(19) Deutsches Patent- und Markenamt

(10) **DE 10 2012 206 272 A1** 2013.10.17

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2012 206 272.6**
(22) Anmeldetag: **17.04.2012**
(43) Offenlegungstag: **17.10.2013**

(51) Int Cl.: ***H04L 9/00*** (2012.01)
G06F 13/00 (2012.01)

(71) Anmelder:
Beckhoff Automation GmbH, 33415, Verl, DE

(74) Vertreter:
Wilhelm & Beck, 80639, München, DE

(72) Erfinder:
Wieczorek, Felix, 81679, München, DE; Schiller, Frank, Prof. Dr., 90409, Nürnberg, DE

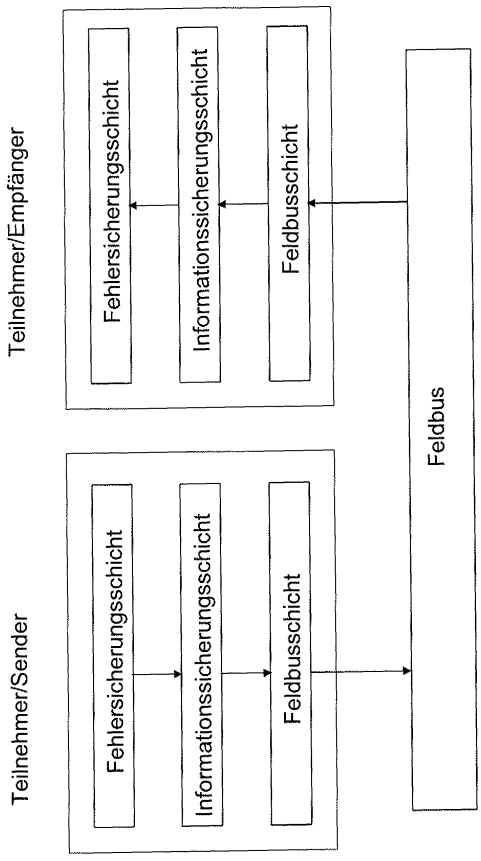
(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:

DE 10 2010 033 229 A1
US 2003 / 0 223 585 A1
US 2007 / 0 061 674 A1

Prüfungsantrag gemäß § 44 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Feldbus-Datenübertragung**



(57) Zusammenfassung: Zum Übertragen von Informationen in einem Feldbussystem zwischen wenigstens zwei Kommunikationsteilnehmern, die jeweils eine Sicherheitsschicht mit einer Fehlersicherungsschicht, die Daten gegen Datenübertragungsfehler sichert, und einer Informationssicherheitsschicht, die gegen Manipulation und/oder unautorisiertes Lesen von Daten sichert, aufweisen, durchlaufen die zu übertragenen Daten in sendenden Kommunikationsteilnehmern zuerst die Fehlersicherungsschicht und dann die Informationssicherheitsschicht und in empfangenden Kommunikationsteilnehmern zuerst die Informationssicherheitsschicht und dann die Fehlersicherungsschicht.

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zum Übertragen von Informationen in Form von Datenpaketen in einem Feldbussystem zwischen wenigstens zwei Kommunikationsteilnehmern, einen Kommunikationsteilnehmer für ein solches Feldbussystem und das Feldbussystem als solches.

[0002] In der Industrieautomation werden technische Prozesse mit Hilfe von Rechnern gesteuert und überwacht. Die Feldgeräte, d.h. die Sensoren und Aktoren, sind mit Steuerungsrechnern über einen Feldbus kommunikationstechnisch verbunden. Der Feldbus ist in der Regel echtzeitfähig.

[0003] Eine wesentliche Anforderung an Feldbussysteme ist die Fehlersicherheit bei der Übertragung von Informationen zwischen Feldgeräten und Steuerungsrechnern. In der Industrieautomation muss beim Steuern und Überwachen von technischen Prozessen sichergestellt sein, dass dann, wenn das Feldbussystem fehlerhaft arbeitet, keine Gefahr für Mensch und Umwelt besteht. Feldbussysteme arbeiten deshalb in der Regel nach dem sogenannten Fail-Safe-Prinzip, gemäß dem das Feldbussystem im Fehlerfall wichtiger Komponenten in einen sicheren Zustand übergeht. Um beim Ausführen solcher sicherheitsrelevanter Steuerfunktionen zu gewährleisten, dass der Datenaustausch zwischen den Feldgeräten und den Steuerungsrechnern nicht verfälscht oder zumindest erkennbar verfälscht erfolgt, werden sogenannte Safety-Maßnahmen auf dem Feldbus implementiert. Zielsetzung der hierbei ergriffenen Safety-Maßnahmen ist es, Fehler bei der Nutzdatenübertragung mit hoher Wahrscheinlichkeit aufzudecken, um die Gefahr unerkannter Fehler zu minimieren. Im Fokus dieser Safety-Maßnahmen stehen dabei vor allem die zufälligen Fehler, die bei der Datenübertragung auftreten.

[0004] Als Safety-Maßnahme führen die Kommunikationsteilnehmer im Feldbussystem in der Regel ein Prüfsummenverfahren (z. B. Cyclic Redundancy Check – CRC) durch, bei dem vor einer Datenübertragung aus den Nutzdaten eine Prüfsumme berechnet wird, die dann in einem Datenpaket, beispielsweise zusammen mit den Nutzdaten, übertragen wird. Zur Überprüfung einer fehlerfreien Datenübertragung wird auf der Empfängerseite ein entsprechendes Berechnungsverfahren auf die empfangenen Nutzdaten und die empfangenen Prüfsumme angewandt. Dem Berechnungsergebnis kann dann entnommen werden, ob die Datenübertragung unverfälscht stattgefunden hat.

[0005] Neben der Notwendigkeit zur Aufdeckung zufälliger Fehler bei der Datenübertragung tritt zunehmend auch die Problemstellung auf, die Integrität der im Feldbussystem übertragenen Information gegen Angriffe zu sichern. Zielsetzung solcher sogenannter Security-Maßnahmen ist es, vor allem die Information vor unautorisierten Änderungen zu schützen. Ferner sollen mit weiteren Security-Maßnahmen oft zusätzlich die Vertraulichkeit der Daten vor unautorisiertem Lesen sichergestellt werden. Dabei werden in der Regel kryptographische Verfahren eingesetzt, um die Informationssicherheit in Bezug auf Angriffe zu gewährleisten. Um in Feldbussystemen zwischen den Kommunikationsteilnehmern für einen schnellen Datenaustausch zum Ausführen von Echtzeitsteueraufgaben zu sorgen, können symmetrische kryptographische Verfahren eingesetzt werden, bei denen mehrere Kommunikationsteilnehmer den gleichen Schlüssel verwenden.

[0006] Bei Feldbussystemen werden üblicherweise aufgrund der unterschiedlichen Zielsetzungen von Fehlersicherheit und Informationssicherheit die Safety- bzw. Security-Maßnahmen unabhängig voneinander entwickelt und umgesetzt. Bei einer Kombination von Safety- und Security-Verfahren besteht jedoch das Problem, dass die Vorgehensweisen sich gegenseitig beeinflussen und zu nicht vollständigem Erreichen der Schutzziele führen können. Bei Safety-Maßnahmen in Feldbussystemen wird in der Regel das sogenannte Black-Channel-Prinzip angewandt, bei dem die Kommunikationsteilnehmer jeweils eine Fehlersicherungsschicht besitzen, die das Übertragungsverhalten auf dem Feldbus und gegebenenfalls auf dem Feldbus ausgeführte Security-Maßnahmen völlig unberücksichtigt lassen, was dazu führt, dass eventuell Beeinträchtigungen der Güte nicht adäquat in den Nachweisen berücksichtigt werden.

[0007] Bei der Fehlerbetrachtung im Rahmen von Safety-Maßnahmen wird der Feldbus ferner als binärer symmetrischer Kanal angesehen, auf dem die Zeichen unabhängig voneinander und mit der gleichen Wahrscheinlichkeit verfälscht werden, so dass die Wahrscheinlichkeit einer Falschübertragung des Zeichens 1 genauso hoch ist wie die Falschübertragung des Zeichens 0. Eine Security-Schicht, in der die Daten ver- bzw. entschlüsselt werden, verändert jedoch den Kommunikationskanal so, dass die Annahme vom binären symmetrischen Kanal nicht mehr ohne weiteres zutrifft. Da bei einer Verschlüsselung in der Regel eine pseudozufällige Gleichverteilung der verschlüsselten Daten angestrebt wird, kann das Problem auftreten, dass die bei Safety-Maßnahmen geforderten deterministischen Kriterien wie z. B. die Hamming-Distanz nicht mehr eingehalten werden. Die Hamming-Distanz gibt an, wieviele Zeichen in einem Datensatz mindestens verfälscht sein müssen, damit bezüglich der Safety-Maßnahmen eine unerkannte Verfälschung überhaupt auftreten kann.

[0008] In Feldbussystemen muss eine Durchgängigkeit der Safety-Maßnahmen im Feldbussystem vom Sender zum Empfänger gewährleistet sein. Wenn

beim Senden die Security-Maßnahmen vor den Safety-Maßnahmen in den Kommunikationsteilnehmern des Feldbussystems ausgeführt werden, müssten deshalb diese Security-Maßnahmen zum Gewährleisten einer Fehlersicherheit durch weitere Safety-Maßnahmen, z. B. zusätzliche Redundanzen, gesichert werden. Es besteht grundsätzlich nicht die Möglichkeit, mit den Safety-Maßnahmen zusätzlich die Security-Anforderungen zu erfüllen bzw. umgekehrt mit den Security-Maßnahmen die Safety-Anforderungen umzusetzen. Safety-Maßnahmen, bei denen für die Nutzdaten eine Prüfsumme bestimmt wird, die übertragen und beim Empfänger verifiziert wird, könnten zwar eine Manipulation der übertragenen Daten erschweren. Eine Anpassung der Prüfsumme an manipulierte Nutzdaten ist für einen Angreifer jedoch in der Regel immer noch möglich, so dass mit den Safety-Maßnahmen die Security-Anforderungen nicht erfüllt werden können. Umgekehrt kann versucht werden, die Safety-Anforderungen mit Security-Maßnahmen zu erfüllen, weil auch zufällige Fehler mit einer bestimmten Wahrscheinlichkeit aufgedeckt werden. Diese Security-Maßnahmen genügen jedoch nicht den Safety-Anforderungen, da die deterministischen Fehleraufdeckungskriterien nicht erfüllt werden.

[0009] Aufgabe der Erfindung ist es, auf einfache Weise bei Feldbussystemen sowohl Safety- als auch Security-Anforderungen zu erfüllen.

[0010] Diese Aufgabe wird mit einem Verfahren gemäß Anspruch 1, einen Kommunikationsteilnehmer gemäß Anspruch 7 und einem Feldbussystem gemäß Anspruch 13 gelöst. Bevorzugte Weiterbildungen sind in den abhängigen Ansprüchen angegeben.

[0011] Erfindungsgemäß wird zum Übertragen von Information in Form von Datenpaketen in einem Feldbussystem zwischen wenigstens zwei Kommunikationsteilnehmern, die jeweils eine Sicherheitsschicht mit einer Fehlersicherungsschicht, die Daten gegen Datenübertragungsfehler sichert, und einer Informationssicherungsschicht, die Daten gegen Manipulation und/oder unautorisiertes Lesen sichert, aufweisen, im Sendebetrieb der Kommunikationsteilnehmer die Daten im Kommunikationsteilnehmer zuerst in der Fehlersicherungsschicht und dann in der Informationssicherungsschicht und im Empfangsbetrieb zuerst in der Informationssicherungsschicht und dann in der Fehlersicherungsschicht verarbeitet.

[0012] Mit dieser erfindungsgemäßen Vorgehensweise, bei der die Safety- und Security-Maßnahmen als zwei getrennte Schichten ausgeführt sind, die im Kommunikationsteilnehmer im Sendevorgang der Feldbus-Protokollschicht vorgeschaltet bzw. im Empfangsbetrieb dieser Protokollschicht nachgeschaltet sind, können robust sowohl die Safety-Anforderungen, Datenübertragungsfehler mit hoher Wahrscheinlichkeit aufzudecken, als auch die Security-Anforderungen, Manipulationen an den Daten festzustellen und/oder unautorisiertes Lesen zu verhindern, erfüllt werden. Durch das Vorsehen der Fehlersicherungsschicht am Anfang bzw. am Ende der Datenübertragungsstrecke kann die Durchgängigkeit der Safety-Maßnahmen sichergestellt werden. Durch das direkte Nachschalten der Informationssicherungsschicht im Sendebetrieb bzw. des direkten Vorschaltens der Informationssicherungsschicht im Empfangsbetrieb können bei der Auslegung der Security-Maßnahmen die Safety-Anforderungen berücksichtigt werden.

[0013] Die erfindungsgemäße Auslegung der Kommunikationsteilnehmer hat ferner den Vorteil, dass die Daten in der Fehlersicherungsschicht und in der Informationssicherungsschicht schnell und ressourcensparend verarbeitet werden, wodurch sich die Echtzeitfähigkeit des Feldbussystems garantieren lässt. Gleichzeitig erlaubt die vorgesehene Architektur einen flexiblen Austausch der im Rahmen der Safety- bzw. Security-Maßnahmen eingesetzten Verarbeitungsprozesse, wodurch sich die geforderten Safety- und Security-Maßnahmen einfach und schnell an neue Anforderungen anpassen lassen.

[0014] Gemäß einer bevorzugten Ausführungsform bestimmt die Fehlersicherungsschicht des sendenden Kommunikationsteilnehmers für die Nutzdaten eine Prüfsumme, wobei die Fehlersicherungsschicht im empfangenden Kommunikationsteilnehmer eine entsprechende Berechnung auf die Daten anwendet. Mit dieser Vorgehensweise kann die Datenintegrität in Bezug auf die Aufdeckung von zufälligen Fehlern bei der Datenübertragung nachweisbar gewährleistet werden. Insbesondere lassen sich mit dieser Vorgehensweise auf einfache Weise die Safety-Anforderungen hinsichtlich der Restfehlerwahrscheinlichkeit und deterministischer Kriterien wie die Hamming-Distanz erfüllen.

[0015] Gemäß einer weiteren bevorzugten Ausführungsform erzeugt die Informationssicherungsschicht des zu sendenden Kommunikationsteilnehmers für die zu übertragenen Daten und für einen vorgegebenen Schlüssel und/oder einen internen Zustand nach einem vorgegebenen Authentifikation-Berechnungsverfahren einen Authentifikationsprüfwert, der ebenfalls übertragen wird, wobei die Informationssicherungsschicht des empfangenen Kommunikationsteilnehmers für die empfangenen Daten einen weiteren Authentifikationsprüfwert berechnet, um durch Vergleich des weiteren Authentifikationsprüfwerts mit dem übertragenen Authentifikationsprüfwert eine Aussage über die Datenintegrität zu treffen. Mit dieser Vorgehensweise wird mit ausreichend hoher Wahrscheinlichkeit eine Datenintegrität in Bezug auf die Aufdeckung von Datenmanipulationen erreicht. Mit dieser Vorgehensweise wird außerdem der

Empfang von Daten in der selben Reihenfolge, wie sie gesendet wurden, mit ausreichend hoher Wahrscheinlichkeit sichergestellt. Dadurch werden unter anderem ein Löschen und/oder ein Wiedereinspielen von Daten erkannt. Gleichzeitig können die Security-Maßnahmen mit den Safety-Maßnahmen kombiniert werden, ohne dass die Güte der Safety-Maßnahmen davon beeinflusst wird. Die Restfehlerwahrscheinlichkeit und die deterministischen Kriterien, wie Hamming-Distanz, bleiben durch die Maßnahmen der Informationssicherungsschicht unbeeinflusst.

[0016] Gemäß einer weiteren bevorzugten Ausführungsform umfasst die Informationssicherungsschicht eine Vertraulichkeitssicherungsschicht, mit der die Vertraulichkeit der Daten garantiert wird. Durch das Vorsehen dieser zusätzlichen Vertraulichkeitsschicht im Rahmen der Informationssicherungsschicht kann eine zusätzliche Sicherung der Daten gegenüber unautorisiertem Lesen erreicht werden. Gleichzeitig bleibt die Verarbeitung in der Fehlersicherungsschicht durch diese zusätzliche Vertraulichkeitssicherungsschicht unbeeinflusst, so dass die Safety-Anforderungen weiterhin erfüllt bleiben.

[0017] Die Vertraulichkeitssicherungsschicht des sendenden Kommunikationsteilnehmers führt vorzugsweise eine Exklusiv-Oder-Überlagerung (XOR) der Daten mit einem pseudozufälligen Schlüsselstrom durch, wobei die Vertraulichkeitssicherungsschicht des empfangenden Kommunikationsteilnehmers wieder eine XOR-Überlagerung der empfangenen Daten mit demselben Schlüsselstrom durchführt. Dieses symmetrische Vorgehen bei der Verschlüsselung ermöglicht eine schnelle und ressourcensparende Verarbeitung, wodurch die Echtzeitfähigkeit des Feldbussystems nicht beeinflusst wird. Vorzugsweise wird dabei zum Bestimmen des Authentifikationsprüfwerts eine Partition desselben Schüsselstroms verwendet, die sich nicht mit der Partition des Schlüsselstroms überdeckt, die im Rahmen der Vertraulichkeitssicherungsschicht genutzt wird, was den Schlüsselaustausch zwischen den Kommunikationsteilnehmern vereinfacht und eine schnelle Verarbeitung ermöglicht.

[0018] Die Erfindung wird anhand der beigefügten Zeichnungen näher erläutert.

[0019] Fig. 1 zeigt schematisch im Modell den Aufbau eines erfindungsgemäßen Feldbussystems mit zwei Kommunikationsteilnehmern; und

[0020] Fig. 2 eine Datenübertragung bei dem in Fig. 1 gezeigten Feldbussystem mit dabei beispielhaft durchgeführten Safety- und Security-Maßnahmen.

[0021] Moderne Konzepte der Industrieautomation, d.h. der Steuerung und Überwachung von technischen Prozessen mit Hilfe von Software, beruhen auf der Idee einer Steuerung mit einer verteilten Sensor-/Aktor-Ebene. Die Kommunikationsteilnehmer kommunizieren dabei untereinander und mit übergeordneten Systemen über lokale Kommunikationsnetzwerke. Die in der Industrieautomation eingesetzten Netzwerke sind in der Regel Feldbussysteme, bei denen die Feldgeräte, d.h. die Sensoren und Aktoren, mit Steuerungsrechnern über einen gemeinsamen Übertragungsweg verbunden sind. Das Übertragungsnetzwerk kann dabei in unterschiedlicher Topologie, z.B. als Ring-, Stern-, Linien- oder Baumtopologie ausgeführt sein.

[0022] Moderne Feldbussysteme nutzen Protokolle, die ein Echtzeitverhalten aufweisen, und erzielen kurze Zykluszeiten mit niedrigem Jitter bei der Anlagensteuerung. Zentrale Anforderung an die Feldbussysteme ist eine sichere und zuverlässige Datenübertragung. Beim Einsatz von Feldbussystemen zur Steuerung und Überwachung von Maschinen ist eine sichere und zuverlässige Datenübertragung zwischen den Steuerungsrechnern und den Feldgeräten, d.h. den Sensoren und Aktoren, zu gewährleisten. So muss sichergestellt werden, dass die Information, repräsentiert durch Nutzdaten, zwischen den Kommunikationsteilnehmern im Feldbussystem ohne Fehler übertragen oder dass Fehler erkannt werden. Hierzu sind im Feldbussystem Safety-Maßnahmenvorgesehen, die gewährleisten, dass Fehler, insbesondere zufällige Fehler, mit hoher Wahrscheinlichkeit entdeckt werden, d.h. eine geringe Restfehlerwahrscheinlichkeit verbleibt. Dabei soll auch mit den Safety-Maßnahmen erreicht werden, dass bestimmte Fehlermuster zuverlässig detektiert werden, um so u. a. eine vorbestimmte Hamming-Distanz einhalten zu können, die die Anzahl an Zeichen angibt, die mindestens verfälscht sein müssen, damit ein verfälschter Datensatz existiert, der nicht als fehlerhaft erkannt wird.

[0023] Zusätzlich muss bei Feldbussystemen auch sichergestellt sein, dass unautorisiertes Lesen der übertragenen Informationen und/oder eine Manipulation dieser Informationen verhindert wird. Die hierbei in Feldbussystemen eingesetzten Security-Maßnahmen verhindern unautorisiertes Lesen der übertragenen Informationen und/oder eine Manipulation dieser Informationen durch Anwendung kryptographischer Verfahren auf die zwischen den Kommunikationsteilnehmern im Feldbussystem übertragenen Daten.

[0024] Bei der Durchführung von Safety- und Security-Maßnahmen im Feldbussystem kann das Problem bestehen, dass aufgrund der unterschiedlichen Anforderungen an die Datenintegrität, d.h. bei den Safety-Maßnahmen das Aufdecken von Datenübertragungsfehlern und bei den Security-Maßnahmen das Aufdecken von Datenmanipulationen und/oder unautorisiertes Lesen, die eingesetzten Maßnahmen

sich gegenseitig in ihrer Wirksamkeit einschränken. Um dies zu verhindern, wird im Feldbussystem ein Aufbau gewählt, bei dem die physikalische Übertragungsschicht des Feldbusses in den angeschlossenen Kommunikationsteilnehmern über eine Sicherungsschicht an die Anwendung angebunden ist. Dieser Sicherungsschicht unterlagert ist eine Feldbusschicht, die den Zugriff auf das Übertragungsmedium regelt und den Datenstrom in Datenpakete gemäß dem eingesetzten Protokoll umsetzt. Über der Feldbusschicht ist als erster Teil der Sicherungsschicht eine Informationssicherungsschicht, die die Security-Maßnahmen ausführt, vorgesehen und als zweiter Teil eine Fehlersicherungsschicht, die die Safety-Maßnahmen enthält.

[0025] Bei einer Übertragung von Nutzdaten im Feldbussystem zwischen den Kommunikationsteilnehmern durchlaufen die Nutzdaten, wie in Fig. 1 gezeigt, im Sender zuerst die Fehlersicherungsschicht und dann die Informationssicherungsschicht, um dann in der Feldbusschicht vom entsprechenden Feldbusprotokoll in Datenpakete umgesetzt und auf den Feldbus ausgegeben zu werden. Im Empfänger durchlaufen die Daten dann die Schichten in umgekehrte Reihenfolge. Die empfangenen Datenpakete der Feldbusschicht werden an die Informationssicherungsschicht weitergegeben, die nach Anwendung der Security-Maßnahmen die Daten dann zur Weiterverarbeitung an die Fehlersicherungsschicht, die die Safety-Maßnahmen durchführt, übergibt.

[0026] Die Entkopplung von Safety- und Security-Maßnahmen durch eine getrennte Verarbeitung in unabhängigen Schichten, nämlich der Fehlersicherungsschicht und der Informationssicherungsschicht, sorgt dafür, dass die Maßnahmen unabhängig voneinander durchgeführt werden können. Zugleich können die Safety- bzw. Security-Maßnahmen flexibel ausgetauscht und an neue Anforderungen angepasst werden.

[0027] Die vorgesehene Verarbeitungsreihenfolge im Sender, zuerst das Ausführen der Safety-Maßnahmen und dann der Security-Maßnahmen, und im Empfänger zuerst das Ausführen der Security-Maßnahmen und dann der Safety-Maßnahmen, sorgt für eine Durchgängigkeit der Safety-Maßnahmen, wodurch die Restfehlerwahrscheinlichkeit und die deterministischen Kriterien, wie Hamming-Distanz, eingehalten werden können.

[0028] In Bezug auf den in der Fehlersicherungsschicht eingesetzten Safety-Maßnahmen bzw. den in der Informationssicherungsschicht eingesetzten Security-Maßnahmen besteht grundsätzlich keine weitere Einschränkung. Als Safety-Maßnahme wird vorzugsweise ein Prüfsummenverfahren eingesetzt. Zur Erkennung von Übertragungsfehlern wird eine Prüfsumme aus den Nutzdaten berechnet. Ein solches Verfahren ist beispielsweise der CRC. Die Berechnung der Prüfsumme erfolgt beim CRC auf Basis einer Polynomdivision. Die Bitfolge der zu übertragenden Nutzdaten wird als binäres Polynom betrachtet, das durch ein Generatorpolynom geteilt wird, wobei ein Rest verbleibt. Dieser Rest ist dann die Prüfsumme, die beispielsweise an die Nutzdaten angehängt wird. Um zu verifizieren, ob eine fehlerfreie Datenübertragung erfolgt ist, werden die empfangenen Daten inklusive der Prüfsumme wiederum als binäres Polynom interpretiert und durch dasselbe Generatorpolynom wie beim Sender geteilt. Wenn sich der Rest 0 ergibt, wird davon ausgegangen, dass eine fehlerfreie Übertragung vorlag. Es gibt weitere Prüfsummenverfahren wie beispielsweise Längs- und Querparität, arithmetische Quersumme, mehrfaches Senden von Daten.

[0029] In der Informationssicherungsschicht werden bevorzugt symmetrische kryptographische Verfahren eingesetzt. Dabei wird in der Regel eine Stromverschlüsselung verwendet, bei der eine pseudozufällige Zeichenfolge, die aus dem vorgegebenen Schlüssel abgeleitet wird, erzeugt wird. Die Stromverschlüsselung eignet sich insbesondere für eine Echtzeitübertragung.

[0030] Gegen Manipulation erzeugt die Informationssicherungsschicht des zu sendenden Kommunikationsteilnehmers für die zu sendenden Daten und für einen vorgegebenen Schlüssel und/oder einen internen Zustand nach einem vorgegebenen Authentifikation-Berechnungsverfahren einen Authentifikationsprüfwert, der ebenfalls übertragen wird, wobei die Informationssicherungsschicht des empfangenen Kommunikationsteilnehmers für die empfangenen Daten einen weiteren Authentifikationsprüfwert berechnet, um durch Vergleich des weiteren Authentifikationsprüfwerts mit dem übertragenen Authentifikationsprüfwert eine Aussage über die Datenintegrität zu treffen. Mit dieser Vorgehensweise wird mit ausreichend hoher Wahrscheinlichkeit eine Datenintegrität in Bezug auf die Aufdeckung von Datenmanipulationen erreicht. Mit dieser Vorgehensweise wird außerdem der Empfang von Daten in derselben Reihenfolge, wie sie gesendet wurden, mit ausreichend hoher Wahrscheinlichkeit sichergestellt. Dadurch werden unter anderem ein Löschen und/oder ein Wiedereinspielen von Daten erkannt. Gleichzeitig können die Security-Maßnahmen mit den Safety-Maßnahmen genutzt werden, ohne dass die Güte der Safety-Maßnahmen davon beeinflusst wird. Die Restfehlerwahrscheinlichkeit und die deterministischen Kriterien, wie Hamming-Distanz, bleiben durch die Maßnahmen der Informationssicherungsschicht unbeeinflusst.

[0031] Die Informationssicherungsschicht kann zweiteilig ausgelegt sein, mit einer zusätzlichen Vertraulichkeitsschicht, die vorzugsweise eine Exklu-

siv-Oder-Überlagerung (XOR) der Daten mit einem pseudozufälligen Schlüsselstrom durchführt. Dieses symmetrische Vorgehen bei der Verschlüsselung ermöglicht eine schnelle und ressourcensparende Verarbeitung, wodurch die Echtzeitfähigkeit des Feldbussystems nicht beeinflusst wird. Vorzugsweise wird dabei zum Bestimmen des Authentifikationsprüfwerts eine Partition desselben Schüsselstroms verwendet, die sich nicht mit der Partition des Schlüsselstroms überdeckt, die im Rahmen der Vertraulichkeitssicherungsschicht genutzt wird, was den Schlüsselaustausch zwischen den Kommunikationsteilnehmern vereinfacht und eine schnelle Verarbeitung ermöglicht.

[0032] Fig. 2 zeigt eine mögliche Ausgestaltung des Datenflusses bei dem in Fig. 1 gezeigten Feldbussystem, wobei nur die Senderseite dargestellt ist. Die Nutzdaten data werden zuerst im sendenden Kommunikationsteilnehmer in dessen Fehlersicherungsschicht verarbeitet, wobei beispielsweise mit Hilfe eines Prüfsummenverfahrens CRC mit einem Generatorpolynom g1 eine Prüfsumme FCS1 erstellt wird, die den Nutzdaten data angefügt wird. In der Informationssicherungsschicht des sendenden Kommunikationsteilnehmers wird dann eine Verschlüsselung und ein Authentifikation-Berechnungsverfahren durchgeführt, wobei zwei disjunkte Partitionen stream1, stream2 eines pseudozufälligen Schlüsselstroms verwendet werden. Dieser Schlüsselstrom wird beispielsweise mit einem Algorithmus Grain aus einem Schlüssel Key oder einem internen Zustand abgeleitet. Die erste Partition stream1 wird dann mit den Nutzdaten data und der angehängten Prüfsumme FCS1 XOR-überlagert. Aus dem XOR-überlagerten Datenstrom mit Nutzdaten data und Prüfsumme FCS1 wird dann mit der zweiten Partition stream2 unter Anwendung beispielsweise eines Authentifikation-Berechnungsverfahrens AccuMAC ein Authentifikationsprüfwert mac erstellt, der dann den Daten angehängt wird.

[0033] Nach Umsetzung des so erzeugten Datensatzes aus XORüberlagerten Nutzdaten data und Prüfwert FCS1 sowie dem Authentifikationsprüfwert mac in der Feldbusschicht in das auf dem Feldbussystem verwendete Übertragungsprotokoll wird der Datensatz dann in das Übertragungsmedium des Feldbussystems eingekoppelt und übertragen. Das Übertragungsmedium muss keine zusätzlichen Sicherungsmaßnahmen umfassen und kann somit ein ungesicherter Kommunikationskanal sein.

[0034] Im empfangenden Kommunikationsteilnehmer wird dann das übertragene Datenpaket von der zugehörigen Feldbusschicht nach Umsetzung gemäß dem auf dem Feldbussystem verwendeten Übertragungsprotokoll an die Informationssicherungsschicht zur Weiterverarbeitung übergeben. In der Informationssicherungsschicht wird dann mit dem Algorithmus Grain derselbe pseudozufällige Schlüsselstrom mit zwei Partitionen erzeugt, wobei mit der einen Partition eine Auswertung des Authentifikationsprüfwerts mac erfolgt und mit der anderen Partition anschließend eine XOR-Überlagerung durchgeführt wird.

[0035] Nach der Entschlüsselung der Daten in der Informationssicherungsschicht werden dann anschließend in der nachgeordneten Fehlersicherungsschicht im empfangenden Kommunikationsteilnehmer die Daten durch Anwendung des Prüfsummenverfahrens CRC daraufhin geprüft, ob die übertragene Prüfsumme FCS1 korrekt ist.

Patentansprüche

1. Verfahren zum Übertragen von Daten in einem Feldbussystem zwischen wenigstens zwei Kommunikationsteilnehmern, die jeweils eine Sicherheitsschicht mit einer Fehlersicherungsschicht, die Daten gegen zufällige Datenübertragungsfehler sichert, und einer Informationssicherheitsschicht, die gegen Manipulation von Daten und/oder gegen unautorisiertes Lesen von Daten sichert, aufweisen, wobei die Daten jedes übertragenen Datenpakets im sendenden Kommunikationsteilnehmern zuerst die Fehlersicherungsschicht und dann die Informationssicherheitsschicht und im empfangenden Kommunikationsteilnehmern zuerst die Informationssicherheitsschicht und dann die Fehlersicherungsschicht durchlaufen.

2. Verfahren nach Anspruch 1, wobei die Fehlersicherungsschicht des sendenden Kommunikationsteilnehmers für die zu sendenden Daten nach einem vorgegebenen Prüfsummenberechnungsverfahren eine Prüfsumme bestimmt, die dann ebenfalls übertragen wird, wobei die Fehlersicherungsschicht des empfangenden Kommunikationsteilnehmers ein entsprechendes Verfahren auf die empfangenen Daten und Prüfsumme anwendet, um Datenübertragungsfehler zu erkennen.

3. Verfahren nach Anspruch 2, wobei die Informationssicherheitsschicht des sendenden Kommunikationsteilnehmers für die zu sendenden Daten und für einen vorgegebenen Schlüssel und/oder einen internen Zustand nach einem vorgegebenen Authentifikation-Berechnungsverfahren einen Authentifikationsprüfwert bestimmt, der ebenfalls übertragen wird, wobei die Informationssicherheitsschicht des empfangenden Kommunikationsteilnehmers für die empfangenen Daten einen weiteren Authentifikationsprüfwert berechnet, um durch Auswertung des weiteren Authentifikationsprüfwerts und dem übertragenen Authentifikationsprüfwert eine Aussage über die Datenintegrität zu erhalten.

4. Verfahren nach einem der Ansprüche 1 bis 3, wobei Informationssicherheitsschicht weiter eine Ver-

traulichkeitssicherungsschicht umfasst, die eine Vertraulichkeit von Daten sichert.

5. Verfahren nach Anspruch 4, wobei die Vertraulichkeitssicherungsschicht des sendenden Kommunikationsteilnehmers ein XOR-Überlagern der zu sendenden Daten mit einem Schlüsselstrom durchführt und wobei die Vertraulichkeitssicherungsschicht des empfangenden Kommunikationsteilnehmers ein XOR-Überlagern der empfangenen Daten mit demselben Schlüsselstrom durchführt.

6. Verfahren nach Anspruch 5, wobei der zum Bestimmen des Authentifikationsprüfwerts verwendete Schlüssel einer Partition eines Schlüsselstroms entspricht, wobei die verbleibende Partition für die Vertraulichkeitssicherungsschicht verwendet wird.

7. Kommunikationsteilnehmer für ein Feldbussystem zum Übertragen von Daten, der eine Sicherheitsschicht mit einer Fehlersicherungsschicht, die Daten gegen Datenübertragungsfehler sichert, und einer Informationssicherheitsschicht, die gegen Manipulation von Daten und/oder gegen unautorisiertes Lesen von Daten sichert, aufweist und ausgelegt ist, die zu übertragenen Daten im Sendebetrieb zuerst mit der Fehlersicherungsschicht und dann mit der Informationssicherheitsschicht und im Empfangsbetrieb zuerst mit der Informationssicherheitsschicht und dann mit der Fehlersicherungsschicht zu verarbeiten.

8. Kommunikationsteilnehmer nach Anspruch 7, wobei die Fehlersicherungsschicht ausgelegt ist, im Sendebetrieb für die zu sendenden Daten nach einem vorgegebenen Prüfsummenberechnungsverfahren eine Prüfsumme zu bestimmen und im Empfangsbetrieb ein entsprechendes Verfahren auf die empfangenen Daten und Prüfsumme anzuwenden.

9. Kommunikationsteilnehmer nach Anspruch 8, wobei die Informationssicherheitsschicht ausgelegt ist, im Sendebetrieb für die zu sendenden Daten und für einen vorgegebenen Schlüssel und/oder internen Zustand nach einem vorgegebenen Authentifikation-Berechnungsverfahren einen Authentifikationsprüfwert zu bestimmen und im Empfangsbetrieb für die empfangenen Daten einen weiteren Authentifikationsprüfwert zu berechnen.

10. Kommunikationsteilnehmer nach einem der Ansprüche 7 bis 9, wobei die Informationssicherheitsschicht weiter eine Vertraulichkeitssicherungsschicht umfasst, die eine Vertraulichkeit von Daten sichert.

11. Kommunikationsteilnehmer nach Anspruch 10, wobei die Vertraulichkeitssicherungsschicht ausgelegt ist, im Sendebetrieb ein XOR-Überlagern der zu sendenden Daten mit einem Schlüsselstrom durchzuführen und im Empfangsbetrieb ein XOR-Überlagern der empfangenen Daten mit demselben Schlüsselstrom durchführt.

12. Kommunikationsteilnehmer nach Anspruch 11, wobei der zum Bestimmen des Authentifikationsprüfwerts verwendete Schlüssel einer Partition des Schlüsselstroms entspricht, und wobei die verbleibende Partition für die Vertraulichkeitsschicht verwendet wird.

13. Feldbussystem mit wenigstens zwei Kommunikationsteilnehmer nach einem Ansprüche 7 bis 12, die über einem bidirektionalen Feldbus miteinander verbunden sind.

Es folgen 2 Blatt Zeichnungen

Anhängende Zeichnungen

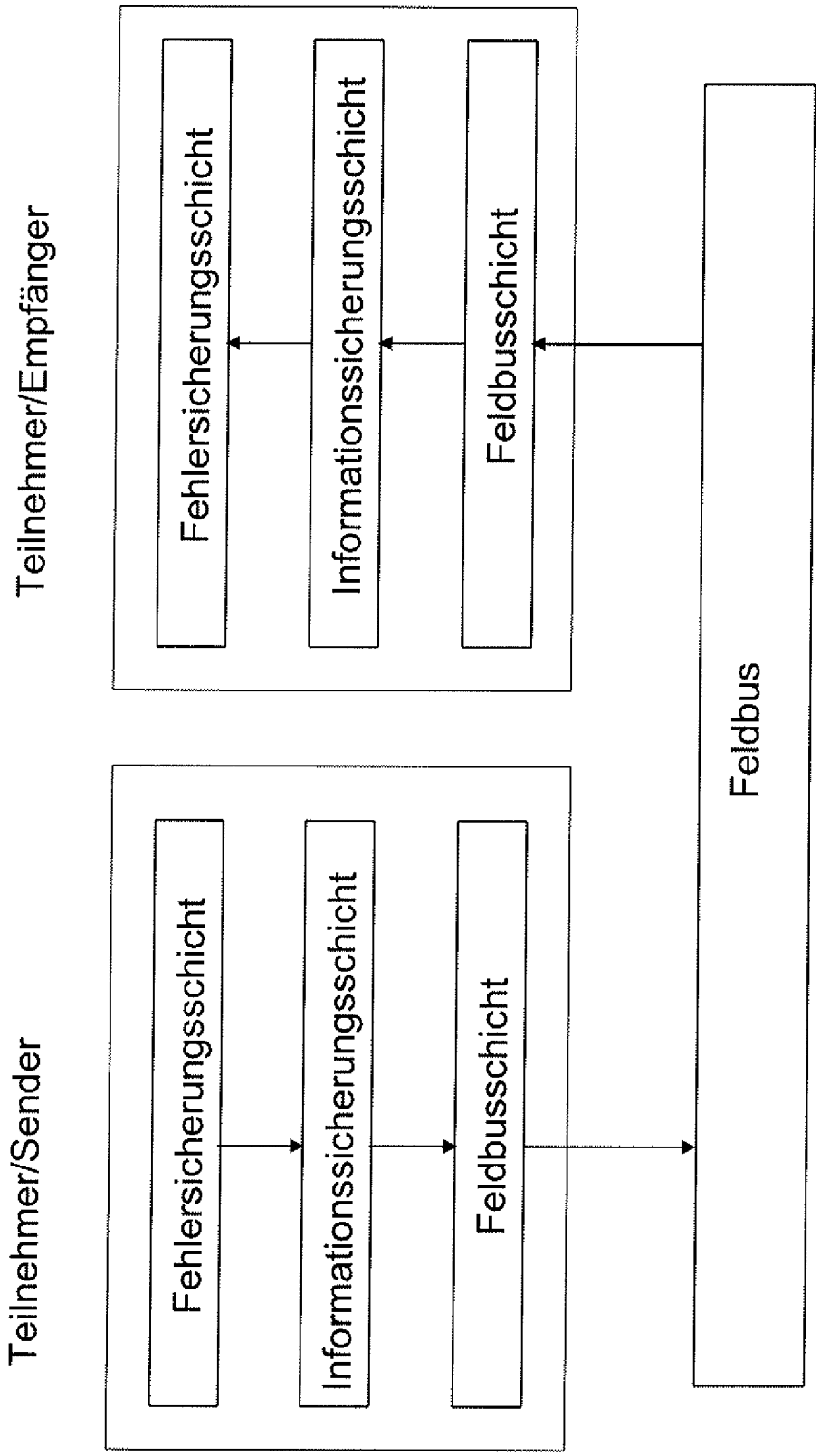


FIG. 1

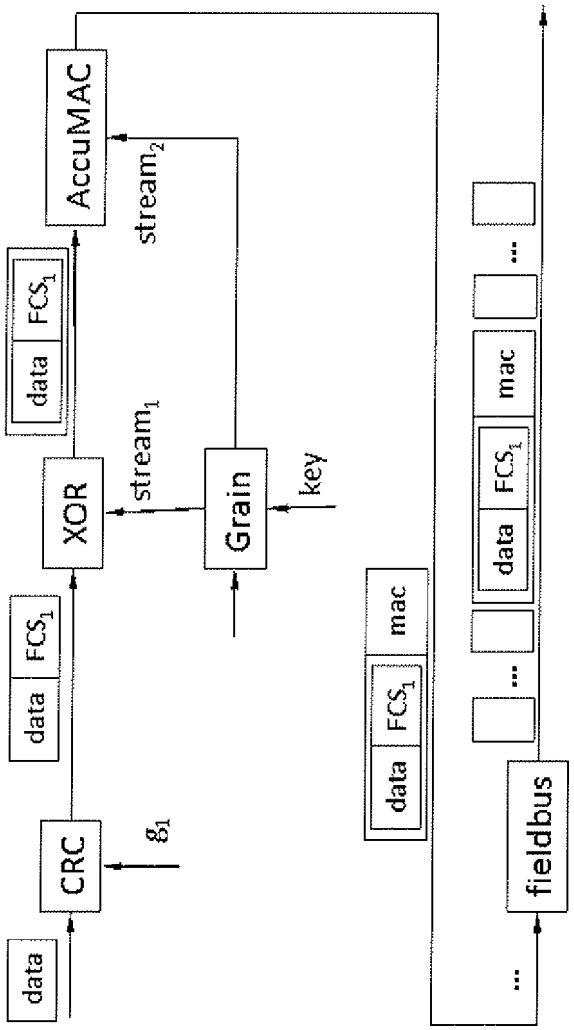

data
CRC
g_1
data
FCS1
XOR
stream1
Grain
key
data
FCS1
AccuMAC
stream2
mac
data
FCS1
...
mac
data
FCS1
...
fieldbus

FIG. 2