertragen der sicherheitsrelevanten Daten 3 über die erste Netzwerkverbindung 5 fest, so kann sie selbst das Umschalten auf die zweite Netzwerkverbindung 7 veranlassen. Die Diagnoseeinheit 20 kann alternativ auch ein Ergebnis der Überprüfung an eine weitere Einheit, beispielsweise eine Steuereinheit, des zweiten Netzwerkteilnehmers 14 übermitteln, woraufhin diese dann ein entsprechendes Umschalten initiiert.

Das erfindungsgemäße Verfahren kann zudem insbesondere den Schritt umfassen, dass im Falle des Feststellens eines nicht störungsfreien Übertragens der sicherheitsrelevanten Daten 3 über die erste Netzwerkverbindung 5 ein Reaktionssignal an eine mit dem physikalischen Netzwerk 2 verbundene zentrale Einheit ausgesandt wird. Dies ist beispielhaft in Figur 3 skizziert, welche eine zweite Ausführungsform eines erfindungsgemäßen Systems zum Durchführen des erfindungsgemäßen Verfahrens darstellt. So zeigt Figur 3 eine zentrale Einheit 22, welche beispielhaft mit dem zweiten Netzwerkteilnehmer 14, insbesondere der von dem zweiten Netzwerkteilnehmer 14 umfassten Diagnoseeinheit 20, verbunden ist.

Ferner zeigen die Figuren 2 und 3 eine erste bzw. zweite Ausführungsform eines erfindungsgemäßen Systems 1 zum Durchführen des erfindungsgemäßen Verfahrens.

Wie in den Figuren 2 und 3 gezeigt, weist das System 1 ein physikalisches Netzwerk 2 für industrielle Steuerungen mit einer Mehrzahl von Netzwerkteilnehmern 10, 12, 14, 16, 18 auf. Wenigstens ein erster und zweiter Netzwerkteilnehmer 10, 14 aus der Mehrzahl von Netzwerkteilnehmern 10, 12, 14, 16, 18 des Systems 1, in den gezeigten Ausführungsformen beispielhaft ein erster, zweiter und dritter Netzwerkteilnehmer 10, 14, 18, sind dazu eingerichtet, sicherheitsrelevante Daten 3 zu übertragen. Zwischen den in Figuren 2 und 3 mit Bezugszeichen 12 und 16 gekennzeichneten Netzwerkteilnehmern werden auch Daten übertragen, welche aber keine sicherheitsrelevanten Daten sind.

Das System 1 ist gemäß Figuren 2 und 3 zum Übertragen dieser sicherheitsrelevanten Daten 3 zwischen dem ersten und zweiten Netzwerkteilnehmer 10, 14 zumindest über eine erste Netzwerkverbindung 5 eines ersten virtuellen Netzwerks 4 in dem physikalischen Netzwerk 2 eingerichtet. Ferner ist das gezeigte System 1 beispielhaft dazu eingerichtet, diese und/oder weitere sicherheitsrelevante Daten 3 ferner zwischen dem ersten Netzwerkteilnehmer 10 und einem dritten Netzwerkteilnehmer 18 zu übertragen, und zwar über eine dritte Netzwerkverbindung 9 eines weiteren, dritten virtuellen Netzwerks 8.

Darüber hinaus besitzt das System 1 gemäß Figuren 2 und 3 eine Diagnoseeinheit 20, und zwar zum Überprüfen, ob das Übertragen dieser sicherheitsrelevanten Daten 3 zwischen dem ersten und zweiten Netzwerkteilnehmer 10, 14 über die erste Netzwerkverbindung 5 störungsfrei erfolgt. Wie bereits bezüglich des in Figur 1 skizzierten Verfahrensablaufs beschrieben, kann diese Diagnoseeinheit 20 beispielsweise von einem der ersten und zweiten Netzwerkteilnehmer 10, 14, insbesondere dem für den Empfang der sicherheitsrelevanten Daten 3 vorgesehenen Netzwerkteilnehmer, umfasst sein. In den gezeigten Ausführungsformen der Figuren 2 und 3 umfasst der zweite Netzwerkteilnehmer 14 eine solche Diagnoseeinheit 20, welche zweckmäßig mit allen Eingängen des zweiten Netzwerkteilnehmers 14 verbunden ist.

Weiterhin ist das System 1 eingerichtet, im Falle eines Feststellens eines nicht störungsfreien Übertragens über die erste Netzwerkverbindung 5 von zumindest dieser

ersten Netzwerkverbindung 5 auf eine zweite, von der ersten verschiedenen Netzwerkverbindung 7 eines zweiten virtuellen Netzwerks 6 in dem physikalischen Netzwerk 2 umzuschalten. Im Gegensatz zu Figur 1 sind die erste und die zweite Netzwerkverbindung 5, 7 in Figuren 2 und 3 nicht redundant ausgeführt. Vielmehr erfolgt ein Übertragen der sicherheitsrelevanten Daten 3 zwischen dem ersten und zweiten Netzwerkteilnehmer 10, 14 in Figuren 2 und 3 zunächst nur über die erste Netzwerkverbindung 5 des ersten virtuellen Netzwerks 4. Somit sieht das von dem System 1 durchzuführende Verfahren im Gegensatz zu Figur 1 zweckmäßigerweise vor, dass die zweite Netzwerkverbindung 7 erst im Falle des Feststellens eines nicht störungsfreien Übertragens der sicherheitsrelevanten Daten 3 über die erste Netzwerkverbindung 5 aufgebaut wird. Dies ist in Figuren 2 und 3 dadurch verdeutlicht, dass die zweite Netzwerkverbindung 7 gestrichelt dargestellt ist.

Der Begriff des Umschaltens auf die zweite Netzwerkverbindung 7 beschreibt im vorliegenden Beispiel der Figuren 2 und 3 demzufolge, dass von einem Schaltzustand, in welchem ein Übertragen der sicherheitsrelevanten Daten 3 zwischen dem ersten und zweiten Netzwerkteilnehmer 10, 14 ausschließlich über die erste Netzwerkverbindung 5 erfolgt, in einen Schaltzustand umgeschaltet wird, in welchem ein Übertragen der sicherheitsrelevanten Daten 3 zwischen dem ersten und zweiten Netzwerkteilnehmer 10, 14 ausschließlich über die zweite Netzwerkverbindung 7 erfolgt. Dabei ist jedoch nicht ausgeschlossen, dass diese oder auch weitere sicherheitsrelevanten Daten 3 beispielsweise zwischen dem ersten und dem dritten Netzwerkteilnehmer 10, 18 über eine dritte Netzwerkverbindung 9 eines weiteren, dritten virtuellen Netzwerks 8, wie in Figuren 2 und 3 gezeigt, übertragen werden.

In weiteren, nicht gezeigten Ausführungsformen der Erfindung ist auch möglich, dass die sicherheitsrelevanten Daten 3 insbesondere nach dem Umschalten auf die zweite Netzwerkverbindung 7 zwischen dem ersten und zweiten Netzwerkteilnehmer 10, 14 in Abwandlung zu Figuren 2 und 3 zusätzlich über eine weitere, vierte Netzwerkverbindung übertragen werden. Ebenso können die sicherheitsrelevanten Daten 3 ergänzend oder alternativ dazu auch bereits vor dem Umschalten auf die zweite Netzwerkverbindung 7 zwischen dem ersten und zweiten Netzwerkteilnehmer 10, 14

zusätzlich zur ersten Netzwerkverbindung 5 über beispielsweise die weitere, vierte Netzwerkverbindung übertragen werden.

Ein solches Umschalten von der ersten Netzwerkverbindung 5 auf die zweite Netzwerkverbindung 7, wie hinsichtlich Figuren 2 und 3 beschrieben, ist insbesondere dann von Vorteil, wenn eine möglichst geringe Kapazitätsauslastung der jeweiligen Netzwerkverbindung(en) in dem physikalischen Netzwerk 2 erwünscht oder erforderlich ist und diese Anforderung wichtiger bzw. höher priorisiert ist als ein schnelles Umschalten auf die zweite Netzwerkverbindung 7 bzw. als ein nahezu unterbrechungsfreies Übertragen der sicherheitsrelevanten Daten 3. Dies ist beispielsweise der Fall, wenn sehr große Datenmengen von sicherheitsrelevanten Daten 3 zwischen dem ersten und dem zweiten Netzwerkteilnehmer 10, 14 übertragen werden sollen. In einem derartigen Fall kann es sich als vorteilhaft erweisen, wenn ein Übertragen dieser sehr großen Datenmengen von sicherheitsrelevanten Daten 3 nicht gleichzeitig über sowohl die erste Netzwerkverbindung 5 als auch in redundanter Weise über die zweite Netzwerkverbindung 7 erfolgt.

Während in Figur 2 für das erste virtuelle Netzwerk 4 und für das zweite virtuelle Netzwerk 6 zwei unterschiedliche virtuelle Netzwerke verwendet werden, wird hingegen in Figur 3 beispielhaft für das erste virtuelle Netzwerk 4 und für das zweite virtuelle Netzwerk 6 dasselbe virtuelle Netzwerk verwendet.

Wie bereits hinsichtlich Figur 1 beschrieben, kann die Diagnoseeinheit 20 zusätzlich zum Schritt des Überprüfens ferner zweckmäßigerweise eingerichtet sein, im Falle eines festgestellten nicht störungsfreien Übertragens der sicherheitsrelevanten Daten 3 über die erste Netzwerkverbindung 5 das Umschalten auf die zweite Netzwerkverbindung 7 zu initiieren. Die Diagnoseeinheit 20 kann alternativ auch ein Ergebnis ihrer Überprüfung an eine weitere Einheit, beispielsweise eine Steuereinheit (nicht dargestellt), des zweiten Netzwerkteilnehmers 14 übermitteln, woraufhin diese dann ein entsprechendes Umschalten initiiert.

Im Falle des Feststellens eines nicht störungsfreien Übertragens der sicherheitsrelevanten Daten 3 zwischen dem ersten und zweiten Netzwerkteilnehmer 10,

14 über die erste Netzwerkverbindung 5 kann das System 1 zum Durchführen des erfindungsgemäßen Verfahrens dazu eingerichtet sein, ein Reaktionssignal an eine mit dem physikalischen Netzwerk 2 verbundene zentrale Einheit 22 auszusenden, wie in Figur 3 beispielhaft gezeigt. Die zentrale Einheit 22 kann von dem System 1 umfasst sein, kann aber auch zum Austausch von Informationen mit diesem verbunden sein. Insbesondere ist die zentrale Einheit 22 gemäß Figur 3 mit der Diagnoseeinheit 20 des zweiten Netzwerkteilnehmers 14 verbunden, sodass die Diagnoseeinheit 20 beispielsweise ein Ergebnis ihrer Überprüfung an die zentrale Einheit 22 übermitteln kann. Die zentrale Einheit 22 kann beispielsweise basierend auf dem empfangenen Reaktionssignal eine Ferndiagnose der jeweils vorliegenden Störung und/oder eine Fernwartung durchführen. Ferner kann die zentrale Einheit 22 beispielsweise Aktualisierungen innerhalb des ersten und/oder zweiten Netzwerkteilnehmers 10, 14 durchführen oder auch einen erneuten Aufbau der ersten Netzwerkverbindung 5 zwischen dem ersten und dem zweiten Netzwerkteilnehmer 10, 14 veranlassen. An die zentrale Einheit 22 übermittelte Diagnosedaten bzgl. der vorliegenden Störung bei dem Übertragen der sicherheitsrelevanten Daten 3 können z.B. in einer Cloud gesammelt werden, wobei u.a. bei Verletzung einer vorab festgelegten Ausfallstatistik z.B. ein außer-Betrieb-Setzen des ersten und/oder zweiten Netzwerkteilnehmers 10, 14 erfolgen kann.

Zusammenfassend schlägt die vorliegende Erfindung ein Verfahren sowie ein System zu dessen Durchführung vor, mit welchem nach einem Feststellen eines nicht störungsfreien Übertragens von sicherheitsrelevanten Daten zwischen einem ersten und zweiten Netzwerkteilnehmer über eine erste Netzwerkverbindung eines ersten virtuellen Netzwerks in einem physikalischen Netzwerk auf eine von der ersten verschiedene zweite Netzwerkverbindung eines zweiten virtuellen Netzwerks in dem physikalischen Netzwerk zum Übertragen dieser sicherheitsrelevanten Daten umgeschaltet werden kann. Damit verbundene Vorteile sind insbesondere eine deutlich verbesserte bzw. erhöhte Verfügbarkeit des Systems, da die Datenverbindung zwischen erstem und zweitem Netzwerkteilnehmer weiterhin zumindest für begrenzte Zeit aufrechterhalten werden kann. Die im Rahmen der Erfindung gefundene Lösung ist ohne großen Kostenaufwand umsetzbar und kann auch bei großen Datenmengen von sicherheitsrelevanten Daten eingesetzt werden.

Bezugszeichenliste

2	physikalisches Netzwerk
3	sicherheitsrelevante Daten
4	erstes virtuelles Netzwerk
5	erste Netzwerkverbindung
6	zweites virtuelles Netzwerk
7	zweite Netzwerkverbindung
8	virtuelles Netzwerk
9	weitere Netzwerkverbindung
10	erster Netzwerkteilnehmer
12	Netzwerkteilnehmer
14	zweiter Netzwerkteilnehmer
16	Netzwerkteilnehmer
18	dritter Netzwerkteilnehmer
20	Diagnoseeinheit
22	zentrale Einheit

Patentansprüche

1. Verfahren zum Übertragen von Daten über ein physikalisches Netzwerk (2) für industrielle Steuerungen, welches eine Mehrzahl von Netzwerkteilnehmern (10, 12, 14, 16, 18) umfasst, wobei für den Fall, dass sicherheitsrelevante Daten (3) zwischen wenigstens einem ersten und zweiten Netzwerkteilnehmer (10, 14, 18) aus der Mehrzahl von Netzwerkteilnehmern (10, 12, 14, 16, 18) übertragen werden sollen, das Verfahren folgende Schritte aufweist:

- Übertragen dieser sicherheitsrelevanten Daten (3) zwischen dem ersten und dem zweiten Netzwerkteilnehmer (10, 14) zumindest über eine erste Netzwerkverbindung (5) eines ersten virtuellen Netzwerks (4) in dem physikalischen Netzwerk (2),
- Überprüfen, ob das Übertragen der sicherheitsrelevanten Daten (3) über die erste Netzwerkverbindung (5) störungsfrei erfolgt;
- im Falle eines Feststellens eines nicht störungsfreien Übertragens über die erste Netzwerkverbindung (5) Umschalten auf eine zweite, von der ersten verschiedenen Netzwerkverbindung (7) eines zweiten virtuellen Netzwerks (6) in dem physikalischen Netzwerk (2) zum Übertragen dieser sicherheitsrelevanten Daten (3) zwischen dem ersten und zweiten Netzwerkteilnehmer (10, 14).

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet,

- dass für das Übertragen dieser sicherheitsrelevanten Daten (3) zwischen dem wenigstens ersten und zweiten Netzwerkteilnehmer (10, 14, 18) ausschließlich den für dieses Übertragen vorgesehenen Netzwerkteilnehmern (10, 14, 18) eine Zugriffsberechtigung für das jeweilige virtuelle Netzwerk (4, 6, 8) erteilt wird, insbesondere durch eine Kontrollinstanz oder durch einen dieser wenigstens ersten und zweiten Netzwerkteilnehmer (10, 14, 18) erteilt wird,

und/oder,

- dass zumindest das erste virtuelle Netzwerk (4) lediglich für den Fall, dass sicherheitsrelevante Daten (3) zwischen dem wenigstens ersten und zweiten Netzwerkteilnehmer (10, 14, 18) aus der Mehrzahl von Netzwerkteilnehmern (10, 12, 14, 16, 18) übertragen werden sollen, eingerichtet wird.

3. Verfahren nach Anspruch 1, oder 2, dadurch gekennzeichnet, dass zusätzlich zu dem Schritt des Übertragens der sicherheitsrelevanten Daten (3) zwischen dem ersten und dem zweiten Netzwerkteilnehmer (10, 14) über die erste Netzwerkverbindung (5) des ersten virtuellen Netzwerks (4) auch ein Übertragen dieser sicherheitsrelevanten Daten (3) zwischen dem ersten und dem zweiten Netzwerkteilnehmer (10, 14) über die zweite Netzwerkverbindung (7) des zweiten virtuellen Netzwerks (6) in dem physikalischen Netzwerk (2) erfolgt, wobei vorzugsweise das zweite virtuelle Netzwerk (6) lediglich für den Fall, dass sicherheitsrelevante Daten (3) zwischen dem wenigstens ersten und zweiten Netzwerkteilnehmer (10, 14, 18) aus der Mehrzahl von Netzwerkteilnehmern (10, 12, 14, 16, 18) übertragen werden sollen, eingerichtet wird.

4. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass die zweite Netzwerkverbindung (7) erst im Falle des Feststellens eines nicht störungsfreien Übertragens der sicherheitsrelevanten Daten (3) über die erste Netzwerkverbindung (5) aufgebaut wird.

5. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass im Falle des Feststellens eines nicht störungsfreien Übertragens der sicherheitsrelevanten Daten (3) ein Reaktionssignal an eine mit dem physikalischen Netzwerk (2) verbundene zentrale Einheit (22) ausgesandt wird.

6. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass das Überprüfen in Bezug auf das störungsfreie Übertragen der sicherheitsrelevanten Daten (3) von wenigstens einem der bei diesem Übertragen beteiligten Netzwerkteilnehmer (10, 14) durchgeführt wird, wobei im Falle des Feststellens eines nicht störungsfreien Übertragens der sicherheitsrelevanten Daten (3) das Umschalten auf die zweite Netzwerkverbindung (7) von dem feststellenden, insbesondere von dem zuerst feststellenden, Netzwerkteilnehmer (10, 14) initiiert wird.

7. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass für das erste virtuelle Netzwerk (4) und für das zweite virtuelle Netzwerk (6) dasselbe virtuelle Netzwerk verwendet wird oder zwei unterschiedliche virtuelle Netzwerke verwendet werden.

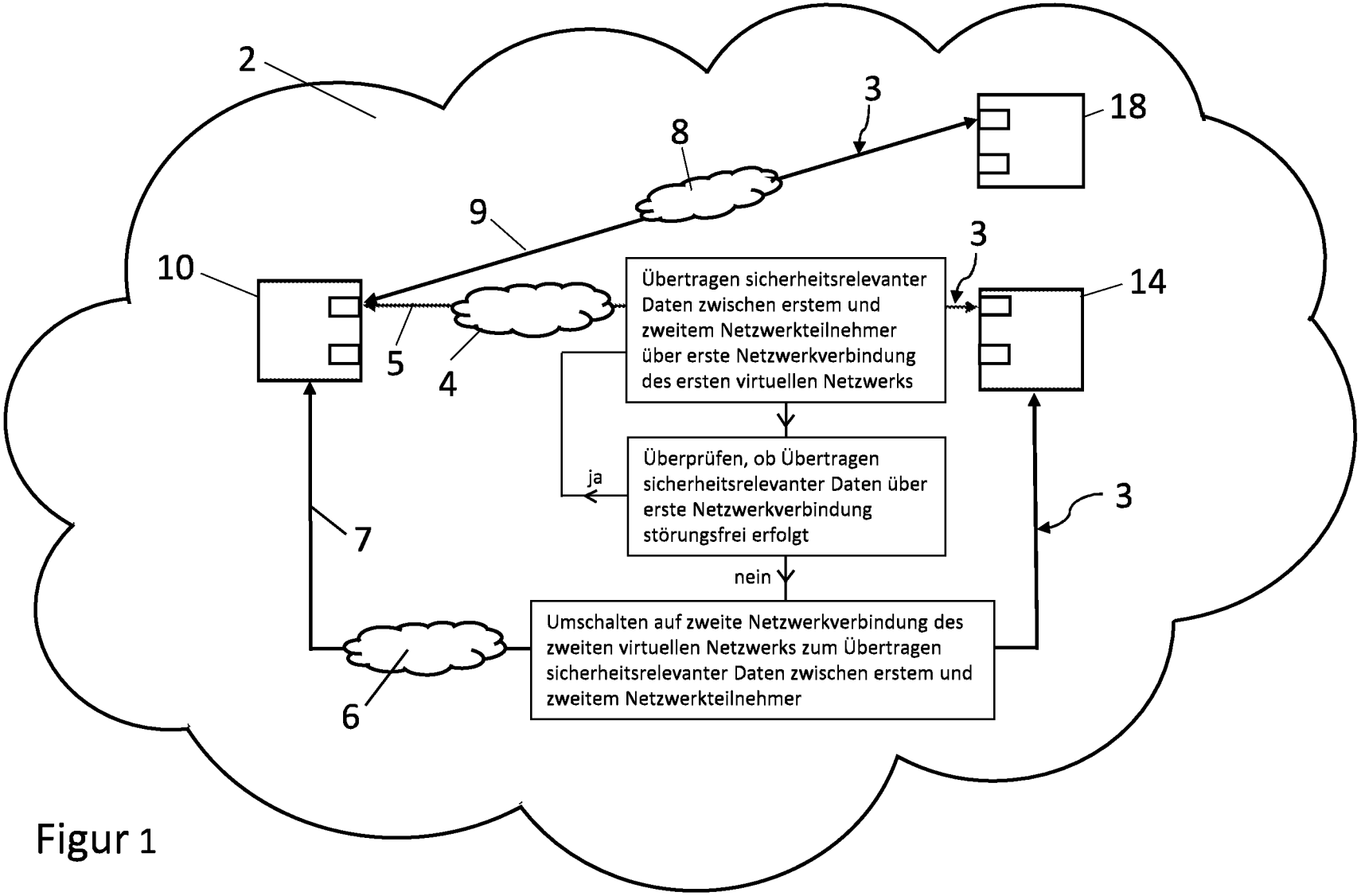
8. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass parallel zum Übertragen der sicherheitsrelevanten Daten (3) über die erste und/oder zweite Netzwerkverbindung (5, 7) diese oder auch weitere sicherheitsrelevante Daten (3) zwischen einem der ersten und zweiten Netzwerkteilnehmer (10, 14) und einem dritten Netzwerkteilnehmer (18) über eine weitere Netzwerkverbindung (9) eines virtuellen Netzwerks (4, 6, 8) in dem physikalischen Netzwerk (2) übertragen werden.

9. Verfahren nach dem vorhergehenden Anspruch, dadurch gekennzeichnet, das für die weitere Netzwerkverbindung (9) des virtuellen Netzwerks (4, 6, 8) in dem physikalischen Netzwerk (2) das erste virtuelle Netzwerk (4) oder das zweite virtuelle Netzwerk (6) oder ein weiteres virtuelles Netzwerk (8) verwendet wird.

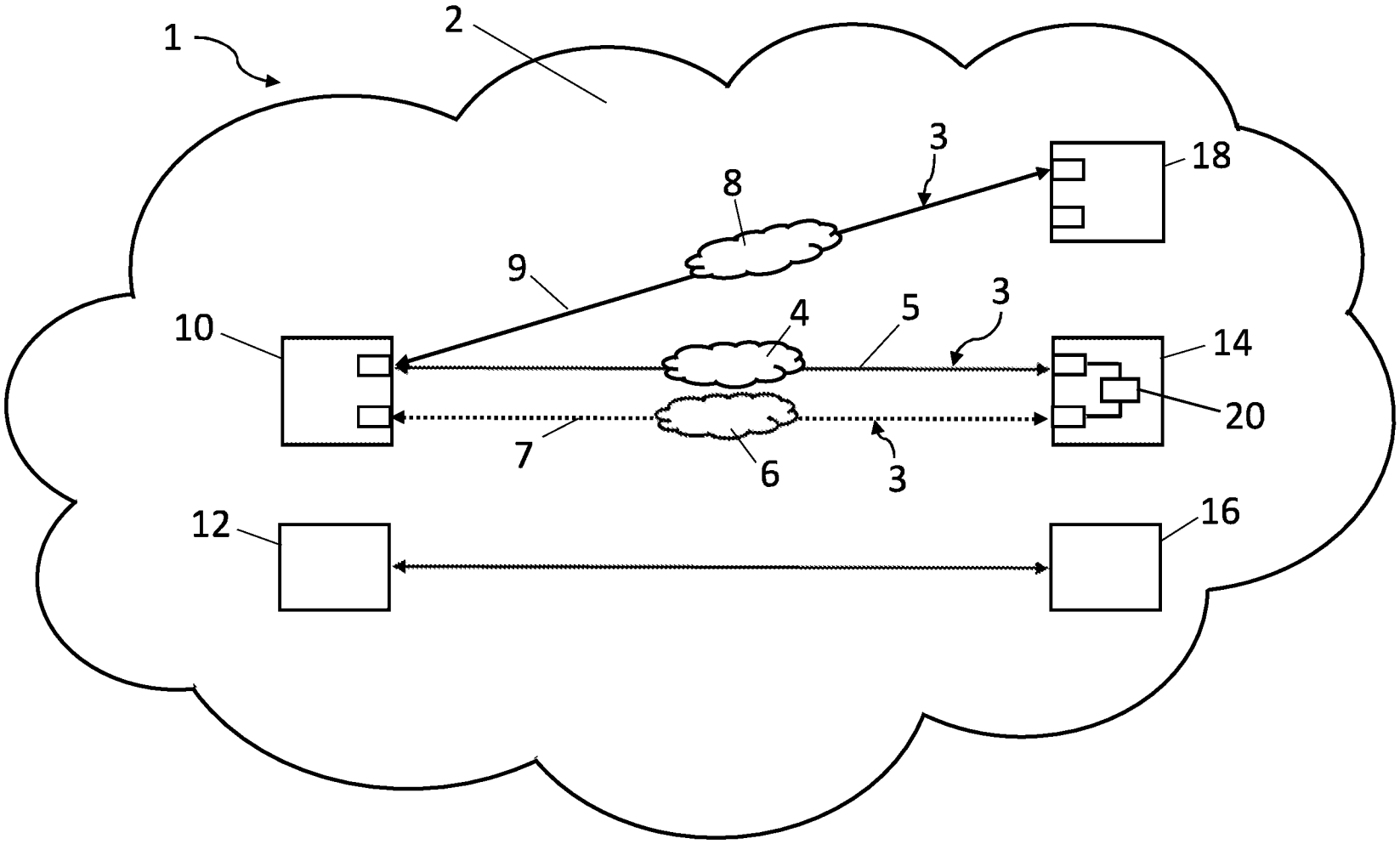
10. System (1) zum Durchführen des Verfahrens nach einem der Ansprüche 1 bis 9, wobei das System (1) ein physikalisches Netzwerk (2) für industrielle Steuerungen mit einer Mehrzahl von Netzwerkteilnehmern (10, 12, 14, 16, 18) umfasst, wobei wenigstens ein erster und zweiter Netzwerkteilnehmer (10, 14, 18) aus der Mehrzahl von Netzwerkteilnehmern (10, 12, 14, 16, 18) eingerichtet sind, sicherheitsrelevante Daten (3) zu übertragen, und wobei das System (1)

- eingerichtet ist, zum Übertragen dieser sicherheitsrelevanten Daten (3) zwischen dem ersten und zweiten Netzwerkteilnehmer (10, 14) zumindest über eine erste Netzwerkverbindung (5) eines ersten virtuellen Netzwerks (4) in dem physikalischen Netzwerk (2),
    - eine Diagnoseeinheit (20) besitzt, und zwar zum Überprüfen, ob das Übertragen dieser sicherheitsrelevanten Daten (3) über die erste Netzwerkverbindung (5) störungsfrei erfolgt, und

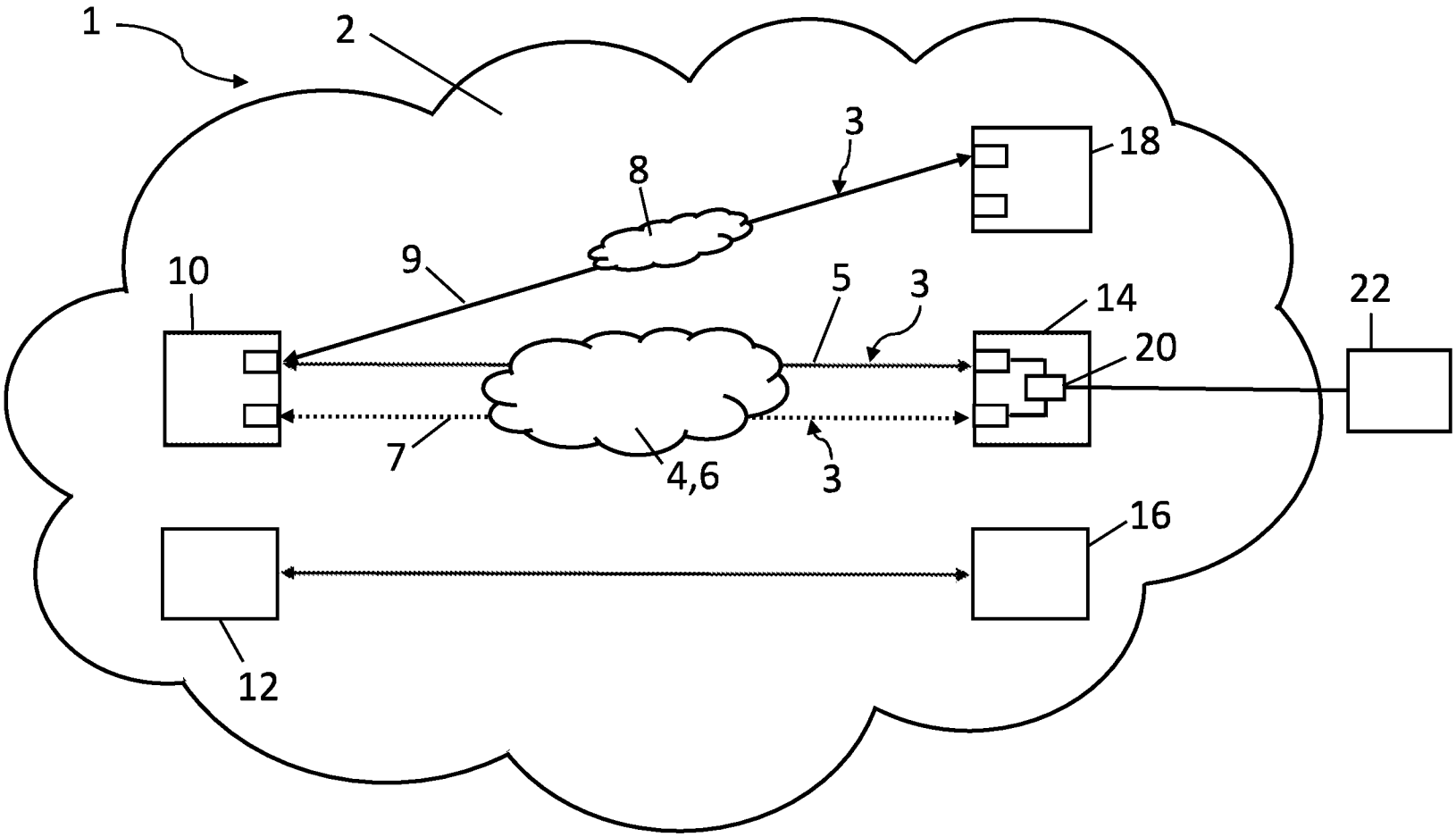
ferner eingerichtet ist, im Falle eines Feststellens eines nicht störungsfreien Übertragens über die erste Netzwerkverbindung (5) auf eine zweite, von der ersten verschiedenen Netzwerkverbindung (7) eines zweiten virtuellen Netzwerks (6) in dem physikalischen Netzwerk (2) umzuschalten.


2
3
18
8
9
10
3
14
Übertragen sicherheitsrelevanter Daten zwischen erstem und zweitem Netzwerkteilnehmer über erste Netzwerkverbindung des ersten virtuellen Netzwerks
5
4
Überprüfen, ob Übertragen sicherheitsrelevanter Daten über erste Netzwerkverbindung störungsfrei erfolgt
ja
3
7
nein
Umschalten auf zweite Netzwerkverbindung des zweiten virtuellen Netzwerks zum Übertragen sicherheitsrelevanter Daten zwischen erstem und zweitem Netzwerkteilnehmer
6

Figur 1



Figur 2



Figur 3