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

(11) **EP 4 035 970 A1**

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
03.08.2022 Patentblatt 2022/31

(21) Anmeldenummer: **21154235.2**

(22) Anmeldetag: **29.01.2021**

(51) Internationale Patentklassifikation (IPC):
B61L 3/12 *(2006.01)* ***B61L 15/00*** *(2006.01)*

(52) Gemeinsame Patentklassifikation (CPC):
B61L 15/0027; B61L 3/125

(84) Benannte Vertragsstaaten:
AL 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 RS SE SI SK SM TR
Benannte Erstreckungsstaaten:
BA ME
Benannte Validierungsstaaten:
KH MA MD TN

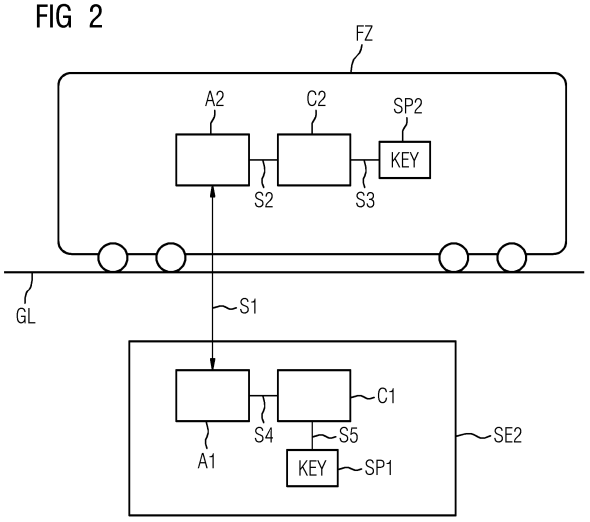
(71) Anmelder: **Siemens Mobility GmbH**
81739 München (DE)

(72) Erfinder: **Braband, Jens**
38106 Braunschweig (DE)

(54) VERFAHREN ZUR CODIERTEN KOMMUNIKATION ZWISCHEN EINEM STRECKENGEBUNDENEN FAHRZEUG UND EINER STRECKENSEITIGEN EINRICHTUNG, UND VORRICHTUNGEN ZUR ANWENDUNG DES VERFAHRENS

(57) Gegenstand der Erfindung ist ein Verfahren zur codierten Kommunikation zwischen einem streckengebundenem Fahrzeug (FZ) und einer streckenseitigen Einrichtung (SE1 ... SE6), bei der mehrere Telegramme (T1, T2) zwischen der streckenseitigen Einrichtung (SE1 ... SE6) und dem streckengebundenen Fahrzeug (FZ) übertragen werden. Die Telegramme (T1, T2) weisen jeweils einen Nutzdatenbereich zum Befüllen mit Nutzdaten sowie einen Codebereich für die Codierung der Nutzdaten auf. Mindestens eines der Telegramme (T1, T2) wird unverschlüsselt derart übertragen, dass der Nutzdatenbereich mit den unverschlüsselten Nutzdaten befüllt wird, wobei diese unter Nutzung des Codebereiches codiert werden, das Telegramm (T1, T2) mit den unverschlüsselten Nutzdaten codiert übertragen wird, und die unverschlüsselten Nutzdaten nach der Übertragung unter Nutzung des Codebereiches decodiert werden. Mindestens eines der Telegramme (T1, T2) wird verschlüsselt und codiert derart übertragen, dass die unverschlüsselten Nutzdaten vor dem Befüllen des Nutzdatenbereiches verschlüsselt werden und der Nutzdatenbereich mit den verschlüsselten Nutzdaten befüllt wird, wobei diese zusätzlich unter Nutzung des Codebereiches codiert werden. Außerdem wird das Telegramm (T1, T2) mit den verschlüsselten Nutzdaten codiert übertragen. Die verschlüsselten Nutzdaten werden nach der Übertragung des Telegramms (T1, T2) unter Nutzung des Codebereiches decodiert und danach werden die verschlüsselten Nutzdaten entschlüsselt. Ferner umfasst die Erfindung ein spurgebundenes Fahrzeug (FZ), eine streckenseitige Einrichtung (SE1 ... SE6), ein Computerprogrammprodukt sowie eine Bereitstellungseinrichtung für das Computerprogrammprodukt.

FIG 2



EP 4 035 970 A1

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zur rechnergestützten codierten Kommunikation zwischen einem streckengebundenen Fahrzeug und einer streckenseitigen Einrichtung, bei der mehrere Telegramme zwischen der streckenseitigen Einrichtung und dem streckengebundenen Fahrzeug übertragen werden, wobei die Telegramme jeweils

- einen Nutzdatenbereich zum Befüllen mit Nutzdaten aufweisen,
- einen Codebereich für die Codierung der Nutzdaten aufweisen.

[0002] Außerdem betrifft die Erfindung ein spurgebundenes Fahrzeug mit einer Kommunikationsschnittstelle für eine streckenseitige Einrichtung. Weiterhin betrifft die Erfindung eine streckenseitige Einrichtung mit einer Kommunikationsschnittstelle für ein streckengebundenes Fahrzeug.

[0003] Zuletzt betrifft die Erfindung ein Computerprogrammprodukt sowie eine Bereitstellungsvorrichtung für dieses Computerprogrammprodukt, wobei das Computerprogrammprodukt mit Programmbefehlen zur Durchführung dieses Verfahrens ausgestattet ist.

[0004] Als streckenseitige Einrichtungen sind beispielsweise Balisen, insbesondere nach dem ERTMS-Standard (Eurobalisen) bekannt. Jede dieser Balisen überträgt einen Datensatz, der als Telegramm bezeichnet wird. Diese Telegramme haben abhängig von der Balise entweder 1023 Bit oder 341 Bit. Davon lassen sich 830 beziehungsweise 210 Bit als Nutzdatenblock für die signaltechnische Anwendung nutzen - der Nutzdatenblock wird in 10 Bit-Symbole geteilt, die nach der Shaping- und Scrambling-Transformation durch je 11 Bit repräsentiert werden (mithin einem Block von 913 = 83*11 Bit oder 231 = 21*11 Bit):

Aufbau eines Telegramms am Beispiel einer Eurobalise
Kodierte Datenbits (Länge abhängig von der Balise)
913 Bit (Nutzdaten: 830 Bit bei einer Gesamtlänge von 1023 Bit) oder
231 Bit (Nutzdaten: 210 Bit bei einer Gesamtlänge von 341 Bit)

Kontrollbits	Cb	3 Bit
Scramblingbits	Sb	12 Bit
Zusätzliche Shapingbits	Esb	10 Bit
Checksumme	CheckBit	85 Bit

[0005] Beim Überfahren der Balise werden die Telegramme zyklisch wiederholt. Zum Schutz gegen Übertragungsfehler werden die Nutzdaten verwürfelt (Scramblingcode), eine Substitution der Nutzungsdaten mit Kodeworten verschiedener Hamming-Distanz gewählt, und die Prüfung durch eine Prüfsumme ermöglicht. Da die Prüfsumme erst nach dem Substitutionscode der Nutzdaten berechnet wird, dienen die zusätzlichen Shapingbits dazu, die Bits der Prüfsumme so aufzufüllen, dass das gesamte Telegramm nur noch aus Symbolen der gewählten Kanalcodierung besteht, wobei jedes übertragene Symbol je 11Bit umfasst.

[0006] Der Nutzdatenbereich besteht aus einem Kopfblock (header), gefolgt von mehreren Nachrichtenfeldern (Packete oder packets), die im ERTMS-Protokoll standardisiert sind, und am Ende dem Packet255 - End of information. Wenn der Nutzdatenbereich mehr als 830 Bit umfasst, können weitere Nachrichtenfelder über Telegramme der folgenden Balisen der gleichen Balisengruppe übertragen werden - mit bis zu acht Balisen pro Balisengruppen kann daher eine ERTMS-Nachricht bis zu 8*830=6640 Nutzdatenbits umfassen (wobei jedes Telegramm einen Kopfblock und das Ende-Paket 255 enthalten muss).

[0007] Eine Verschlüsselung der gesendeten Daten nach dem ER TMS-Standard und auch bei der Übertragung von Telegrammen durch andere streckenseitige Vorrichtungen ist nicht vorgesehen. Hierauf wurde in der Vergangenheit im Interesse einer möglichst schnellen Übertragung verzichtet, da Schienenfahrzeuge die Balisen mit vergleichsweise hohen Geschwindigkeiten überfahren und daher zur Übertragung des Telegramms nur wenig Zeit zur Verfügung steht. Andererseits besteht ein Interesse, die Kommunikation zwischen streckenseitiger Einrichtung und streckengebundenem Fahrzeug möglichst sicher zu machen.

[0008] Die Aufgabe der Erfindung ein Verfahren zur codierten Kommunikation zwischen streckengebundenen Fahrzeugen und streckenseitigen Einrichtungen anzugeben, welches einerseits standardisiert erfolgen kann und andererseits einen hohen Sicherheitsstandard bei der Übertragung erfüllt. Außerdem ist es Aufgabe der Erfindung, ein spurgebundenes Fahrzeug sowie eine streckenseitige Einrichtung anzugeben, welche zum Einsatz des genannten Verfahrens geeignet sind. Außerdem besteht die Aufgabe der Erfindung darin, ein Computerprogrammprodukt sowie eine Bereitstellungsvorrichtung für dieses Computerprogrammprodukt anzugeben, mit dem das vorgenannte Verfahren durchgeführt werden kann.

[0009] Diese Aufgabe wird mit dem eingangs angegebenen Anspruchsgegenstand (Verfahren) erfindungsgemäß dadurch gelöst, dass mindestens eines der Telegramme unverschlüsselt derart übertragen wird, dass

- der Nutzdatenbereich mit den unverschlüsselten Nutzdaten befüllt wird, wobei diese unter Nutzung des Codebereiches codiert werden,
- das Telegramm mit den unverschlüsselten Nutzdaten codiert übertragen wird,
- die unverschlüsselten Nutzdaten nach der Übertragung unter Nutzung des Codebereiches decodiert

werden,

und dass mindestens eines der Telegramme verschlüsselt und codiert derart übertragen wird, dass

- die unverschlüsselten Nutzdaten vor dem Befüllen des Nutzdatenbereiches verschlüsselt werden,
- der Nutzdatenbereich mit den verschlüsselten Nutzdaten befüllt wird, wobei diese zusätzlich unter Nutzung des Codebereiches codiert werden,
- das Telegramm mit den verschlüsselten Nutzdaten codiert übertragen wird,
- die verschlüsselten Nutzdaten nach der Übertragung des Telegramms unter Nutzung des Codebereiches decodiert werden,
- danach die verschlüsselten Nutzdaten entschlüsselt werden.

[0010] Erfindungsgemäß kann man also Nutzdaten (beispielsweise vor einer standardisierten Codierung) einfach verschlüsseln, beispielsweise mit einer Blockchiffre (und aufgefüllten Padding-Bits, um auf das benötigte Format zu kommen) oder einer Stromchiffre. Dazu müssen Sender und Empfänger (d. h. die streckenseitige Einrichtung und das streckengebundene Fahrzeug) über einen gemeinsamen Schlüssel verfügen.

[0011] Der codierte Übertragungsstandard selbst muss zum Zwecke der Übertragung der verschlüsselten Informationen nicht angetastet werden. Aus technischer Sicht werden erfindungsgemäß somit nur andere Daten als bei dem bekannten Verfahren, nämlich die verschlüsselten, übertragen, die durchaus denselben Inhalt haben können. Das heißt, dass ein verschlüsseltes Telegramm nach der Entschlüsselung identischen Inhalts mit einem vergleichbaren unverschlüsselten Telegramm sein kann. Der Inhalt eines Telegramms ist in den Nutzdaten untergebracht (hierzu im Folgenden noch mehr) .

[0012] Dadurch, dass die Übertragung des Telegramms aus technischer Sicht unangetastet bleibt, ist der Eingriff in den Übertragungsstandard, dessen Übertragung erfindungsgemäß sicherer gemacht werden soll, auf ein Minimum begrenzt. Dies erleichtert vorteilhaft die Zulassung für einen bereits bestehenden Standard, welche in vielen Fällen mit einem hohen Aufwand verbunden ist. Auch sind vorteilhaft an dem streckengebundenen Fahrzeug sowie an der streckenseitigen Einrichtung keine hardwarebezogenen Änderungen erforderlich. Die Verschlüsselung kann durch eine Modifikation der Betriebssoftware erfolgen, was mit bedeutend geringeren Investitionen einhergeht. Durch die erfindungsgemäß gemischte Übertragung von verschlüsselten und unverschlüsselten Telegrammen ist außerdem vorteilhaft eine schrittweise Einführung des verbesserten Übertragungsverfahrens möglich. Mit einer schrittweisen Einführung ist gemeint, dass ein betreffender Streckenabschnitt, der mit streckenseitigen Einrichtungen ausgerüstet ist, welche das erfindungsgemäße Verfahren bereits anwenden können, auch von streckengebundenen Fahrzeugen befahren werden kann, welche verschlüsselte Telegramme nicht entschlüsseln können. Denn an solche Fahrzeuge können seitens der streckenseitigen Einrichtungen unverschlüsselte Telegramme übertragen werden.

[0013] Die erfindungsgemäße Modifikation kann beispielsweise für die Kommunikation von Eurobalisen mit schienengebundenen Fahrzeugen durchgeführt werden. Die Modifikation ist allerdings nicht auf diesen Anwendungsfall beschränkt. Überall, wo eine codierte Übertragung zwischen streckenseitigen Einrichtungen und strecken gebundenen Fahrzeugen vorgesehen ist, kann diese zusätzlich durch eine Verschlüsselung der zu übertragenden Informationen vor deren Kodierung ergänzt werden, um den Sicherheitsstandard zu erhöhen. Insbesondere kann diese Modifikation nicht nur bei schienengebundenen Fahrzeugen von Vorteil sein, sondern beispielsweise auch bei Fahrzeugen (Automobile), die durch einen autonomen Betrieb an eine bestimmte Strecke, zum Beispiel eine Straße, gebunden sind.

[0014] Der Dekodierungsschritt selbst entspricht eventuell nicht dem Standard, da geprüft werden muss, ob alle empfangenen Telegramme identisch sind. Hier müsste der Standard gegebenenfalls geändert werden. Zumindest die Übertragung selbst kann aber unter Ausnutzung des erfindungsgemäßen Vorteils ohne Änderungen des Standards erfolgen. Damit könnte der Standard erweitert werden, was eine Abwärtskompatibilität einer unverschlüsselten Übertagung sicherstellt. Eine Entschlüsselung könnte alternativ losgelöst vom Standard nach Dekodierung erfolgen.

[0015] Grundsätzlich ist für das Verfahren ohne Bedeutung, in welche Richtung die Übertragung erfolgen soll. Die Übertragung erfolgt von einem Sender zu einem Empfänger. Bei der Übertragung des Telegramms zwischen dem streckengebundenen Fahrzeug und der streckenseitigen Einrichtung kann sowohl das streckengebundene Fahrzeug der Empfänger und die streckenseitige Einrichtung der Sender als auch das streckengebundene Fahrzeug der Sender und die streckenseitige Einrichtung der Empfänger sein. Es ist sowohl möglich, dass eine Übertragung nur in eine Richtung (und optional zu einer anderen Zeit in andere Richtung) erfolgt, als auch, dass die Übertragung in beide Richtungen gleichzeitig erfolgt.

[0016] Als Kodierung im Sinne der Erfindung wird eine Modifikation der Nutzdaten des Nutzdatenbereiches mithilfe des Codebereiches verstanden, der die notwendigen Informationen für die Kodierung enthält. Eine solche Kodierung kann beispielsweise in einem Standard zur Übertragung des Telegramms festgelegt sein und ist daher an sich bekannt. Daher kann eine solche Kodierung auch nicht für eine Zugriffsbeschränkung auf das Telegramm durch Unbefugte dienen, da die Kodierung nachvollzogen werden kann.

[0017] Demgegenüber ist unter einer Verschlüsselung im Sinne der Erfindung eine Modifikation der Nutzdaten mithilfe von Schlüsseln zu verstehen, wobei die Verschlüsselung einen Schutz vor einem unbefugten Zugriff

auf die Telegramme gewährleistet. Der Schlüssel muss sowohl beim Sender als auch beim Empfänger verfügbar sein, um eine Verschlüsselung des Telegramms und eine anschließende Entschlüsselung zu gewährleisten. Dabei kann auf an sich bekannte Verschlüsselungsverfahren zurückgegriffen werden.

[0018] Unter "rechnergestützt" oder "computerimplementiert" kann im Zusammenhang mit der Erfindung eine Implementierung des Verfahrens verstanden werden, bei dem mindestens ein Computer oder Prozessor mindestens einen Verfahrensschritt des Verfahrens ausführt.

[0019] Der Ausdruck "Rechner" oder "Computer" deckt alle elektronischen Geräte mit Datenverarbeitungseigenschaften ab. Computer können beispielsweise Personal Computer, Server, Handheld-Computer, Mobilfunkgeräte und andere Kommunikationsgeräte, die rechnergestützt Daten verarbeiten, Prozessoren und andere elektronische Geräte zur Datenverarbeitung sein, die vorzugsweise auch zu einem Netzwerk zusammengeschlossen sein können.

[0020] Unter einem "Prozessor" kann im Zusammenhang mit der Erfindung beispielsweise einen Wandler einen Sensor zur Erzeugung von Messsignalen oder eine elektronische Schaltung, verstanden werden. Bei einem Prozessor kann es sich insbesondere um einen Hauptprozessor (engl. Central Processing Unit, CPU), einen Mikroprozessor, einen Mikrocontroller, oder einen digitalen Signalprozessor, möglicherweise in Kombination mit einer Speichereinheit zum Speichern von Programmbefehlen, etc. handeln. Auch kann unter einem Prozessor ein virtualisierter Prozessor oder eine Soft-CPU verstanden werden.

[0021] Unter einer "Speichereinheit" kann im Zusammenhang mit der Erfindung beispielsweise ein computerlesbarer Speicher in Form eines Arbeitsspeichers (engl. Random-Access Memory, RAM) oder Datenspeichers (Festplatte oder Datenträger) verstanden werden.

[0022] Als "Schnittstellen" können hardwaretechnisch, beispielsweise kabelgebunden oder als Funkverbindung, und/oder softwaretechnisch, beispielsweise als Interaktion zwischen einzelnen Programmmodulen oder Programmteilen eines oder mehrerer Computerprogramme, realisiert sein.

[0023] Als "Cloud" soll eine Umgebung für ein "Cloud-Computing" (deutsch Rechnerwolke oder Datenwolke) verstanden werden. Gemeint ist eine IT-Infrastruktur, welche über Schnittstellen eines Netzwerks wie das Internet verfügbar gemacht wird. Sie beinhaltet in der Regel Speicherplatz, Rechenleistung oder Software als Dienstleistung, ohne dass diese auf dem die Cloud nutzenden lokalen Computer installiert sein müssen. Die im Rahmen des Cloud-Computings angebotenen Dienstleistungen umfassen das gesamte Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur, Plattformen und Software.

[0024] Als "Programmmodule" sollen einzelne Funktionseinheiten verstanden werden, die einen erfindungsgemäßen Programmablauf von Verfahrensschritten ermöglichen. Diese Funktionseinheiten können in einem einzigen Computerprogramm oder in mehreren miteinander kommunizierenden Computerprogrammen verwirklicht sein. Die hierbei realisierten Schnittstellen können softwaretechnisch innerhalb eines einzigen Prozessors umgesetzt sein oder hardwaretechnisch, wenn mehrere Prozessoren zum Einsatz kommen.

[0025] Gemäß einer Ausgestaltung der Erfindung ist vorgesehen, dass mindestens eines der mit unverschlüsselten Nutzdaten übertragenen Telegramme auch als Telegramm mit verschlüsselten Nutzdaten desselben Inhalts übertragen wird.

[0026] Hierbei ist zu bemerken, dass die unverschlüsselten Nutzdaten sich natürlich von den verschlüsselten Nutzdaten unterscheiden. Dies ändert allerdings nichts daran, dass die unverschlüsselten Nutzdaten denselben Inhalt haben können, wie die verschlüsselten Nutzdaten. Als Inhalt im Sinne der Erfindung ist somit der Informationsgehalt der Nutzdaten zu verstehen, der nach Entschlüsselung der verschlüsselten Nutzdaten zugänglich wird und dann denselben Inhalt aufweist, wie die unverschlüsselt übertragenen Nutzdaten des entsprechenden Telegramms.

[0027] Durch die Übertragung eines Telegramms desselben Inhalts sowohl in verschlüsselter wie auch in unverschlüsselt Form ist es möglich, dass der Inhalt des Telegramms sowohl von spurgebundenen Fahrzeugen ausgewertet werden kann, die das verschlüsselte Telegrammen entschlüsseln können (nachfolgend ausgerüstetes Fahrzeug genannt) als auch von spurgebundenen Fahrzeugen die (noch) nicht über den Schlüssel verfügen (nachfolgend nicht ausgerüstetes Fahrzeug genannt). Letztere können zwar nicht mithilfe des verschlüsselt übertragenen Telegramms prüfen, ob das unverschlüsselt übertragene Telegramm manipuliert wurde, jedoch lässt sich der Betrieb des Fahrzeugs mittels des unverschlüsselten Telegramms sicherstellen.

[0028] Durch die Versendung von Telegrammen gleichen Inhalts sowohl verschlüsselt als auch unverschlüsselt ist es ausgerüsteten Fahrzeugen möglich, die Inhalte der Telegramme gleichen Inhalts nach Entschlüsselung und Dekodierung bzw. nach Dekodierung zu vergleichen und aus dem Vergleichsergebnis gegebenenfalls weitere Schritte abzuleiten. Beispielsweise können Manipulationen oder Fehler in den unverschlüsselt übertragenen Telegrammen aufgedeckt werden. Auch ist es möglich, (wenn auch unwahrscheinlicher,) dass der Inhalt des verschlüsselten Telegramms einen Fehler aufweist.

[0029] Wenn eine Manipulation oder ein Fehler festgestellt wird, kann aus dieser Feststellung eine Sicherheitsmaßnahme abgeleitet werden.

[0030] Diese kann sich vorteilhaft auch auf nicht ausgerüstete Fahrzeuge beziehen, die beispielsweise in einem bestimmten Zeitintervall vor der Feststellung der Manipulation mit der betroffenen streckenseitigen Einrichtung kommuniziert haben. Vorteilhaft macht somit die Dekodierung der kodierten Telegramme den Zugbetrieb

insgesamt sicherer, also auch den Betrieb nicht ausgerüsteter Fahrzeuge, wenn auch Telegramme mit geändertem Inhalt bezüglich der nicht ausgerüsteten Züge nur zeitverzögert festgestellt werden können. Die Sicherheitsmaßnahmen können sich auf einzelne streckengebundene Fahrzeuge, streckenseitige Einrichtungen oder bestimmte Streckenabschnitte oder auch den gesamten Betrieb beziehen, je nachdem, wie schwerwiegend der festgestellte Fehler oder die festgestellten Fehler (in Form von Abweichungen im Inhalt von Telegrammen) ausfallen.

[0031] Gemäß einer Ausgestaltung der Erfindung ist vorgesehen, dass

- zuerst die unverschlüsselten Nutzdaten nach der Übertragung unter Nutzung des Codebereiches decodiert werden,
- danach die verschlüsselten Nutzdaten nach der Übertragung des Telegramms unter Nutzung des Codebereiches decodiert werden,
- danach die verschlüsselten Nutzdaten entschlüsselt werden.

[0032] Diese Ausgestaltung der Erfindung zielt auf eine Verbesserung der Performance bei der Dekodierung der Nutzdaten. Dabei werden zunächst die unverschlüsselten Nutzdaten dekodiert (vor den verschlüsselten desselben Inhalts), da bei diesen der Schritt einer Entschlüsselung eingespart werden kann und auf diese Weise eine Zugänglichkeit des Inhaltes früher gegeben ist. Dieser Effekt wirkt sich besonders stark aus, wenn die Telegramme von einem Fahrzeug oder einer streckenseitigen Einrichtung empfangen werden, die noch keine Entschlüsselung der verschlüsselten Nutzdaten vornehmen kann. Diese müssten nämlich sonst in einem weiteren Schritt auf die unverschlüsselten Nutzdaten zurückgreifen, was einen zusätzlichen Zeitverlust bedeuten würde.

[0033] Gemäß einer Ausgestaltung der Erfindung ist vorgesehen, dass

- zuerst das mindestens eine mit unverschlüsselten Nutzdaten übertragenen Telegramm,
- danach das Telegramm mit den verschlüsselten Nutzdaten desselben Inhalts übertragen wird.

[0034] Hierdurch lässt sich vorteilhaft ein zusätzlicher Performancegewinn bei der Auswertung der übertragenen Nutzdaten bei dem Empfänger erzeugen. Dieser Performancegewinn wird dadurch erreicht, dass mit der Dekodierung der unverschlüsselten Nutzdaten in dem übertragenen Telegramm bereits begonnen werden kann, während das Telegramm mit den verschlüsselten Nutzdaten desselben Inhalts noch übertragen wird. Dies wäre bei umgekehrter Reihenfolge nicht möglich.

[0035] Gemäß einer Ausgestaltung der Erfindung ist vorgesehen, dass in wechselnder Reihenfolge Telegramme mit verschlüsselten und unverschlüsselten Nutzdaten übertragen werden.

[0036] Hierdurch wird das Problem gelöst, dass bei bestehenden Strecken und bereits im Einsatz befindlichen streckengebundenen Fahrzeugen (zumindest vor einer Aktualisierung) ein Kommunikationsstandard verwendet wird, welcher eine Entschlüsselung der Nutzdaten noch nicht ermöglicht. Dadurch, dass sowohl verschlüsselte als auch unverschlüsselte Nutzdaten codiert in wechselnder Reihenfolge übertragen werden, ist es sowohl ausgerüsteten Fahrzeugen als auch nicht ausgerüsteten Fahrzeugen möglich, die für den Betrieb erforderlichen Informationen aus den Nutzdaten mehrerer unterschiedlicher Telegramme zu extrahieren. Dabei wird erfindungsgemäß berücksichtigt, dass für die Übertragung der Daten zwischen der streckenseitigen Einrichtung und dem streckengebundenen Fahrzeug während der Vorbeifahrt des Letzteren nur ein begrenzter Zeitraum zur Verfügung steht.

[0037] Damit die Wahrscheinlichkeit, dass bei der Vorbeifahrt nicht alle Telegramme übertragen werden, möglichst gering ist, kann beispielsweise ein erstes Telegramm verschlüsselt und unverschlüsselt dann ein zweites Telegramm verschlüsselt und unverschlüsselt dann ein drittes Telegramm verschlüsselt und unverschlüsselt werden usw. Wenn alle zu übertragenen Telegramme verschlüsselt und unverschlüsselt übertragen wurden, kann wieder mit dem ersten Telegramm begonnen werden usw. Passiert beispielsweise das streckengebundene Fahrzeug die streckenseitige Einrichtung, während das dritte Telegramm übertragen wird, so können das erste und das zweite Telegrammen im zweiten Übertragungszyklus empfangen werden.

[0038] Die wechselnde Reihenfolge bedeutet nicht zwangsläufig, dass unverschlüsselte Telegramme (U) und verschlüsselte Telegramme (V) abwechselnd gesendet werden müssen, also:
U, V, U, V...

[0039] Je nachdem, ob man Sicherheit oder Verfügbarkeit höher priorisieren möchte, kann man auch andere Kombinationen senden, d. h. entweder mehr N (höhere Verfügbarkeit) oder mehr V-Telegramme (höhere Sicherheit) senden z. B.:

U, V, V, U, V, V ...
U, U, V, U, U, V ...
U, U, U, V, U, U, U, V ...

[0040] Bei den letztgenannten Beispielen ergibt sich in der wechselnden Reihenfolge eine Wiederholung von Sequenzen (nämlich U, V und U, V, V und U, U, U, V - andere Sequenzen sind denkbar). Allerdings kann die zu wiederholende Sequenz je nach Bedarf während der Übertragung auch gewechselt werden. Eine weitere Möglichkeit besteht darin, die wechselnde Reihenfolge, ohne eine Wiederholungsregel zu bestimmen.

[0041] In der Regel werden zum Beispiel bei einer Balisenüberfahrt ohnehin mehrere Telegramme übertragen. Um hierbei Kompatibilität zu erreichen, werden im Sendestrom der Balise einfach unverschlüsselte Tele-

gramme (U) und verschlüsselte Telegramme (V) in wechselnder Reihenfolge, d. h. gemischt und aufeinanderfolgend gesendet, z. B. abwechselnd. Insbesondere bei Eurobalisen, bei denen Langtelegramme und Kurztelegramme übertragen werden können, können Dreiersequenzen von Kurztelegrammen gewählt werden, die der Übertragung eines Langtelegramms entsprechen. Der oben beschriebene Effekt, dass auch bei kurzen Übertragungszeiten (beispielsweise bei hohen Geschwindigkeiten des streckengebundenen Fahrzeugs) möglichst alle Daten übertragen werden, lässt sich daher bei Eurobalisen besonders wirkungsvoll umsetzen.

[0042] Gemäß einer Ausgestaltung der Erfindung ist vorgesehen, dass in einer Sequenz von Telegrammen im Verhältnis mehr Telegramme mit unverschlüsselten Nutzdaten als Telegramme mit verschlüsselten Nutzdaten übertragen werden, wobei

- die Nutzdatenbereiche der unverschlüsselt übertragenen Telegramme der Sequenz mit unterschiedlichen Inhalten befüllt sind,
- mindestens eines der mit unverschlüsselten Nutzdaten übertragenen Telegramme der Sequenz auch als Telegramm mit verschlüsselten Nutzdaten desselben Inhalts übertragen wird.

[0043] Diese Ausführungsformen der Erfindung hat den Vorteil, das bei einer begrenzten zur Verfügung stehenden Übertragungszeit, beispielsweise bei der Überfahrt des streckengebundenen Fahrzeugs über eine Balise als streckenseitige Einrichtung, eine größere Datenmenge übertragen werden kann. Denn die Übertragung unverschlüsselter Daten kann schneller erfolgen als die Übertragung von unverschlüsselten Daten. Dies hängt in erster Linie damit zusammen, dass die Daten vor dem Versenden noch verschlüsselt werden müssen, aber auch damit, dass die Verschlüsselung die Datenmenge und damit die erforderliche Übertragungszeit vergrößert.

[0044] Bei dem Verhältnis von ausschließlich unverschlüsselt übertragenen Telegrammen einerseits und verschlüsselt und unverschlüsselt übertragenen Telegrammen andererseits muss ein technischer Kompromiss gefunden werden, der sowohl die zu übertragende Datenmenge in Bezug auf die zur Verfügung stehende Übertragungszeit (Datenrate) berücksichtigt als auch eine ausreichende Möglichkeit schafft, durch einen Vergleich eines verschlüsselten Telegramms mit einem unverschlüsselten Telegramm desselben Inhalts eine Datenmanipulation oder Fehler feststellen zu können. Je mehr Telegramme auch verschlüsselt versendet werden, desto sicherer wird das Übertragungsverfahren. Je mehr Telegramme nur unverschlüsselt versendet werden, desto höher wird die übertragbare Datenrate.

[0045] Gemäß einer Ausgestaltung der Erfindung ist vorgesehen, dass die Nutzdaten eines verschlüsselt gesendeten Telegramms nach dem Entschlüsseln mit den Nutzdaten eines unverschlüsselt gesendeten Telegramms desselben Inhalts vor und/oder nach dem Dekodieren miteinander verglichen werden.

[0046] Der Vergleich dient, wie oben beschrieben, dem Aufdecken von Fehlern oder Manipulationen der Nutzdaten in den Telegrammen. Hierdurch kann also das Übertragungsverfahren genügend sicher gemacht werden, auch wenn ein Teil der Telegramme unverschlüsselt versendet wird. Inhaltliche Abweichungen in unverschlüsselten Telegrammen werden dadurch nämlich zeitnah auffallen, sodass Gegenmaßnahmen getroffen werden können, und die Sicherheit des Betriebs nur geringfügig beeinträchtigt ist.

[0047] Gemäß einer Ausgestaltung der Erfindung ist vorgesehen, dass in dem Fall, dass das Vergleichen ergibt, dass die Nutzdaten des verschlüsselt gesendeten Telegramms von den Nutzdaten des unverschlüsselt gesendeten Telegramms desselben Inhalts, abweicht, ein Fehlersignal generiert und/oder ausgegeben wird.

[0048] Das Fehlersignal dient damit für die Einleitung weiterer Schritte. Diese Schritte können in einer Interpretation oder Bewertung der Abweichungen des betreffenden Telegramms vom zu erwartenden Inhalt bestehen. Auch können diese Schritte bereits sicherheitsrelevante Reaktionen beinhalten, wie dies oben bereits näher beschrieben wurde. Das Fehlersignal ist somit die Grundlage für eine informationstechnische Verarbeitung, die auf die Registrierung eines Fehlers oder einer Manipulation folgen muss.

[0049] Gemäß einer Ausgestaltung der Erfindung ist vorgesehen, dass mehrere Telegramme mit unterschiedlich großen Nutzdatenbereichen übertragen werden.

[0050] Hierdurch ist es vorteilhaft möglich, dass die Größe der Nutzdatenbereiche entsprechend der zu übertragenden Informationsmenge ausgewählt werden kann. Bei einer Verschlüsselung ist dies von besonderem Vorteil, da die Verschlüsselung kleinerer Datenmengen einen geringeren Zeitaufwand und Rechenaufwand nach sich zieht und daher die Übertragung und Entschlüsselung, und damit die Nutzung der Daten in einem kürzeren Zeitintervall erfolgen kann. Insbesondere, wenn Daten über eine Balise an ein streckengebundenes Fahrzeug überragen werden sollen, steht hierbei während der Überfahrt des Fahrzeugs über die Balise nur ein kurzes Zeitintervall zur Verfügung.

[0051] Gemäß einer Ausgestaltung der Erfindung ist vorgesehen, dass die Schritte, dass

- der Nutzdatenbereich mit den verschlüsselten Nutzdaten befüllt wird, wobei diese zusätzlich unter Nutzung des Codebereiches codiert werden,
- das Telegramm mit den verschlüsselten Nutzdaten codiert übertragen wird,
- die verschlüsselten Nutzdaten nach der Übertragung des Telegramms unter Nutzung des Codebereiches decodiert werden,
  oder
- der Nutzdatenbereich mit den unverschlüsselten Nutzdaten befüllt wird, wobei diese unter Nutzung

des Codebereiches codiert werden,
- das Telegramm mit den unverschlüsselten Nutzdaten codiert übertragen wird,
- die unverschlüsselten Nutzdaten nach der Übertragung unter Nutzung des Codebereiches decodiert werden,

nach für dem ETCS (European Train Control System) geltenden ERTMS-Standard (European Rail Traffic Management System) oder dem CBTC-Standard (Communication-Based Train Control) oder dem PTC-Standard (Positive Train Control) durchgeführt werden.

[0052] Alle diese Standards sehen einer Übertragung zwischen streckenseitigen Einrichtungen und streckengebundenen Fahrzeugen in codierter Form vor. Diese Standards profitieren daher in der oben angegebenen Weise von einer zusätzlichen Verschlüsselung eines Teils der übertragenen Daten, wodurch die Sicherheit im Betrieb erhöht werden kann.

[0053] Gemäß einer Ausgestaltung der Erfindung ist vorgesehen, dass die Übertragung zwischen einer Balise als streckenseitige Einrichtung und dem streckengebundenen Fahrzeug stattfindet.

[0054] Die Vorteile der Anwendung des erfindungsgemäßen Verfahrens bei Balisen ist oben stehend bereits erläutert worden.

[0055] Gemäß einer Ausgestaltung der Erfindung ist vorgesehen, dass geprüft wird, ob die Balise zu einem Balisenverband gehört, wobei die empfangenen Daten dann als vertrauenswürdig eingestuft werden.

[0056] Nicht gelinkte Balisen sollen im Rahmen der Erfindung als Balisen verstanden werden, welche bei der Übertragung nicht im Zusammenhang mit anderen Balisen stehen: Diese bieten daher ein größeres Potential für nicht autorisierte Angriffe. Beispielsweise könnten Hacker einen Gefahrpunkt löschen oder die zulässige Geschwindigkeit für einen Zug erhöhen.

[0057] Gelinkte Balisen stehen im Gegensatz zu nicht gelinkten Balisen mit anderen Balisen eines Balisenverbandes in einem funktionalen Zusammenhang. Dies bedeutet aber auch, dass ein nicht autorisierter Angriff auch ohne die verschlüsselte Übertragung von Telegrammen gleichen Inhalts aufgedeckt werden kann, wenn die durch die Balisen gesendete Information nicht in den Kontext des Balisenverbandes passt, d. h. nicht in den Sinnzusammenhang passt, der bei der Überfahrt der betreffenden Balisen zu erwarten wäre. Dadurch, dass die Funktionalität des Balisenverbandes bekannt ist, ist nämlich im Rahmen einer Plausibilitätsprüfung) ein Rückschluss möglich, welche Information von einer bestimmten Balisen des Balisenverbandes zu erwarten ist, und wann diese Information übermittelt wird (in Abhängigkeit von der Position der Balise innerhalb des Balisenverbandes).

[0058] Damit besteht die Möglichkeit, vorzugsweise ungelinkte Balisen mit einer Verschlüsselung im Sinne der Erfindung auszustatten. Hierbei handelt es sich nämlich häufig ohnehin um nachgerüstete Balisen, die nicht in einen Balisenverband integriert werden. Gleichzeitig schafft die Nachrüstung die Möglichkeit, diese von Anfang an mit einer erfindungsgemäßen Verschlüsselungsmöglichkeit für die übertragenen Telegramme auszustatten. Die verschlüsselte Übertragung schafft dann einen Schutz, von dem eine nicht gelinkte Balise in besonderem Maße profitiert. Diese würde außerhalb des Balisenverbandes aufgrund der oben angeführten Zusammenhänge nämlich eine Schwachstelle für unautorisierte Angriffe bilden.

[0059] Die genannte Aufgabe wird alternativ mit dem eingangs angegebenen Anspruchsgegenstand (Fahrzeug) erfindungsgemäß auch dadurch gelöst, dass dieses dafür eingerichtet ist, an einem Verfahren zur codierten Kommunikation gemäß einem der voranstehenden Ansprüche teilzunehmen.

[0060] Die genannte Aufgabe wird außerdem alternativ mit dem eingangs angegebenen Anspruchsgegenstand (Einrichtung) erfindungsgemäß auch dadurch gelöst, dass diese dafür eingerichtet ist, an einem Verfahren zur codierten Kommunikation gemäß einem der Ansprüche 1 - 12 teilzunehmen.

[0061] Mit den Vorrichtungen (d.h. Fahrzeug und Einrichtung) lassen sich die Vorteile erreichen, die im Zusammenhang mit dem obenstehend näher beschriebenen Verfahren bereits erläutert wurden. Das zum erfindungsgemäßen Verfahren Aufgeführte gilt entsprechend auch für die erfindungsgemäßen Vorrichtungen.

Des Weiteren wird ein Computerprogrammprodukt mit Programmbefehlen zur Durchführung des genannten erfindungsgemäßen Verfahrens und/oder dessen Ausführungsbeispielen beansprucht, wobei mittels des Computerprogrammprodukts jeweils das erfindungsgemäße Verfahren und/oder dessen Ausführungsbeispiele durchführbar sind.

[0062] Darüber hinaus wird eine Bereitstellungsvorrichtung zum Speichern und/oder Bereitstellen des Computerprogrammprodukts beansprucht. Die Bereitstellungsvorrichtung ist beispielsweise ein Speichereinheit, die das Computerprogrammprodukt speichert und/oder bereitstellt. Alternativ und/oder zusätzlich ist die Bereitstellungsvorrichtung beispielsweise ein Netzwerkdienst, ein Computersystem, ein Serversystem, insbesondere ein verteiltes, beispielsweise cloudbasiertes Computersystem und/oder virtuelles Rechnersystem, welches das Computerprogrammprodukt vorzugsweise in Form eines Datenstroms speichert und/oder bereitstellt.

[0063] Die Bereitstellung erfolgt in Form eines Programmdatenblocks als Datei, insbesondere als Downloaddatei, oder als Datenstrom, insbesondere als Downloaddatenstrom, des Computerprogrammprodukts. Diese Bereitstellung kann beispielsweise aber auch als partieller Download erfolgen, der aus mehreren Teilen besteht. Ein solches Computerprogrammprodukt wird beispielsweise unter Verwendung der Bereitstellungsvorrichtung in ein System eingelesen, sodass das erfindungsgemäße Verfahren auf einem Computer zur Ausführung gebracht wird.

[0064] Weitere Einzelheiten der Erfindung werden nachfolgend anhand der Zeichnung beschrieben. Gleiche oder sich entsprechende Zeichnungselemente sind jeweils mit den gleichen Bezugszeichen versehen und werden nur insoweit mehrfach erläutert, wie sich Unterschiede zwischen den einzelnen Figuren ergeben.

[0065] Bei den im Folgenden erläuterten Ausführungsbeispielen handelt es sich um bevorzugte Ausführungsformen der Erfindung. Bei den Ausführungsbeispielen stellen die beschriebenen Komponenten der Ausführungsformen jeweils einzelne, unabhängig voneinander zu betrachtende Merkmale der Erfindung dar, welche die Erfindung jeweils auch unabhängig voneinander weiterbilden und damit auch einzeln oder in einer anderen als der gezeigten Kombination als Bestandteil der Erfindung anzusehen sind. Des Weiteren sind die beschriebenen Komponenten auch durch mit den vorstehend beschriebenen Merkmalen der Erfindung kombinierbar.

[0066] Es zeigen:

Figur 1 ein Ausführungsbeispiel der erfindungsbemäßen Vorrichtungen (streckenseitige Einrichtung, streckengebundenes Fahrzeug) mit ihren Wirkzusammenhängen schematisch,

Figur 2 ein Ausführungsbeispiel einer Computer-Infrastruktur der Vorrichtungen (streckenseitige Einrichtung, streckengebundenes Fahrzeug) gemäß Figur 1 als Blockschaltbild, wobei die einzelnen Funktionseinheiten Programmmodule enthalten, die jeweils in einem oder mehreren Prozessoren ablaufen können und die Schnittstellen demgemäß softwaretechnisch oder hardwaretechnisch ausgeführt sein können,

Figur 3 und 4 Ausführungsbeispiele der Übertragung von verschlüsselten sowie unverschlüsselten Kurztelegrammen und Langtelegrammen, abhängig von einem Zeitverlauf t,

Figur 5 ein Ausführungsbeispiel des erfindungsgemäßen Verfahrens als Flussdiagramm, wobei die einzelnen Verfahrensschritte einzeln oder in Gruppen durch Programmmodule verwirklicht sein können und wobei die Funktionseinheiten und Schnittstellen gemäß Figur 2 beispielhaft angedeutet sind.

[0067] In Figur 1 ist als Strecke ein Gleis GL dargestellt, auf dem ein streckengebundenes Fahrzeug FZ in einer Fahrtrichtung FR fährt. Außerdem ist die Strecke in Form des Gleises GL mit streckenseitigen Einrichtungen SE1 ... SE6 ausgestattet, die in dem Ausführungsbeispiel gemäß Figur 1 als Eurobalisen ausgeführt sind.

[0068] Die streckenseitigen Einrichtungen SE1 sowie SE3 ... SE6 bilden einen Verband VB von streckenseitigen Einrichtungen. Diese streckenseitigen Einrichtungen können beispielsweise bereits bei der Erstausstattung der Strecke vorgesehen worden sein, wobei diese in einem funktionalen Zusammenhang stehen und deshalb im Folgenden als gelinkte Balisen bezeichnet werden sollen. Die streckenseitige Einrichtung SE2 könnte beispielsweise zu einem späteren Zeitpunkt nachgerüstet worden sein, um auf der Strecke einen weiteren Referenzpunkt zur Ortung des streckengebundenen Fahrzeugs FZ zu bekommen. Diese streckenseitige Einrichtung SE2 gehört jedoch nicht dem Verband VB an und soll daher als nicht gelinkte Balise bezeichnet werden.

[0069] Die streckenseitigen Einrichtungen des Verbandes VB sind im Vergleich zur nicht gelinkten Balise, repräsentiert durch die streckenseitige Einrichtung SE2, weniger angreifbar für Hacker bzw. fehleranfällig. Dies kann damit begründet werden, dass der funktionale Zusammenhang dazu führt, dass von den streckenseitigen Einrichtungen SE1 und SE3 ... SE6 bestimmte Daten erwartet werden, die in den Kontext des Fahrgeschehens des streckengebundenen Fahrzeugs FZ passen. Eine Abweichung hiervon fällt also schneller auf als bei der nicht gelinkten Balise, repräsentiert durch die streckenseitige Einrichtung SE2. Von dem erfindungsgemäßen Verfahren einer gemischt verschlüsselten und unverschlüsselten Übertragung von Telegrammen profitiert daher die streckenseitige Einrichtung SE2 am meisten. Diese kann beispielsweise im Rahmen einer Nachrüstung von Anfang an für das erfindungsgemäße Verfahren ausgelegt werden.

[0070] In Figur 2 sind das streckengebundene Fahrzeug FZ sowie die streckenseitige Einrichtung SE2 schematisch dargestellt. Die Übertragung von Daten erfolgt über eine erste Schnittstelle S1, die als Funkschnittstelle ausgeführt ist. Daher weist die streckenseitige Einrichtung SE2 eine erste Antenne A1 und das streckengebundene Fahrzeug FZ eine zweite Antenne A2 auf.

[0071] Die erste Antenne A1 ist mit einem ersten Computer C1 über eine vierte Schnittstelle S4 verbunden. Außerdem kann der erste Computer C1 über eine fünfte Schnittstelle S5 einen Schlüssel KEY aus einer ersten Speichereinrichtung SP1 abrufen. Der Schlüssel KEY ermöglicht somit die erfindungsgemäße Entschlüsselung bzw. Verschlüsselung eines über die erste Schnittstelle S1 zu übertragenden Telegramms (in der Funktion als Balise wird die streckenseitige Einrichtung SE2 vorzugsweise das Telegramm über die erste Schnittstelle S1 an das streckengebundene Fahrzeug FZ senden).

[0072] Die zweite Antenne A2 ist über eine zweite Schnittstelle S2 mit einem zweiten Computer C2 verbunden. Der zweite Computer C2 kann über eine dritte Schnittstelle S3 auf eine zweite Speichereinrichtung SP2 zugreifen, in der u. a. ein Schlüssel KEY abgespeichert ist. Somit weisen das streckengebundene Fahrzeug FZ sowie die streckenseitige Einrichtung SE2 jeweils einen Schlüssel KEY zur Entschlüsselung bzw. Verschlüsselung des über die erste Schnittstelle S1 zu übertragenden Telegramms auf.

[0073] Figur 3 zeigt anhand des Beispiels von durch Eurobalisen zu übertragenden Telegrammen den Vorteil, wenn statt einem Langtelegramm LT mehrere Kurz-

telegramme KT übertragen werden. Dabei ergeben jeweils drei Kurztelegramme KT, wie in Figur 3 angedeutet, ein Langtelegramm LT - zumindest vom zu übertragenden Datenumfang her.

[0074] Die Übertragung von Telegrammen ist in Figur 3 als Band dargestellt, wobei dies einem zeitlichen Ablauf entsprechend einer Zeitachse t entspricht. Während der Überfahrt des Fahrzeugs FZ über die streckenseitige Einrichtung (beispielsweise SE2 wie in Figur 2 dargestellt) gibt es nur ein bestimmtes Zeitfenster, in dem die beiden Antennen A1, A2 genügend nah beieinander liegen, damit eine Übertragung erfolgen kann. Diese Zeitfenster wird als Übertragungsfenster REC bezeichnet und ist in Figur 3 eingetragen.

[0075] In dem Beispiel gemäß Figur 3 überquert das streckengebundene Fahrzeug FZ die streckenseitige Einrichtung SE2 gerade mit einer Geschwindigkeit, bei welcher theoretisch vier Kurztelegramme KT übertragen werden können. Allerdings zeigt Figur 3 auch, dass sich das Übertragungsfenster REC öffnet, während gerade ein Kurztelegramm KT übertragen wird, sodass dieses abgeschnitten ist und von dem streckengebundenen Fahrzeug FZ nicht ausgewertet werden kann. Dasselbe gilt für das fünfte und letzte Kurztelegramm KT, welches (zumindest teilweise) in dem Übertragungsfenster REC gemäß Figur 3 liegt. Dazwischen liegen drei vollständig übertragene Kurztelegramme KT, die von ihrem Informationsgehalt gerade die Informationen eines Langtelegramms LT enthalten können. Werden also die übertragenen Daten von drei Kurztelegrammen KT wiederholt durch die streckenseitige Einrichtung SE2 gesendet, so kann in dem Übertragungsfenster REC der vollständige Informationsgehalt der streckenseitigen Einrichtung SE2 übertragen werden.

[0076] Dieses Beispiel dient lediglich exemplarisch der Verdeutlichung eines Übertragungsstandards und kann auch beliebig anders ausgeführt sein. Dieses Beispiel soll jedoch in der folgenden Figur 4 herangezogen werden, um eine Folge von verschlüsselten und unverschlüsselten Telegrammen in Bezug auf die Länge des Übertragungsfensters REC zu diskutieren.

[0077] Bei den Telegrammen T1, T2 handelt es sich mit Blick auf Figur 3 vorzugsweise um Kurztelegramme nach dem ETCS-Standard. Es können jedoch auch beliebige andere Telegramme übertragen werden, beispielsweise Langtelegramme LT, wenn das streckengebundene Fahrzeug FZ beispielsweise langsamer fährt, oder auch Telegramme eines anderen Übertragungsstandards.

[0078] In Figur 4 sind zwei Varianten V1 und V2 dargestellt für die gezielte verschlüsselte und unverschlüsselte Übertragung eines ersten Telegramms T1 und eines zweiten Telegramms T2. In der Variante V1 wird zuerst das erste Telegramm unverschlüsselt versendet (T1U) und dann das erste Telegramm verschlüsselt versendet (T1V). Anschließend wird das zweite Telegramm unverschlüsselt (T2U) und dann das zweite Telegramm verschlüsselt (T2V) versendet. Anschließend wird die beschriebene Folge wiederholt, wie dies in Figur 4 angegeben ist.

[0079] Wird jetzt, wie in Figur 3, davon ausgegangen, dass in dem Übertragungsfenster REC lediglich drei Telegramme vollständig übertragen werden können, so wird deutlich, dass das erste Telegramm verschlüsselt und unverschlüsselt, und das zweite Telegramm nur verschlüsselt übertragen wird. Wird die streckenseitige Einrichtung somit von einem nicht ausgerüsteten streckengebundenen Fahrzeug passiert, kann dieses den Inhalt des zweiten Telegramms T2 nicht verarbeiten, da keine Möglichkeit dafür besteht, dass zweite verschlüsselte Telegramm T2V zu entschlüsseln.

[0080] Für solche Fälle ist die Übertragungsfolge von Sequenzen gemäß der Variante V2 besser geeignet. Hier wird immer das erste Telegramm zuerst unverschlüsselt (T1U) und dann verschlüsselt (T1V) und dann das zweite Telegramm nur unverschlüsselt (T2U) übertragen und diese Sequenz anschließend wiederholt.

[0081] Es zeigt sich, dass das Übertragungsfenster REC nun ausreicht, um immer das erste Telegramm sowohl verschlüsselt als auch unverschlüsselt sowie das zweite Telegramm unverschlüsselt zu empfangen (wobei die Reihenfolge unterschiedlich sein kann). Ein nicht ausgerüstetes streckengebundenes Fahrzeug FZ kann daher auch ohne die Möglichkeit einer Entschlüsselung des ersten Telegramms T1 alle Daten decodieren und somit verarbeiten.

[0082] Allerdings wird die Möglichkeit eines gemischten Betriebs von ausgestatteten und nicht ausgestatteten streckengebundenen Fahrzeugen FZ dadurch erkauft, dass das zweite Telegramm nie verschlüsselt versendet wird und eine Fehleruntersuchung bzw. Untersuchung von Manipulationsversuchen nur mithilfe des ersten Telegramms T1 erfindungsgemäß erfolgen kann.

[0083] Es zeigt sich somit, dass die Wahl der Folge von Telegrammen (verschlüsselt, unverschlüsselt) in der Sequenz von dem betreffenden Einsatzfall abhängt und immer ein Kompromiss gefunden werden muss, eine möglichst hohe Sicherheit zu erlangen und dabei die technischen Gegebenheiten (ausgerüstete Fahrzeuge, nicht ausgerüstete Fahrzeuge, Länge der Übertragungsfenster REC, Geschwindigkeit der Fahrzeuge bei Überfahrt der streckenseitigen Einrichtung) zu berücksichtigen.

[0084] In Figur 5 ist der Verfahrensablauf bei der Übertragung der Telegramme als Flussdiagramm dargestellt. Das Verfahren beginnt mit einem Startschritt START und findet zunächst im Sender S statt. Dort wird nach einem Initialisierungsschritt INI eine Abfrage durchgeführt, ob ein hohes Sicherheitslevel SEC für das zu übertragende Telegramm gewählt werden soll. Ist dies der Fall, wird aus der Speichereinrichtung SP der Schlüssel KEY geladen und mit diesem in einem Verschlüsselungsschritt CRYP das Telegramm verschlüsselt. Anschließend wird das Telegramm in einem Codierungsschritt CODE codiert und über die Schnittstelle S1 an den Empfänger R gesendet.

[0085] In dem Empfänger R findet ein Decodierungsschritt DECO statt und anschließend unter Nutzung des Schlüssels KEY, der aus der Speichereinrichtung SP geladen wird, eine Decodierung DECR. Dort steht das Telegramm dann zur weiteren Verarbeitung zur Verfügung.

[0086] Die Speichereinrichtungen SP im Sender S und im Empfänger R sind unterschiedliche Speichereinrichtungen. Handelt es sich bei dem Sender um die streckenseitige Einrichtung SE2 gemäß Figur 2, könnte die Speichereinrichtung SP beispielsweise durch die Speichereinrichtung SP1 ausgebildet sein und die Speichereinrichtung im Empfänger die durch die Speichereinrichtung SP2.

[0087] Wird die Abfrage nach dem Sicherheitslevel SEC negativ beantwortet, so fallen bei der Übertragung, wie in Figur 5 dargestellt, der Verschlüsselungsschritt CRYP sowie der Entschlüsselungsschritt DECR weg. Es findet nur der Kodierungsschritt CODE, der Übertragungsschritt TRN und der Dekodierungsschritt DECO statt.

[0088] Im Sender S wird wiederholt eine Abfrage RECEND durchgeführt, ob die Übertragung beendet wurde. Ist dies der Fall, wird die Übertragung in einem Stoppschritt STOP abgebrochen. Ist dies nicht der Fall, wird erneut die Abfrage des Sicherheitslevels SEC für das nächste Telegramm durchgeführt.

Bezugszeichenliste

[0089]

FZ	streckengebundenes Fahrzeug
SE1 ... SE6	streckenseitige Einrichtung
GL	Gleis
FR	Fahrtrichtung
VB	Verband
A1 ... A2	Antenne
SP1 ... SP2	Speichereinrichtung
C1 ... C2	Computer
S1 ... S5	Schnittstelle
LT	Langtelegramm
KT	Kurztelegramm
T1 ... T2	Telegramm
T1U ... T2U	unverschlüsseltes Telegramm
T1V ... T2V	verschlüsseltes Telegramm
t	Zeit
REC	Übertragungsfenster
V1 ... V2	Variante
S	Sender
R	Empfänger
START	Startschritt
INI	Initialisierungsschritt
SEC	Abfrage des Sicherheitslevels
KEY	Schlüssel
CRYP	Verschlüsselungsschritt
CODE	Kodierungsschritt
TRN	Übertragungsschritt
DECO	Dekodierungsschritt
DECR	Entschlüsselungsschritt
RECEND	Abfrage des Endes der Übertragung
STOP	Stopschritt

Patentansprüche

1. Verfahren zur codierten Kommunikation zwischen einem streckengebundenem Fahrzeug (FZ) und einer streckenseitigen Einrichtung (SE1 ... SE6), bei der mehrere Telegramme (T1, T2) zwischen der streckenseitigen Einrichtung (SE1 ... SE6) und dem streckengebundenen Fahrzeug (FZ) übertragen werden, wobei die Telegramme (T1, T2) jeweils

- einen Nutzdatenbereich zum Befüllen mit Nutzdaten aufweisen,
- einen Codebereich für die Codierung der Nutzdaten aufweisen, **dadurch gekennzeichnet,**

dass mindestens eines der Telegramme (T1, T2) unverschlüsselt derart übertragen wird, dass

- der Nutzdatenbereich mit den unverschlüsselten Nutzdaten befüllt wird, wobei diese unter Nutzung des Codebereiches codiert werden,
- das Telegramm (T1, T2) mit den unverschlüsselten Nutzdaten codiert übertragen wird,
- die unverschlüsselten Nutzdaten nach der Übertragung unter Nutzung des Codebereiches decodiert werden,

und **dass** mindestens eines der Telegramme (T1, T2) verschlüsselt und codiert derart übertragen wird, dass

- die unverschlüsselten Nutzdaten vor dem Befüllen des Nutzdatenbereiches verschlüsselt werden,
- der Nutzdatenbereich mit den verschlüsselten Nutzdaten befüllt wird, wobei diese zusätzlich unter Nutzung des Codebereiches codiert werden,
- das Telegramm (T1, T2) mit den verschlüsselten Nutzdaten codiert übertragen wird,
- die verschlüsselten Nutzdaten nach der Übertragung des Telegramms (T1, T2) unter Nutzung des Codebereiches decodiert werden,
- danach die verschlüsselten Nutzdaten entschlüsselt werden.

2. Verfahren nach Anspruch 1
dadurch gekennzeichnet,
dass mindestens eines der mit unverschlüsselten Nutzdaten übertragenen Telegramme (T1, T2) auch als Telegramm mit verschlüsselten Nutzdaten des-

selben Inhalts übertragen wird.

3. Verfahren nach Anspruch 2,
dadurch gekennzeichnet,
dass

- zuerst die unverschlüsselten Nutzdaten nach der Übertragung unter Nutzung des Codebereiches decodiert werden.
- danach die verschlüsselten Nutzdaten nach der Übertragung des Telegramms (T1, T2) unter Nutzung des Codebereiches decodiert werden,
- danach die verschlüsselten Nutzdaten entschlüsselt werden.

4. Verfahren nach Anspruch 3,
dadurch gekennzeichnet,
dass

- zuerst das mindestens eine mit unverschlüsselten Nutzdaten übertragenen Telegramm (T1, T2),
- danach das Telegramm (T1, T2) mit den verschlüsselten Nutzdaten desselben Inhalts übertragen wird.

5. Verfahren nach einem der voranstehenden Ansprüche,
dadurch gekennzeichnet,
dass in wechselnder Reihenfolge Telegramme (T1, T2) mit verschlüsselten und unverschlüsselten Nutzdaten übertragen werden.

6. Verfahren nach Anspruch 5,
dadurch gekennzeichnet,
dass in einer Sequenz von Telegrammen (T1, T2) im Verhältnis mehr Telegramme (T1, T2) mit unverschlüsselten Nutzdaten als Telegramme (T1, T2) mit verschlüsselten Nutzdaten übertragen werden, wobei

- die Nutzdatenbereiche der unverschlüsselt übertragenen Telegramme (T1, T2) der Sequenz mit unterschiedlichen Inhalten befüllt sind,
- mindestens eines der mit unverschlüsselten Nutzdaten übertragenen Telegramme (T1, T2) der Sequenz auch als Telegramm (T1, T2) mit verschlüsselten Nutzdaten desselben Inhalts übertragen wird.

7. Verfahren nach Anspruch 1,
dadurch gekennzeichnet,
dass die Nutzdaten eines verschlüsselt gesendeten Telegramms (T1, T2) nach dem Entschlüsseln (DECR) mit den Nutzdaten eines unverschlüsselt gesendeten Telegramms (T1, T2) desselben Inhalts vor und/oder nach dem Dekodieren (DECO) miteinander verglichen werden.

8. Verfahren nach Anspruch 7,
dadurch gekennzeichnet,
dass in dem Fall, dass das Vergleichen ergibt, dass die Nutzdaten des verschlüsselt gesendeten Telegramms (T1, T2) von den Nutzdaten des unverschlüsselt gesendeten Telegramms (T1, T2) desselben Inhalts, abweicht, ein Fehlersignal generiert und/oder ausgegeben wird.

9. Verfahren nach einem der voranstehenden Ansprüche,
dadurch gekennzeichnet,
dass mehrere Telegramme (T1, T2) mit unterschiedlich großen Nutzdatenbereichen übertragenen werden.

10. Verfahren nach einem der voranstehenden Ansprüche,
dadurch gekennzeichnet,
dass die Schritte, dass

- der Nutzdatenbereich mit den verschlüsselten Nutzdaten befüllt wird, wobei diese zusätzlich unter Nutzung des Codebereiches codiert werden,
- das Telegramm (T1, T2) mit den verschlüsselten Nutzdaten codiert übertragen wird,
- die verschlüsselten Nutzdaten nach der Übertragung des Telegramms (T1, T2) unter Nutzung des Codebereiches decodiert werden,

oder

- der Nutzdatenbereich mit den unverschlüsselten Nutzdaten befüllt wird, wobei diese unter Nutzung des Codebereiches codiert werden,
- das Telegramm (T1, T2) mit den unverschlüsselten Nutzdaten codiert übertragen wird,
- die unverschlüsselten Nutzdaten nach der Übertragung unter Nutzung des Codebereiches decodiert werden,

nach dem ETCS-Standard oder dem ERTMS-Standard oder dem CBTC-Standard oder dem PTC-Standard durchgeführt werden.

11. Verfahren nach einem der voranstehenden Ansprüche,
dadurch gekennzeichnet,
dass die Übertragung zwischen einer Balise als streckenseitige Einrichtung (SE1 ... SE6) und dem streckengebundenen Fahrzeug (FZ) stattfindet.

12. Verfahren nach Anspruch 11,
dadurch gekennzeichnet,
dass geprüft wird, ob die Balise zu einem Balisenverband (VB) gehört, wobei die empfangenen Daten dann als vertrauenswürdig eingestuft werden.

13. Spurgebundenes Fahrzeug (FZ) mit einer Kommunikationsschnittstelle (S1) für eine streckenseitige Einrichtung (SE1 ... SE6),
dadurch gekennzeichnet,
dass dieses dafür eingerichtet ist, an einem Verfahren zur codierten Kommunikation gemäß einem der voranstehenden Ansprüche teilzunehmen.

14. Streckenseitige Einrichtung (SE1 ... SE6) mit einer Kommunikationsschnittstelle (S1) für eine streckengebundenes Fahrzeug (FZ),
dadurch gekennzeichnet,
dass diese dafür eingerichtet ist, an einem Verfahren zur codierten Kommunikation gemäß einem der Ansprüche 1 - 12 teilzunehmen.

15. Computerprogrammprodukt mit Programmbefehlen zur Durchführung des Verfahrens nach einem der Ansprüche 1 - 12.

16. Bereitstellungsvorrichtung für das Computerprogrammprodukt nach dem letzten voranstehenden Anspruch, wobei die Bereitstellungsvorrichtung das Computerprogrammprodukt speichert und/oder bereitstellt.

FIG 1

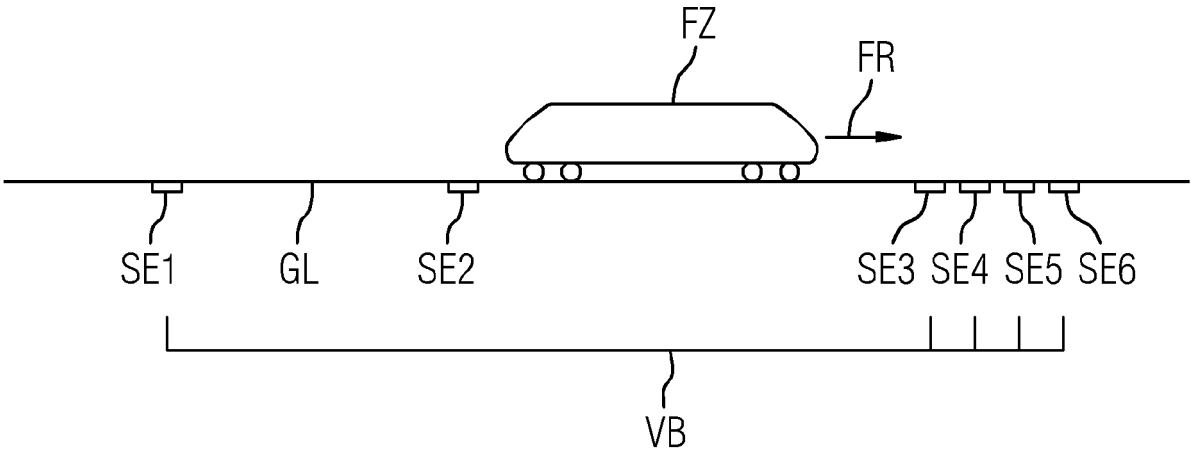

FZ
FR
SE1
GL
SE2
SE3
SE4
SE5
SE6
VB

FIG 2

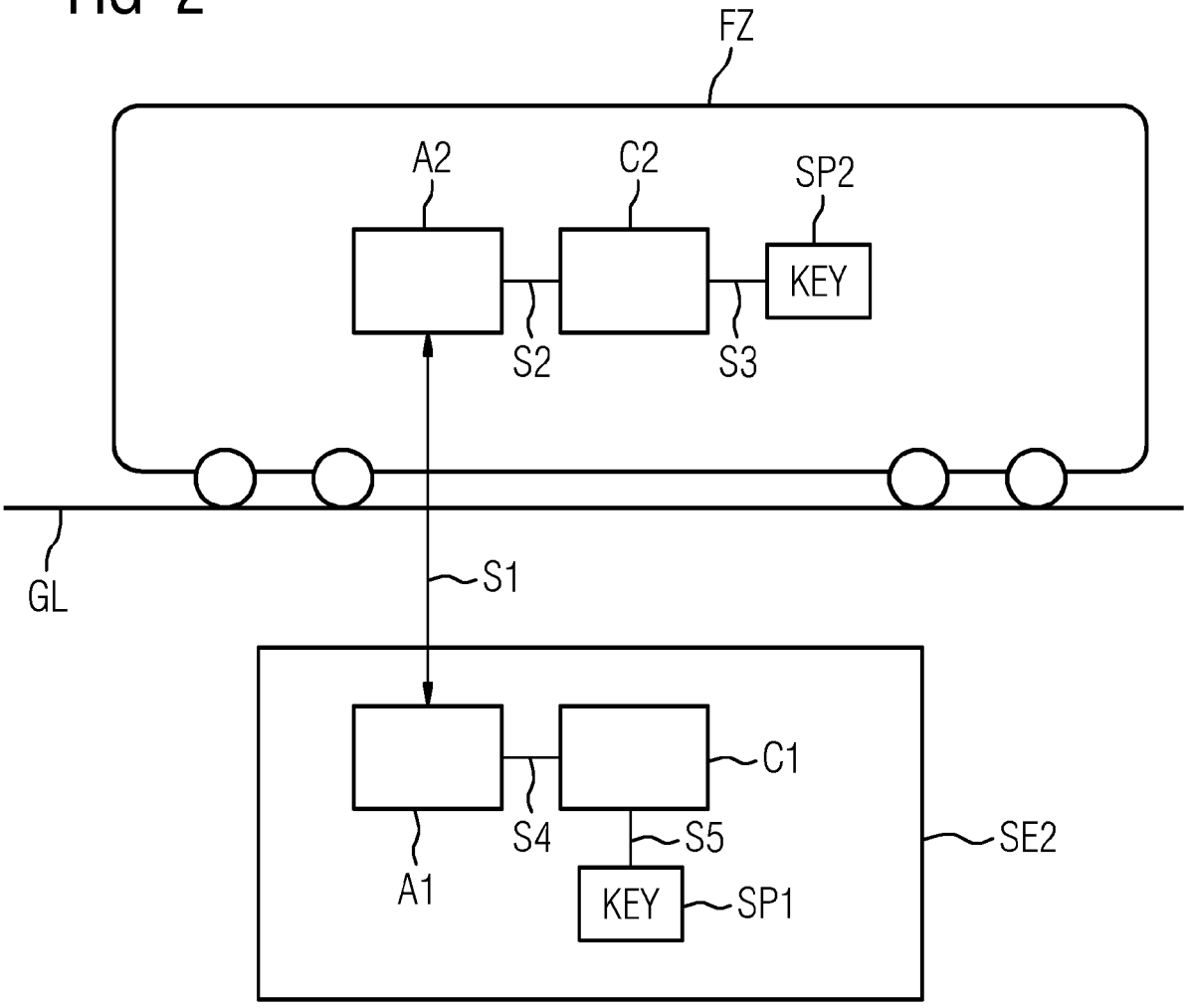

FZ
A2
C2
SP2
KEY
S2
S3
GL
S1
C1
S4
S5
SE2
A1
KEY
SP1

FIG 3

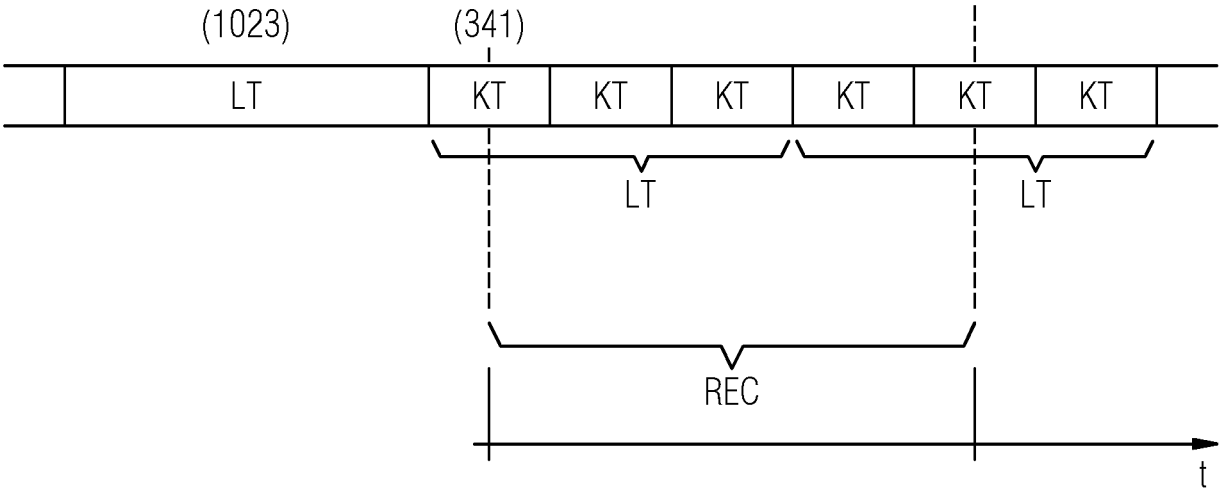

(1023)
(341)
LT
KT
KT
KT
KT
KT
KT
LT
LT
REC
t

FIG 4

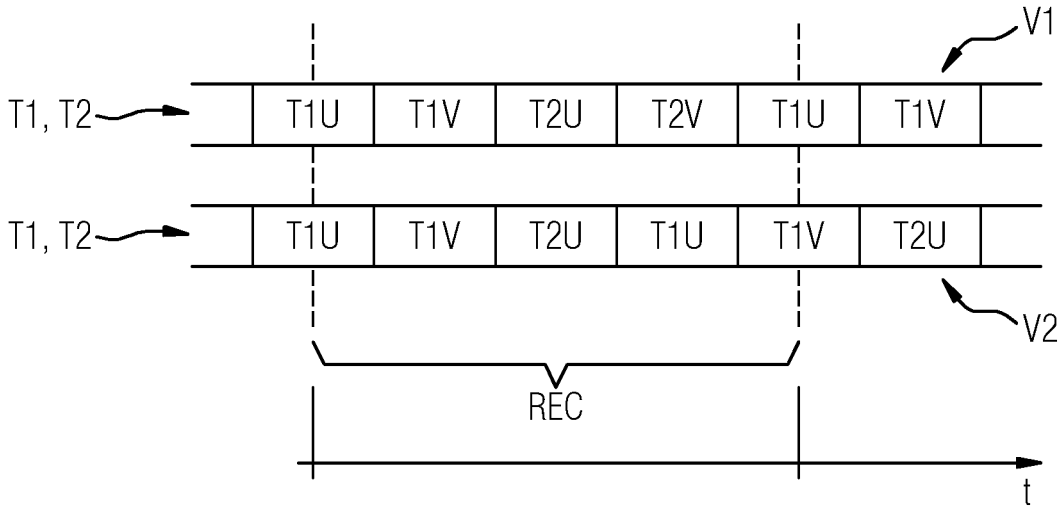
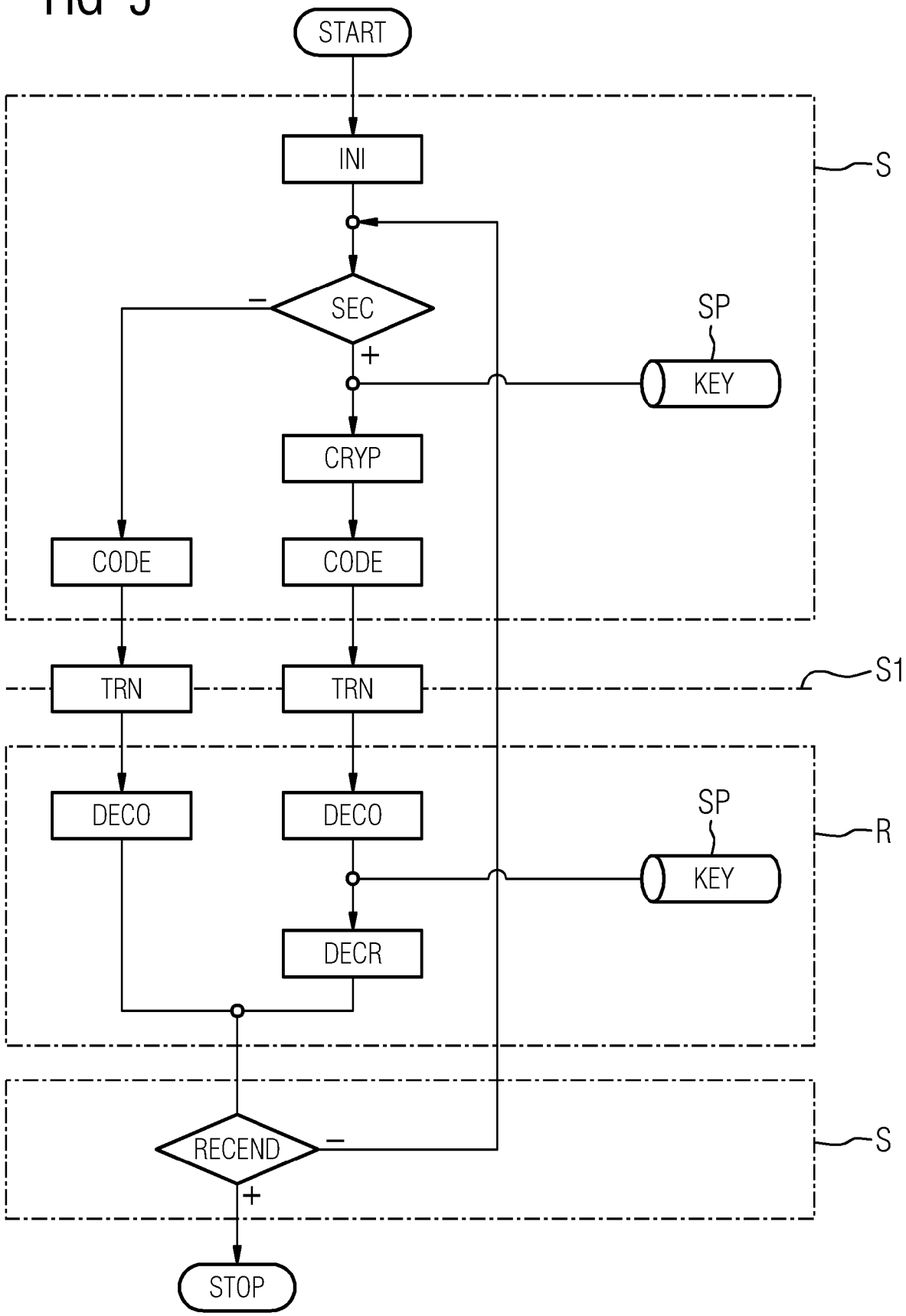

V1
T1, T2
T1U
T1V
T2U
T2V
T1U
T1V
T1, T2
T1U
T1V
T2U
T1U
T1V
T2U
V2
REC
t

FIG 5


START
INI
S
SEC
−
+
SP
KEY
CRYP
CODE
CODE
TRN
TRN
S1
DECO
DECO
SP
KEY
R
DECR
RECEND
−
+
S
STOP

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 21 15 4235

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (IPC)
X	GUO HUAQUN ET AL: "Protecting Train Balise Telegram Data Integrity", 2018 21ST INTERNATIONAL CONFERENCE ON INTELLIGENT TRANSPORTATION SYSTEMS (ITSC), IEEE, 4. November 2018 (2018-11-04), Seiten 806-811, XP033470223, DOI: 10.1109/ITSC.2018.8569616 ISBN: 978-1-7281-0321-1 [gefunden am 2018-12-07] * Abschnitte II und III * * Zusammenfassung; Abbildungen 2, 3,4,5 *	1,5-16	INV. B61L3/12 B61L15/00
A	WO 2019/166182 A1 (SIEMENS AG [DE]) 6. September 2019 (2019-09-06) * Seite 1, Zeile 7 - Seite 2, Zeile 36 *	1-16	
A	EP 3 219 575 A1 (ALSTOM TRANSP TECH [FR]) 20. September 2017 (2017-09-20) * Absätze [0001] - [0018] *	1-16	
A	DE 10 2016 204630 A1 (SIEMENS AG [DE]) 21. September 2017 (2017-09-21) * Absätze [0001] - [0010], [0036] - [0044]; Abbildung 1 *	1-16	RECHERCHIERTE SACHGEBIETE (IPC) B61L

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
München	12. Juli 2021	Robinson, Victoria

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 21 15 4235

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.

12-07-2021

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 2019166182 A1	06-09-2019	CN 111869160 A	30-10-2020
		DE 102018203072 A1	05-09-2019
		EP 3747152 A1	09-12-2020
		US 2021067327 A1	04-03-2021
		WO 2019166182 A1	06-09-2019
EP 3219575 A1	20-09-2017	KEINE	
DE 102016204630 A1	21-09-2017	DE 102016204630 A1	21-09-2017
		WO 2017162386 A1	28-09-2017

EPO FORM P0461

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