(19) Deutsches Patent- und Markenamt

(10) **DE 10 2014 111 361 A1** 2016.02.11

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2014 111 361.6**
(22) Anmeldetag: **08.08.2014**
(43) Offenlegungstag: **11.02.2016**

(51) Int Cl.: ***H04L 12/403*** (2006.01)
H04L 12/26 (2006.01)

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

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

(72) Erfinder:
Schiller, Frank, Prof. Dr., 90409 Nürnberg, DE; Büttner, Holger, 12157 Berlin, DE; Sachs, Jens, 32469 Petershagen, DE

(56) Ermittelter Stand der Technik:

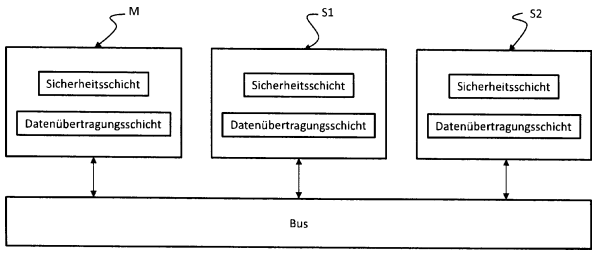
DE	**10 2007 028 767**	**A1**
US	**2012 / 0 239 256**	**A1**
US	**2012 / 0 266 053**	**A1**

Prüfungsantrag gemäß § 44 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Verfahren zum Betreiben einer Sicherheitssteuerung und Automatisierungsnetzwerk mit einer solchen Sicherheitssteuerung**

(57) Zusammenfassung: Zum Betreiben einer Sicherheitssteuerung auf einem Automatisierungsnetzwerk mit einem die Sicherheitssteuerung ausführenden Master-Teilnehmer, wenigstens einem ersten Slave-Teilnehmer mit einer ersten Sicherheitsanforderungsstufe und wenigstens einem zweiten Slave-Teilnehmer mit einer zweiten Sicherheitsanforderungsstufe ist dem ersten Slave-Teilnehmer ein erstes Sicherheitscode-Bestimmungsverfahren und dem zweiten Slave-Teilnehmer ein zweites Sicherheitscode-Bestimmungsverfahren zugeordnet, wobei der Master-Teilnehmer und der ersten Slave-Teilnehmer für einen Austausch eines Sicherheitsdatenblock das erste Sicherheitscode-Bestimmungsverfahren und der Master-Teilnehmer und der zweite Slave-Teilnehmer für einen Austausch eines Sicherheitsdatenblock das zweiten Sicherheitscode-Bestimmungsverfahren verwenden.



Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zum Betreiben einer Sicherheitssteuerung auf einem Automatisierungsnetzwerk mit einem Master-Teilnehmer und einer Mehrzahl von Slave-Teilnehmer, den unterschiedliche Sicherheitsanforderungsstufen zugeordnet sind, und ein Automatisierungsnetzwerk mit einer solchen Sicherheitssteuerung.

[0002] Moderne Konzepte der Industrieautomation, d.h. der Steuerung und Überwachung von technischen Prozessen mit Hilfe von Software, beruhen auf der Idee einer zentralen Steuerung mit verteilter Sensor-/Aktorebene. Die Teilnehmer kommunizieren dabei untereinander und mit übergeordneten Systemen über industrielle lokale Netzwerke, im Weiteren auch als Automatisierungsnetzwerke bezeichnet. Die Steuerungsfunktion beruht auf zwei Grundideen, der geographischen Dezentralisierung und der hierarchischen Aufteilung der Steuerungsfunktionen. Die funktionelle Hierarchie teilt die Automatisierungsaufgabe dabei im Wesentlichen in eine Steuerungsebene und eine Sensor-/Aktorebene ein. Die industriellen lokalen Netzwerke sind üblicherweise als sogenannte Master-Slave-Kommunikationsnetze ausgelegt, bei denen der Master-Teilnehmer die Steuerungsebene und die Slave-Teilnehmer die Sensor-/Aktorebene bildet.

[0003] Eine wesentliche Anforderung an ein Automatisierungsnetzwerk ist die Fehlersicherheit. Beim Steuern und Überwachen von technischen Prozessen muss sichergestellt sein, dass dann, wenn das Automatisierungsnetzwerk fehlerhaft arbeitet, daraus keine Gefahr für Mensch und Umwelt resultiert. Das Automatisierungsnetzwerk arbeitet in der Regel nach dem sogenannten Fail-Safe-Prinzip, bei dem das Automatisierungsnetzwerk im Fehlerfall in einen sicheren Zustand übergeht.

[0004] Um die Gefährdung durch ein Automatisierungsnetzwerk einstufen zu können, ist es Vorschrift, eine Gefahrenanalyse vorzunehmen. Gemäß der europäischen Norm EN 1050 hat die Risikobeurteilung als eine Folge von logischen Schritten zu erfolgen, welche die systematische Untersuchung von Gefährdung erlaubt, die vom Automatisierungsnetzwerk bzw. den einzelnen Teilnehmern ausgehen. Auf der Grundlage der Gefahrenanalyse werden dann die technischen und organisatorischen Anforderungen an das Automatisierungsnetzwerk zur Gewährleistung einer ausreichenden Sicherheit festgelegt.

[0005] Im Bereich der Maschinen- und Anlagensicherheit, insbesondere auch von programmierbaren elektronischen Steuerungssystemen, haben sich die Normen EN ISO13849-1 und IEC/EN 62061 als internationaler Standard zur Durchführung einer Gefährdungsanalyse etabliert. Die Normen beziehen alle sicherheitsrelevanten Teilnehmer unabhängig vom Teilnehmertyp mit ein und unterteilen die sicherheitstechnische Leistungsfähigkeit in Kategorien. Ausgehend von der ermittelten Sicherheitskategorie wird dann die Steuerungsstruktur im Automatisierungsnetzwerk festgelegt, um die Anforderungen an die Sicherheitsfunktionen und ein gefordertes Systemverhalten im Fehlerfall zu erreichen.

[0006] Die Normen EN ISO 13849-1 und IEC/EN 62061 spezifizieren die zur Risikoreduzierung erforderliche sicherheitstechnische Leistungsfähigkeit von programmierbaren elektronischen Steuerungssystemen. Zur Unterteilung der sicherheitstechnischen Leistungsfähigkeit werden in den beiden Normen Sicherheitsanforderungsstufen definiert. Hierzu werden alle Sicherheitsfunktionen des Automatisierungsnetzwerks mit allen an ihrer Ausführung beteiligten Teilnehmern betrachtet.

[0007] Die Norm IEC/EN 62061 gibt vier Sicherheitsanforderungsstufe („Safety Integrity Level“ – SIL) SIL1 bis SIL4 vor, wobei die einzelnen Stufen durch die zulässige Restfehlerwahrscheinlichkeit für das Auftreten eines Fehlers definiert sind. Die geringsten Anforderungen nach der Norm stellt die Sicherheitsanforderungsstufe SIL1. Von Stufe zu Stufe steigen dann die Anforderungen bis zur Sicherheitsanforderungsstufe SIL4 an. Die Sicherheitsanforderungsstufe des Automatisierungsnetzwerks wird dabei auf der Grundlage von sicherheitstechnischen Kenngrößen der an den Sicherheitsfunktionen beteiligten Teilnehmer bestimmt. Zum Bestimmen der Sicherheitsanforderungsstufe des Automatisierungsnetzwerkes ist ferner neben der Kenntnis der sicherheitstechnischen Kenngrößen aller an der Sicherheitsfunktion beteiligten Teilnehmer eine genaue Information über die logische Verknüpfung der Teilnehmer im Automatisierungsnetzwerk erforderlich. Die Sicherheitsanforderungsstufe wird außerdem wesentlich von der im Automatisierungsnetzwerk eingesetzten Busarchitektur beeinflusst.

[0008] Da die Anforderungen an die Teilnehmer in einem Automatisierungsnetzwerk in Bezug auf die Sicherheitsfunktionen oft verschieden sind, werden Automatisierungsnetzwerk in der Regel mit Teilnehmern betrieben werden, die unterschiedliche SIL-Stufe besitzen. Die Sicherheitsanforderungsstufe des Gesamtsystems wird in einem solchen Fall aber durch den Teilnehmer mit der niedrigsten SIL-Stufe bestimmt. Grund hierfür ist, dass in einem Automatisierungsnetzwerk ein Datenverkehr zwischen Teilnehmern mit unterschiedlicher SIL-Stufe zu erheblichen sicherheitstechnischen Problemen führt. Wenn nämlich ein Teilnehmer mit einer niedrigen SIL-Stufe Datenpakete an einen Teilnehmer mit einer hohen SIL-Stufe versendet, kann auch bei Auftreten eines einfachen Fehlers bei der Datenpaket-Erzeugung in dem sendenden Teilnehmer, der im Rahmen

der niedrigen SIL-Stufe des sendenden Teilnehmers zulässig ist, eine gültiges Datenpaket für den empfangenden Teilnehmer mit hoher SIL-Stufe erzeugt werden. Der Fehler im übertragenen Datenpaket wird zwar dann im Empfänger aufgrund seiner hohen SIL-Stufe mit großer Wahrscheinlichkeit erkannt. Durch den möglichen Datenverkehr mit dem Teilnehmer, der die niedrige SIL-Stufe besitzt, kann jedoch dann die Erfüllung der im Empfänger geforderten hohen SIL-Stufe nicht mehr gewährleistet werden, da von dem Teilnehmer mit der niedrigen SIL-Stufe ein an sich gültiges Datenpaket gebildet werden kann.

[0009] Ferner ist es bei der Erweiterung eines Automatisierungsnetzes mit weiteren sicherheitsrelevanten Teilnehmer, insbesondere dann, wenn deren SIL-Stufe von der SIL-Stufe der anderen Teilnehmer abweichen, in der Regel erforderlich, das Gesamtsystem neu zu konfigurieren, um zu verhindern, dass die von den bereits im Automatisierungssystem vorhandenen Teilnehmern auszuführenden Sicherheitsfunktionen in Konflikt mit den Sicherheitsfunktionen der neu hinzugefügten Teilnehmer kommen. Dabei besteht insbesondere die Gefahr, dass bei der Adressenvergabe neuen Teilnehmern die gleichen Adressen wie alten Teilnehmern zugewiesen werden, was zur Fehlleitungen von Datenpaketen, die dann nicht erfasst werden, führen kann. Die Adressenvergabe ist insbesondere dann aufwendig, wenn die den Teilnehmern zugeordneten Adressen in den Datenpaketen nur impliziert im Rahmen von Sicherheitscodes, die von einem Datensicherungsmechanismus erzeugt werden, übertragen werden und oder von außen nicht ermittelbar sind.

[0010] Aufgabe der vorliegenden Erfindung ist es, ein Verfahren zum Betreiben einer Sicherheitssteuerung und ein Automatisierungsnetzwerk bereitzustellen, bei den sich Teilnehmer mit beliebiger Sicherheitsanforderungsstufe ohne eine Beeinträchtigung der Sicherheit über das Automatisierungsnetzwerk verbinden lassen.

[0011] Diese Aufgabe wird mit einem Verfahren gemäß Anspruch 1 und einem Automatisierungsnetzwerk gemäß Anspruch 5 gelöst. Bevorzugte Weiterbildungen sind in den abhängigen Ansprüchen angegeben.

[0012] Gemäß der Erfindung wird zum Betreiben einer Sicherheitssteuerung auf einem Automatisierungsnetzwerk mit einem die Sicherheitssteuerung ausführenden Master-Teilnehmer, wenigstens einem ersten Slave-Teilnehmer, dem eine erste Sicherheitsanforderungsstufe zugeordnet ist, und einem wenigstens zweiten Slave-Teilnehmer, dem eine zweite Sicherheitsanforderungsstufe zugeordnet ist, wobei der Master-Teilnehmer, der erste Slave-Teilnehmer und der zweite Slave-Teilnehmer über eine Datenübertragungsstrecke miteinander verbunden sind und jeweils eine Sicherheitsschicht und eine Übertragungsschicht aufweisen, im Sendebetrieb in der Sicherheitsschicht des jeweiligen Teilnehmers für einen zu sendenden Sicherheitsdatenblock ein Sicherheitscode mithilfe eines Sicherheitscode-Bestimmungsverfahrens bestimmt und in der Übertragungsschicht des jeweiligen Teilnehmers ein Datenpaket mit dem Sicherheitsdatenblock und dem Sicherheitscode für das Versenden auf der Datenübertragungsstrecke gebildet, und im Empfangsbetrieb in der Übertragungsschicht des jeweiligen Teilnehmers aus einem über die Datenübertragungsstrecke empfangenen Datenpaket ein Sicherheitsdatenblock und ein zugehöriger Sicherheitscode extrahiert und in der Sicherheitsschicht des jeweiligen Teilnehmers mit dem Sicherheitscode-Bestimmungsverfahren der Sicherheitscode für den Sicherheitsdatenblock verifiziert. Dem ersten Slave-Teilnehmer ist dabei ein erstes Sicherheitscode-Bestimmungsverfahren und dem zweiten Slave-Teilnehmer ein zweites Sicherheitscode-Bestimmungsverfahren zugeordnet ist, wobei der Master-Teilnehmer und der ersten Slave-Teilnehmer für einen Austausch eines Sicherheitsdatenblock das erste Sicherheitscode-Bestimmungsverfahren und der Master-Teilnehmer und der zweite Slave-Teilnehmer für einen Austausch eines Sicherheitsdatenblock das zweiten Sicherheitscode-Bestimmungsverfahren verwenden.

[0013] Erfindungsgemäß wird für die Kommunikation zwischen Teilnehmern im Automatisierungsnetzwerk mit gleicher Sicherheitsanforderungsstufe je ein eigenes Sicherheitscode-Bestimmungsverfahren verwendet. Eine gegenseitige unerkannte Beeinflussung insbesondere von Teilnehmern mit unterschiedlicher Sicherheitsanforderungsstufe wird so ausgeschlossen. Eine Fehlleitung von Datenpaketen im Datenverkehr zwischen Teilnehmer mit unterschiedlicher Sicherheitsanforderungsstufe wird zuverlässig erkannt. Im Automatisierungsnetzwerk ist so auch ein Datenverkehr zwischen Teilnehmer mit beliebiger Sicherheitsanforderungsstufe ohne sicherheitstechnische Probleme möglich.

[0014] Gemäß einer bevorzugten Ausführungsform ist das erste und zweite Sicherheitscode-Bestimmungsverfahren ein zyklisches Redundanzprüfverfahren, wobei dem ersten Sicherheitscode-Bestimmungsverfahren ein erstes Sicherheitscode-Generatorpolynom und dem zweiten Sicherheitscode-Bestimmungsverfahren ein zweites Sicherheitscode-Generatorpolynom zugeordnet ist. Dabei unterscheidet sich der Hamming-Abstand des ersten Sicherheitscode-Generatorpolynoms vorzugsweise von dem Hamming-Abstand des zweiten Sicherheitscode-Generatorpolynoms. Mit dieser Vorgehensweise besteht die Möglichkeit, für beide Sicherheitscode-Bestimmungsverfahren den augenblicklichen Standard-Sicherheitsmechanismus zyklische Redundanzprüfung einzusetzen, sodass auf zusätzliche

zeitraubende Sicherheitsmaßnahmen, die darüber hinaus zusätzliche Hard- und Software nötig machen, verzichtet werden kann. Durch die Einstellung des Hamming-Abstands des ersten und zweiten Sicherheitscode-Generatorpolynoms kann für die für die jeweilige Sicherheitsanforderungsstufe geforderte Aufdeckwahrscheinlichkeit von Fehlern im Datenpaket gesorgt werden.

[0015] Gemäß einer bevorzugten Ausführungsform kann die Auslegung des Automatisierungsnetzwerkes für die Teilnehmer mit der ersten Sicherheitsanforderungsstufe vollkommen getrennt von der Auslegung des Automatisierungsnetzwerkes für die Teilnehmer mit der zweiten Sicherheitsanforderungsstufe erfolgen. In beiden Netzwerkbereichen können dann gleiche Adressen verwendet werden, ohne dass es zu Fehlleitungen im Datenverkehr kommt, da jedem Netzwerkbereich ein unabhängiges Sicherheitscodebestimmungsverfahren zugeordnet ist, das eine solche Fehlleitung verhindert.

[0016] Die Erfindung wird anhand der beigefügten Zeichnungen näher erläutert.

[0017] **Fig.** 1 zeigt schematisch den Aufbau eines erfindungsgemäßen Automatisierungsnetzwerkes mit einem eine Sicherheitssteuerung ausführenden Master-Teilnehmer, einem ersten Slave-Teilnehmer, dem eine erste Sicherheitsanforderungsstufe zugeordnet ist, und einem zweiten Slave-Teilnehmer, dem eine zweite Sicherheitsanforderungsstufe zugeordnet ist.

[0018] **Fig.** 2 zeigt eine mögliche Auslegung der Datenübertragung bei dem in **Fig.** 1 gezeigten Automatisierungssystem.

[0019] **Fig.** 3 zeigt die Restfehlerrate und den Hamming-Abstand für Generatorpolynome, die den Sicherheitsanforderungsstufen SIL1 bis SIL3 eingesetzt werden.

[0020] In der Industrieautomation werden Netzwerke verwendet, bei denen die dezentral angeordneten Geräte einer Sensor-/ Aktorebene wie E/A-Module, Messwerterfasser, Ventile, Antriebe etc. über ein leistungsfähiges Bussystem mit einem Automatisierungsrechner einer Steuerungsebene kommunizieren. Als Bussysteme werden in Automatisierungsnetzwerken vorzugsweise Feldbussysteme eingesetzt.

[0021] Automatisierungsnetzwerke sind in der Regel hierarchisch aufgebaut und arbeiten nach dem Master-Slave-Prinzip. Die Master-Teilnehmer sind der Steuerungsebene zugeordnet und stellen die aktiven Teilnehmer dar, die eine Zugriffsberechtigung auf die Kommunikationsverbindung im Automatisierungsnetzwerk haben und den Datenverkehr bestimmen. Die Slave-Teilnehmer sind Teil der Sensor-/ Aktorebene und bilden die passiven Teilnehmer. Sie haben keine eigene Zugriffsberechtigung auf das Bussystem und dürfen empfangene Daten nur quittieren oder auf Anfrage eines Master-Teilnehmers Daten an diesen übermitteln.

[0022] Eine zentrale Anforderung an Automatisierungssysteme ist die sichere und zuverlässige Datenübertragung. Um Gefahren für Mensch und Umwelt auszuräumen, muss sichergestellt sein, dass die Nutzdaten zwischen den Slave-Teilnehmern der Sensor-/ Aktorebene und den Master-Teilnehmern der Steuerungsebene fehlerfrei übertragen oder alternativ Fehler bei der Datenübertragung zuverlässig erkannt werden. In Automatisierungssystemen sind deshalb Sicherungsmaßnahmen, sogenannte Safety-Maßnahmen, implementiert, die gewährleisten, dass Fehler bei der Datenübertragung mit hoher Wahrscheinlichkeit aufgedeckt werden, um so die Gefahr unerkannter Fehler zu minimieren. Die zu übertragenden Daten werden deshalb vom sendenden Teilnehmer mit einem Sicherheitscode versehen, der vom empfangenen Teilnehmer dann verifiziert wird. Als Verfahren zum Bestimmen des Sicherheitscodes wird in der Regel das zyklische Redundanzprüfverfahren, auch CRC-Verfahren genannt, eingesetzt.

[0023] Bei dem CRC-Verfahren wird vor einer Datenübertragung im Sender für den zu übertragenden Datenblock mithilfe eines Generatorpolynoms eine Prüfzeichenfolge ermittelt, die dann an den Datenblock angehängt und zusammen mit diesen an den Empfänger übermittelt wird. Vom Empfänger wird mithilfe desselben Generatorpolynoms, das vom Sender zum Berechnen der Prüfzeichenfolge für das übertragene Datenpaket eingesetzt wurde, die übertragene Prüfzeichenfolge verifiziert, um festzustellen, ob die Datenübertragung unverfälscht stattgefunden hat.

[0024] Im Allgemeinen sind nicht alle Teilnehmer im Automatisierungsnetzwerk gleich sicherheitsrelevant. Auch ist die Anzahl der Sicherheitsfunktionen in einem Automatisierungsnetzwerk in der Regel geringer als die Anzahl der nicht sicherheitsrelevanten Steuerungsfunktionen.

[0025] Um die Gefährdung für Mensch und Umwelt durch das Automatisierungsnetzwerk einzustufen, ist es Vorschrift, eine Gefahrenanalyse durchzuführen. Die zentrale Norm ist die IEC/EN 62061, die die zur Risikoreduzierung erforderliche sicherheitstechnische Leistungsfähigkeit von programmierbaren elektronischen Steuerungssystemen spezifiziert. Zur Unterteilung der sicherheitstechnischen Leistungsfähigkeit sind in der Norm IEC/EN 62061 vier Sicherheitsanforderungsstufen (Safety Integrity Level – SIL, SIL1 bis SIL4) definiert. Die einzelnen Sicherheitsanforderungsstufen legen dabei die zulässige Rest-

fehlerwahrscheinlichkeit für das Auftreten eines Fehlers fest. Gemäß Sicherheitsanforderungsstufe SIL1 darf die mittlere Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde (PFH_D) größer als 10^{-5}, muss aber kleiner als S10^{-6} sein. Für die Sicherheitsanforderungsstufe SIL2 ist der Wertebereich größer als 10^{-6} aber kleiner als 10^{-7}, für die Sicherheitsanforderungsstufe SIL3 größer als 10^{-7}, aber kleiner als 10^{-8} und für die Sicherheitsanforderungsstufe SIL4 größer als 10^{-8}, aber kleiner als 10^{-9}. Neben der Norm IEC/EN 62061 kommt auch oft die einfacher anzuwendende Norm EN ISO 13849, die die Performance-Level A bis E kennt, zum Einsatz.

[0026] Die für die einzelnen Teilnehmer geforderte Sicherheitsanforderung im Automatisierungsnetzwerk hängt von den dem jeweiligen Teilnehmer zugeordneten Sicherheitsfunktionen ab. Automatisierungsnetzwerke werden deshalb oft mit Teilnehmern betrieben, die aufgrund ihrer Sicherheitsfunktionen unterschiedliche Sicherheitsanforderungen aufweisen.

[0027] Fig. 1 zeigt schematisch die Grundstruktur eines Automatisierungsnetzwerks mit einem Master-Teilnehmer M, der die Steuerungsebene bildet und zwei Slave-Teilnehmer S1 und S2, die die Sensor-/Aktorebene repräsentieren. Der Master-Teilnehmer M und die zwei Slave-Teilnehmer S1, S2 sind über einen seriellen Bus miteinander verbunden, über den der Datenverkehr zwischen den Teilnehmern stattfindet. Der Datenverkehr im Automatisierungsnetzwerk wird dabei vom Master-Teilnehmer M in Form von Datenpaketen organisiert, die sich aus Steuerdaten und Nutzdaten zusammensetzen, wobei die Steuerdaten im Datenpaket eine Adresseninformation enthalten, das den Sender bzw. Empfänger identifiziert.

[0028] Bei dem in **Fig.** 1 gezeigten Automatisierungsnetzwerk sind beide Slave-Teilnehmer S1 und S2 sicherheitsrelevant. Es können natürlich mehr als zwei sicherheitsrelevante Slave-Teilnehmer vorgesehen sein. Auch können im Automatisierungsnetzwerk neben sicherheitsrelevanten Teilnehmern nicht sicherheitsrelevante Teilnehmer eingebunden werden. Die Steuerungsebene im Automatisierungsnetzwerk kann auch auf mehrere Master-Teilnehmer aufteilt sein.

[0029] Die Datenübertragung im Automatisierungsnetzwerk wird in der Regel einheitlich, vorzugsweise auf Grundlage des Ethernet-Protokolls ausgeführt, wobei alle sicherheitsrelevanten Teilnehmer im Automatisierungssystem, das heißt der Master-Teilnehmer M und die beiden Slave-Teilnehmer S1, S2 neben der Datenübertragungsschicht zum Verarbeiten der Standarddaten eine weitere übergeordnete Sicherheitsschicht zur Verarbeitung der Sicherheitsdaten aufweisen. Die Sicherheitsschicht und die Datenübertragungsschicht sind in den sicherheitsrelevanten Teilnehmern vollständig voneinander abgekapselt, um die Gefahr der Verfälschung bei der Verarbeitung von Sicherheitsdaten zu verhindern. Mit dieser Auslegung der sicherheitsrelevanten Teilnehmer kann der Hard- und Softwareaufwand reduziert werden, da durch die vollständige Abschottung der Sicherheitsebene von der Datenübertragungsebene sowohl Sicherheitsdaten als auch Standardnutzdaten mithilfe eines Standardprotokolls wie dem Ethernet-Protokoll übertragen werden können.

[0030] Fig. 2 zeigt eine Datenübertragung bei dem in **Fig.** 1 gezeigten Automatisierungssystem. In der Sicherheitsschicht des Senders wird mithilfe eines Sicherheitscode-Bestimmungsverfahren Safety CRC ein Sicherheitscode FCS_{Safety} für einen zu sendenden Sicherheitsdatenblock ND_{Safety} erzeugt. Wenn als Sicherheitscode-Bestimmungsverfahren Safety CRC, wie in **Fig.** 2 gezeigt, das zyklische Redundanzprüfungsverfahren eingesetzt wird, wird unter Verwendung eines Sicherheitsdaten-Generatorpolynoms der Sicherheitscode als Sicherheitsdatenblock-Prüfzeichenfolge ermittelt. Der Sicherheitscode FC_{Safety} wird dann an den Sicherheitsdatenblock ND_{Safety} angehängt und in Form eines Sicherheitsblocks an die Datenübertragungsschicht übergeben.

[0031] In der Datenübertragungsschicht des Senders wird anschließend das Sicherheitspaket in einem Standarddatenblock $ND_{Standard}$ eingebettet, wobei vorzugsweise mithilfe eines weiteren Sicherheitscode-Bestimmungsverfahrens Standard CRC ein weiterer Sicherheitscode $FCS_{Standard}$ ermittelt wird. Wenn als Sicherheitscode-Bestimmungsverfahren Standard CRC wiederum, wie in **Fig.** 2 gezeigt, das zyklische Redundanzprüfungsverfahren eingesetzt wird, wird ein gegenüber dem zur Berechnung der Sicherheitsdatenblock-Prüfzeichenfolge eingesetzten Sicherheitsdaten-Generatorpolynom verändertes Standarddaten-Generatorpolynom verwendet.

[0032] Die Datenübertragungsschicht versendet dann den Standarddatenpaketblock $ND_{Standard}$ mit eingebettetem Sicherheitspaket ND_{Safety} und Sicherheitscode FC_{Safety} und angehängter Standarddatenblock-Prüfzeichenfolge $FCS_{Standard}$ und überträgt diesen über den Bus Communication Channel zum Empfänger. Im Empfänger werden dann, wie in **Fig.** 2 gezeigt, wiederum zwei zyklische Redundanzprüfungen durchgeführt. In der Datenübertragungsschicht des Empfängers wird die Standarddatenblock-Prüfzeichenfolge $FCS_{Standard}$ des übertragenen Datenpakets mithilfe der zyklischen Redundanzprüfung Standard CRC unter Verwendung des Standarddaten-Generatorpolynoms verifiziert. Anschließend wird dann in der Sicherheitsschicht des Empfängers eine weitere Verifizierung der Sicherheitsdatenblock-Prüfzeichenfolge FCS_{Safety} des im übertragenen Datenpaket eingebetteten Sicherheitsdatenpakets mithilfe der zy-

klischen Redundanzprüfung Safety CRC unter Verwendung des Sicherheitsdaten-Generatorpolynoms vorgenommen. Falls beide Überprüfungen zu einem positiven Ergebnis führen, können die Sicherheitsdaten verwendet werden. Andernfalls werden sie verworfen. Der Empfänger wartet dann auf ein weiteres Datenpaket, verwendet Ersatzdaten oder führt Sicherheitsmaßnahmen durch.

[0033] Das Sicherheitsdaten-Generatorpolynom erzeugt dabei vorzugsweise eine Sicherheitsdatenblock-Prüfzeichenfolge der Länge R. Als Sicherheitsdaten-Generatorpolynom wird dann vorzugsweise ein Generatorpolynom eingesetzt, dessen Hamming-Abstand sich einer fiktiven Berechnung einer Prüfzeichenfolge für den Standarddatenblock gegenüber dem Hamming-Abstand für die Prüfzeichenfolge für den um R längeren Sicherheitsdatenblock unterscheidet. Mit dieser Vorgehensweise wird gewährleistet, dass Verfälschungen in der Sicherheitsdatenblock-Zeichenfolge zuverlässig nachgewiesen werden können, auch dann, wenn wie bei dem in **Fig.** 1 gezeigten Automatisierungssystem vorgesehen, die Sicherheitsschicht und die Datenübertragung im sicherheitsrelevanten Teilnehmer vollständig voneinander getrennt sind.

[0034] Wenn in einem Automatisierungsnetzwerk sicherheitsrelevante Teilnehmer unterschiedlichen Sicherheitsanforderungsstufen zugeordnet sind, kann es beim Datenverkehr zu erheblichen sicherheitstechnischen Problemen kommen. Im in **Fig.** 1 gezeigten Automatisierungsnetzwerk erfüllt der Slave-Teilnehmer S1 die Sicherheitsanforderungsnorm SIL3, während der Slave-Teilnehmer S2 die Sicherheitsanforderungsnorm SIL2 erfüllt. Wenn der Slave-Teilnehmer S2 mit der niedrigen SIL-Stufe 2 Datenpakete erzeugt, kann bei dem Auftreten eines einfachen Fehlers in diesem Slave-Teilnehmer, der im Rahmen der niedrigen SIL-Stufe 2 im Slave-Teilnehmer zuverlässig ist, ein gültiges Datenpaket für den Slave-Teilnehmer S1 mit der höheren SIL-Stufe 3 erzeugt werden. Der Slave-Teilnehmer S1 würde zwar den Fehler im übertragenen Datenpaket vom Slave-Teilnehmer S2 mit hoher Wahrscheinlichkeit feststellen. Die für den Slave-Teilnehmer S1 geforderte hohe SIL-Stufe 3 wird aufgrund der dann jedoch auftretenden hohen Fehlerrate nicht mehr eingehalten.

[0035] Dieses Problem wird erfindungsgemäß dadurch vermieden, dass der Teilnehmer, dem eine erste Sicherheitsanforderungsstufe zugeordnet ist, für den Austausch von Datenpaketen ein erstes Sicherheitscode-Bestimmungsverfahren und der Teilnehmer, dem eine zweiten Sicherheitsanforderungsstufe zugeordnet ist, für den Austausch von Datenpaketen ein zweites Sicherheitscode-Bestimmungsverfahren verwendet. Im Falle dass als Sicherheitscode-Bestimmungsverfahren immer ein zyklisches Redundanzprüfungsverfahren eingesetzt wird, werden unterschiedliche Sicherheitscode-Generatorpolynome für die Teilnehmer mit den unterschiedlichen Sicherheitsanforderungen eingesetzt. Mit dieser Vorgehensweise können Fehlleitungen bei der Datenübertragung zuverlässig aufgedeckt werden, da der Datenverkehr zwischen den Teilnehmergruppen mit den unterschiedlichen Sicherheitsanforderungen mithilfe der unterschiedlichen Sicherheitscodes eindeutig voneinander abgegrenzt werden kann.

[0036] Bei dem in **Fig.** 1 gezeigten Automatisierungssystem wird so vorgegangen, dass der Master-Teilnehmer M und der Slave-Teilnehmer S1 für den Datenaustausch ein erstes, für die Sicherheitsanforderungsstufe SIL3 geeignetes Generatorpolynom nutzen. Für den Datenaustausch mit dem zweiten Slave-Teilnehmer S2, dessen Sicherheitsanforderungsstufe SIL2 ist, nutzt der Master-Teilnehmer M und der Slave-Teilnehmer S2 dagegen ein anderes, für die Sicherheitsanforderungsstufe SIL2 geeignetes Generatorpolynom.

[0037] **Fig.** 3 zeigt beispielhaft drei unterschiedliche Generatorpolynome die jeweils einer der Sicherheitsanforderungsstufen SIL1, SIL2 und SIL3 zugeordnet sind. Als Generatorpolynom für die SIL-Stufe 3 wird 0 × 12A23, als Generatorpolynom für die SIL-Stufe 2 wird 0 × 17B0F und als Generatorpolynom für die SIL-Stufe 1 wird 0 × 1571F eingesetzt. Für die einzelnen Generatorpolynome sind dabei jeweils der Hamming-Abstand sowie die Restfehlerwahrscheinlichkeit angegeben. Der Hamming-Abstand gibt dabei an, wie viele Zeichen in einem Datensatz mindestens verfälscht sein müssen, damit trotz der eingesetzten Safety-Maßnahme der zyklischen Redundanzprüfung eine unerkannte Verfälschung auftreten kann. Die Auswahl der Generatorpolynome erfolgt dabei so, der Hamming-Abstand des Generatorpolynoms die gemäß der Sicherheitsanforderungsstufe geforderte Restfehlerwahrscheinlichkeit für das Auftreten eines Fehlers erfüllt. Dabei wird grundsätzlich so vorgegangen, dass, wenn den Sicherheitsanforderungsstufe unterschiedliche Restfehlerwahrscheinlichkeiten für das Auftreten eines Fehlers zugeordnet sind, der Hamming-Abstand der zugeordneten Generatorpolynome sich unterscheidet.

[0038] Die Zuordnung unterschiedlicher Sicherheitscode-Bestimmungsverfahren zu verschiedenen Teilnehmergruppen im Automatisierungsnetzwerk, die jeweils eine Sicherheitsanforderungsstufe repräsentieren, ermöglicht es auch, auf einfache Weise das Automatisierungsnetzwerk zu erweitern. Im Falle, dass eine neue Gruppe von Slave-Teilnehmer mit einer zugeordneten Sicherheitsanforderungsstufe an das Automatisierungsnetzwerk angebunden werden soll, wird der hinzugefügten Gruppe ein eigenständiges Sicherheitscode-Bestimmungsverfahren zum Datenaustausch untereinander und mit den Master-Teilnehmern zugeordnet. Mit dieser Vorgehenswei-

se ist es nicht mehr erforderlich, bei der Konfiguration der neuen Gruppe von Slave-Teilnehmer im Automatisierungsnetzwerk die übrigen Slave-Teilnehmer zu berücksichtigen, da die verschiedenen Gruppen von Teilnehmern, den jeweils eine Sicherheitsanforderungsstufe zugeordnet ist, mithilfe der getrennten Sicherheitscode-Bestimmungsverfahren den Datenverkehr unabhängig voneinander ausführen. Nur der Master-Teilnehmer muss mit allen Teilnehmergruppen sprechen und für den Datenpaket-Austausch mit der jeweiligen Teilnehmergruppe das dafür vorgesehene Sicherheitscode-Bestimmungsverfahren durchführen können.

[0039] Durch das Zuordnen unterschiedlicher Sicherheitscode-Bestimmungsverfahren zu Teilnehmergruppe, den durch ihre Sicherheitsanforderungsstufen voneinander abgegrenzt sind, besteht ferner die Möglichkeit die Adressen an die Teilnehmer der jeweiligen Sicherheitsgruppen unabhängig voneinander zu vergeben. Durch das Ausführen jeweils eigenständiger Sicherheitscode-Bestimmungsverfahren können dann die Teilnehmer in den verschiedenen Gruppen zum Beispiel auch gleiche Adressen aufweisen, da eine Datenpaket-Fehlleitung durch die separaten Sicherheitscode-Bestimmungsverfahren zuverlässig verhindert wird. Dies ist insbesondere dann vorteilhaft, wenn wie bei der in **Fig.** 2 gezeigten Auslegung der Sicherheitsdatenblock gekapselt im Standarddatenblock übertragen wird und die Adresse im Sicherheitsdatenblock nicht mehr expliziert vorliegen, sondern nur die Prüfzeichenfolge einfließen. Bei der erfindungsgemäßen Adressenvergabe ist nur erforderlich, dass die Teilnehmer innerhalb einer Sicherheitsanforderungsstufe eine eindeutige Adresse besitzen.

ZITATE ENTHALTEN IN DER BESCHREIBUNG

Diese Liste der vom Anmelder aufgeführten Dokumente wurde automatisiert erzeugt und ist ausschließlich zur besseren Information des Lesers aufgenommen. Die Liste ist nicht Bestandteil der deutschen Patent- bzw. Gebrauchsmusteranmeldung. Das DPMA übernimmt keinerlei Haftung für etwaige Fehler oder Auslassungen.

Zitierte Nicht-Patentliteratur

- europäischen Norm EN 1050 [0004]
- Normen EN ISO13849-1 [0005]
- IEC/EN 62061 [0005]
- Normen EN ISO 13849-1 [0006]
- IEC/EN 62061 [0006]
- Norm IEC/EN 62061 [0007]
- IEC/EN 62061 [0025]
- Norm IEC/EN 62061 [0025]
- Norm IEC/EN 62061 [0025]
- Norm EN ISO 13849 [0025]

Patentansprüche

1. Verfahren zum Betreiben einer Sicherheitssteuerung auf einem Automatisierungsnetzwerk mit einem die Sicherheitssteuerung ausführenden Master-Teilnehmer, wenigstens einem ersten Slave-Teilnehmer, dem eine erste Sicherheitsanforderungsstufe zugeordnet ist, und wenigstens einem zweiten Slave-Teilnehmer, dem eine zweite Sicherheitsanforderungsstufe zugeordnet ist,
wobei der Master-Teilnehmer, der erste Slave-Teilnehmer und der zweite Slave-Teilnehmer über eine Datenübertragungsstrecke miteinander verbunden sind und jeweils eine Sicherheitsschicht und eine Übertragungsschicht aufweisen,
wobei im Sendebetrieb die Sicherheitsschicht für einen zu sendenden Sicherheitsdatenblock eine Sicherheitscode mithilfe eines Sicherheitscode-Bestimmungsverfahrens bestimmt und die Übertragungsschicht ein Datenpaket mit dem Sicherheitsdatenblock und dem Sicherheitscode für das Versenden auf der Datenübertragungsstrecke bildet, und
wobei im Empfangsbetrieb die Übertragungsschicht aus einem über die Datenübertragungsstrecke empfangenen Datenpaket einen Sicherheitsdatenblock und einen zugehörigen Sicherheitscode extrahiert und die Sicherheitsschicht mit dem Sicherheitscode-Bestimmungsverfahren den Sicherheitscode für den Sicherheitsdatenblock verifiziert,
wobei dem ersten Slave-Teilnehmer ein erstes Sicherheitscode-Bestimmungsverfahren und dem zweiten Slave-Teilnehmer ein zweites Sicherheitscode-Bestimmungsverfahren zugeordnet ist, und
wobei der Master-Teilnehmer und der ersten Slave-Teilnehmer für einen Austausch eines Sicherheitsdatenblock das erste Sicherheitscode-Bestimmungsverfahren und der Master-Teilnehmer und der zweite Slave-Teilnehmer für einen Austausch eines Sicherheitsdatenblock das zweiten Sicherheitscode-Bestimmungsverfahren verwenden.

2. Verfahren nach Anspruch 1, wobei das ersten und zweiten Sicherheitscode-Bestimmungsverfahren eine zyklische Redundanzprüfung durchführen, wobei dem ersten Sicherheitscode-Bestimmungsverfahren ein erstes Sicherheitscode-Generatorpolynom und dem zweiten Sicherheitscode-Bestimmungsverfahren ein zweites Sicherheitscode-Generatorpolynom zugeordnet ist, wobei der Master-Teilnehmer und der ersten Slave-Teilnehmer für einen Austausch eines Sicherheitsdatenblock das erste Sicherheitscode-Generatorpolynom für die zyklische Redundanzprüfung und der Master-Teilnehmer und der zweite Slave-Teilnehmer für einen Austausch eines Sicherheitsdatenblock das zweiten Sicherheitscode-Generatorpolynom für die zyklische Redundanzprüfung verwenden.

3. Verfahren nach Anspruch 2, wobei der ersten und zweiten Sicherheitsanforderungsstufe unterschiedliche Restfehlerwahrscheinlichkeiten für das Auftreten eines Fehlers zugeordnet sind und wobei der Hamming-Abstand des ersten Sicherheitscode-Generatorpolynoms sich von dem Hamming-Abstand des zweiten Sicherheitscode-Generatorpolynoms unterscheidet.

4. Verfahren nach einem der Ansprüche 1 bis 3, wobei eine Adressenvergabe für den wenigstens ersten Slave-Teilnehmer mit der ersten Sicherheitsanforderungsstufe und den wenigstens zweiten Slave-Teilnehmer mit der zweiten Sicherheitsanforderungsstufe unabhängig voneinander erfolgt.

5. Automatisierungsnetzwerk mit einem eine Sicherheitssteuerung ausführenden Master-Teilnehmer, wenigstens einem ersten Slave-Teilnehmer, dem eine erste Sicherheitsanforderungsstufe zugeordnet ist, und wenigstens einem zweiten Slave-Teilnehmer, dem eine zweite Sicherheitsanforderungsstufe zugeordnet ist,
wobei der Master-Teilnehmer, der erste Slave-Teilnehmer und der zweite Slave-Teilnehmer über eine Datenübertragungsstrecke miteinander verbunden sind und jeweils eine Sicherheitsschicht und eine Übertragungsschicht aufweisen, wobei im Sendebetrieb die Sicherheitsschicht für einen zu sendenden Sicherheitsdatenblock mit einem Sicherheitscode-Bestimmungsverfahren einen Sicherheitscode bestimmt und die Übertragungsschicht ein Datenpaket mit dem Sicherheitsdatenblock und dem Sicherheitscode für das Versenden auf der Datenübertragungsstrecke bildet, und
wobei im Empfangsbetrieb die Übertragungsschicht aus einem über die Datenübertragungsstrecke empfangenen Datenpaket einen Sicherheitsdatenblock und einen zugehörigen Sicherheitscode extrahiert und die Sicherheitsschicht mit dem Sicherheitscode-Bestimmungsverfahren den Sicherheitscode für den Sicherheitsdatenblock verifiziert,
wobei dem ersten Slave-Teilnehmer ein erstes Sicherheitscode-Bestimmungsverfahren und dem zweiten Slave-Teilnehmer ein zweites Sicherheitscode-Bestimmungsverfahren zugeordnet ist, und
wobei der Master-Teilnehmer und der ersten Slave-Teilnehmer für einen Austausch eines Sicherheitsdatenblock das erste Sicherheitscode-Bestimmungsverfahren und der Master-Teilnehmer und der zweite Slave-Teilnehmer für einen Austausch eines Sicherheitsdatenblock das zweiten Sicherheitscode-Bestimmungsverfahren verwenden.

6. Automatisierungsnetzwerk nach Anspruch 5, wobei das ersten und zweiten Sicherheitscode-Bestimmungsverfahren eine zyklische Redundanzprüfung durchführen, wobei dem ersten Sicherheitscode-Bestimmungsverfahren ein erstes Sicherheitscode-Generatorpolynom und dem zweiten Sicherheitscode-Bestimmungsverfahren ein zweites Sicherheitscode-Generatorpolynom zugeordnet ist,

wobei der Master-Teilnehmer und der ersten Slave-Teilnehmer für einen Austausch eines Sicherheitsdatenblock das erste Sicherheitscode-Generatorpolynom für die zyklische Redundanzprüfung und der Master-Teilnehmer und der zweite Slave-Teilnehmer für einen Austausch eines Sicherheitsdatenblock das zweiten Sicherheitscode-Generatorpolynom für die zyklische Redundanzprüfung verwenden.

7. Automatisierungsnetzwerk nach Anspruch 6, wobei der ersten und zweiten Sicherheitsanforderungsstufe unterschiedliche Restfehlerwahrscheinlichkeiten für das Auftreten eines Fehlers zugeordnet sind und wobei der Hamming-Abstand des ersten Sicherheitscode-Generatorpolynoms sich von dem Hamming-Abstand des zweiten Sicherheitscode-Generatorpolynoms unterscheidet.

8. Automatisierungsnetzwerk nach einem der Ansprüche 5 bis 7, wobei die Datenübertragungsstrecke ein Ethernetbasierender Feldbus ist.

Es folgen 5 Seiten Zeichnungen

Anhängende Zeichnungen

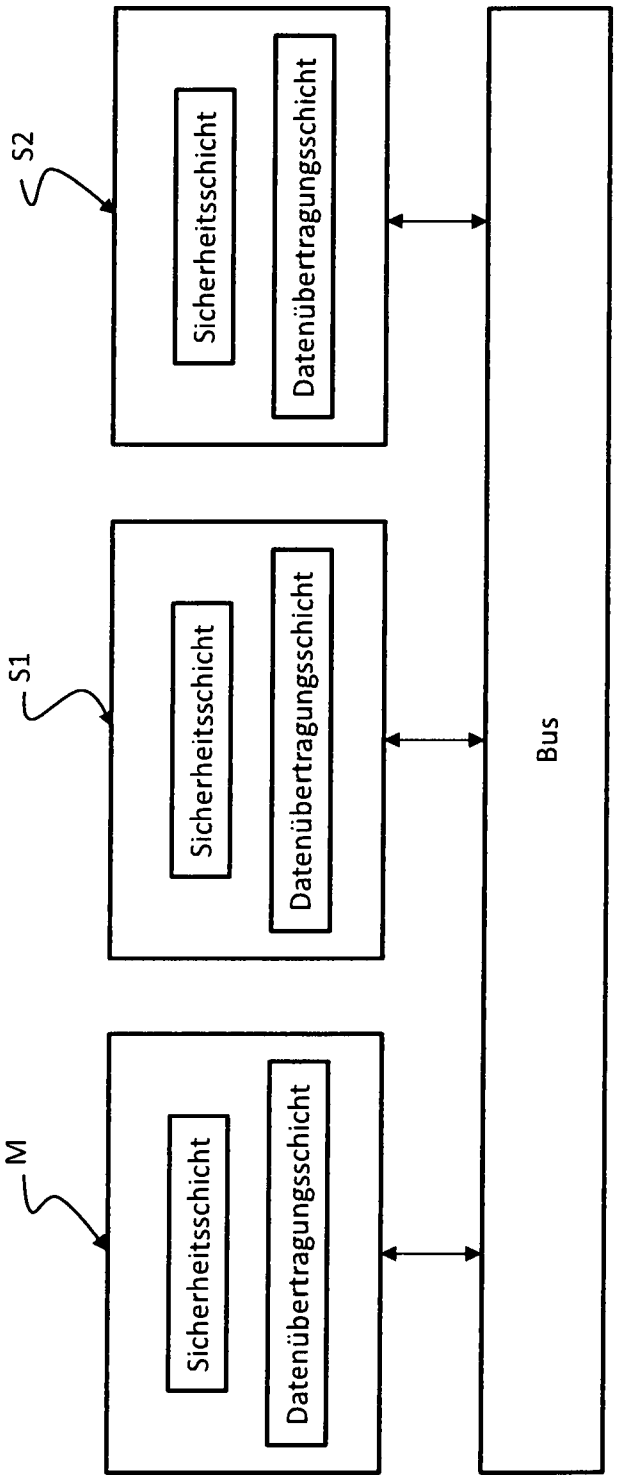


Fig. 1

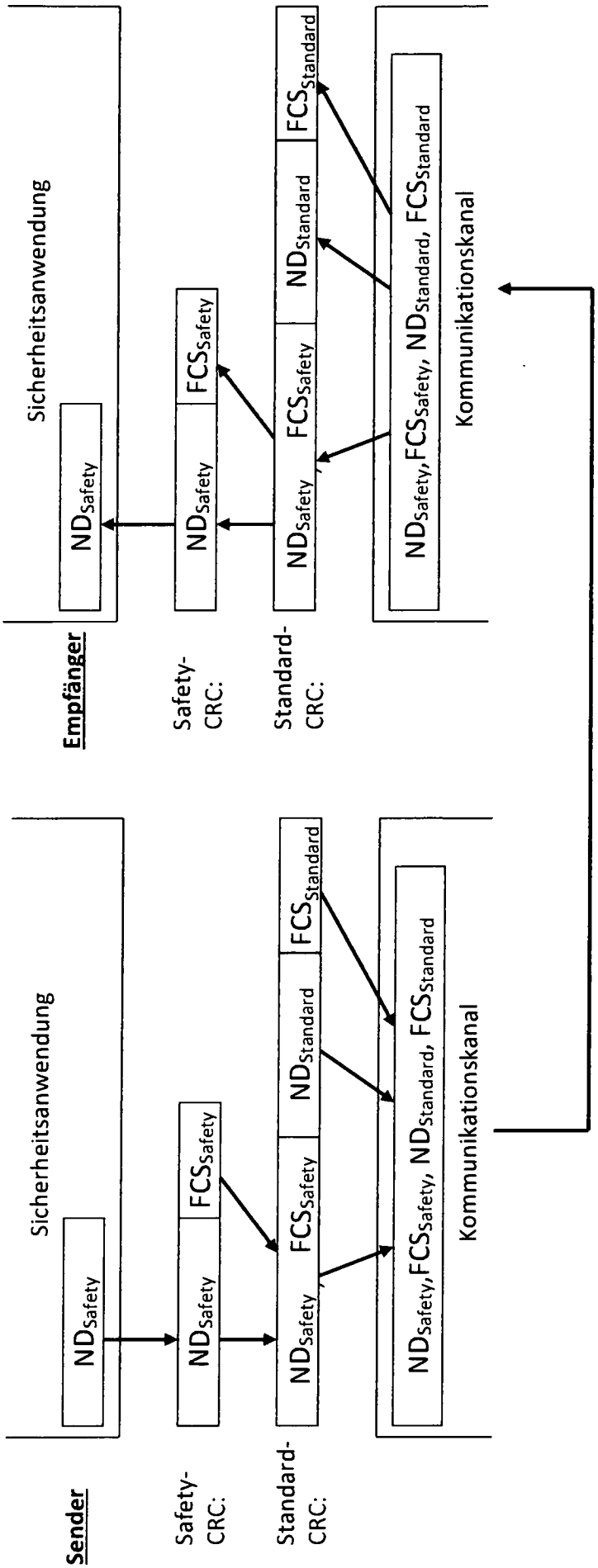

Sicherheitsanwendung
ND Safety
Empfänger
Safety-CRC:
ND Safety
FCS Safety
Standard-CRC:
ND Safety
FCS Safety
ND Standard
FCS Standard
ND Safety, FCS Safety, ND Standard, FCS Standard
Kommunikationskanal
Sicherheitsanwendung
ND Safety
Sender
Safety-CRC:
ND Safety
FCS Safety
Standard-CRC:
ND Safety
FCS Safety
ND Standard
FCS Standard
ND Safety, FCS Safety, ND Standard, FCS Standard
Kommunikationskanal

Fig. 2

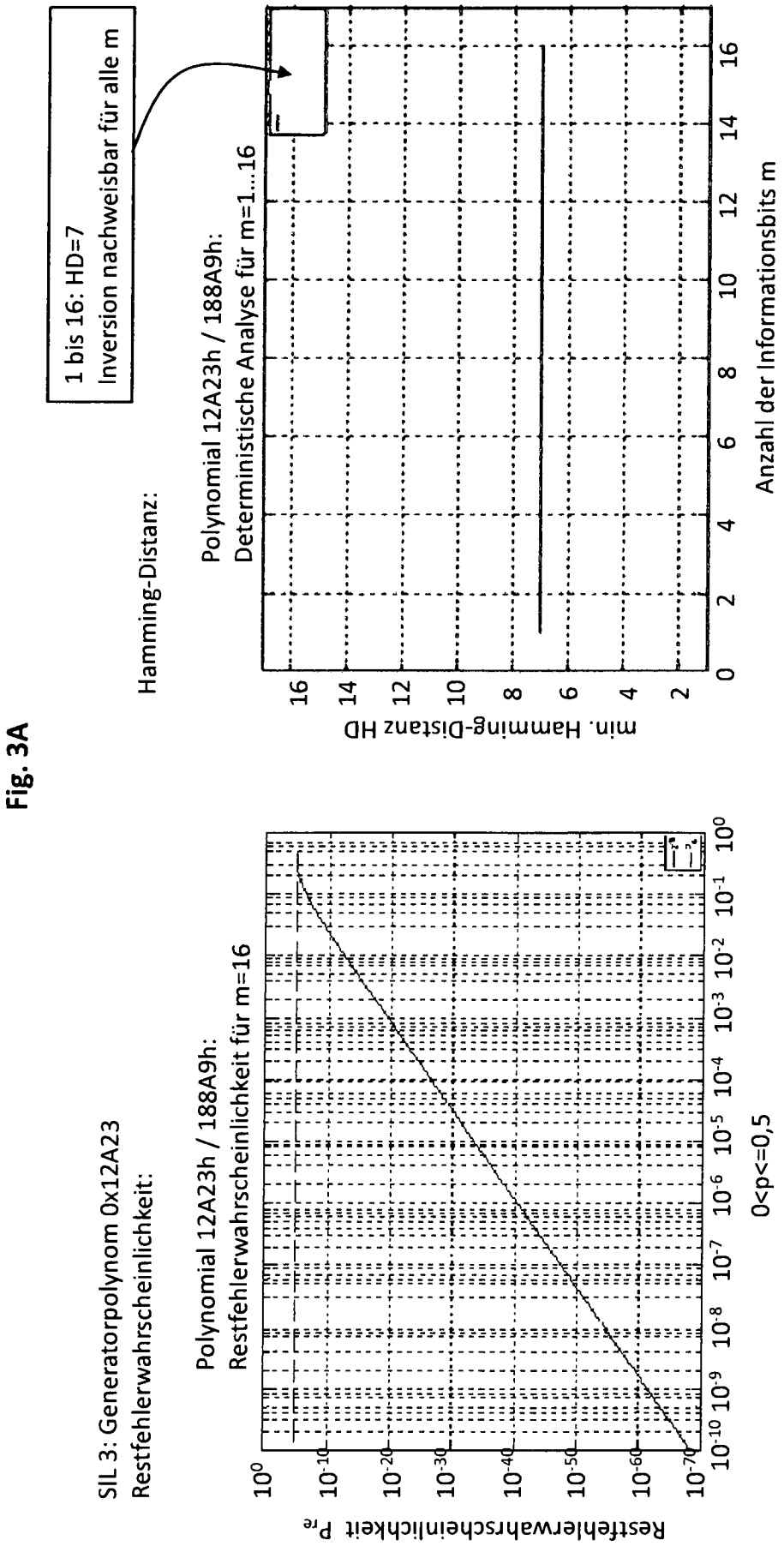

1 bis 16: HD=7
Inversion nachweisbar für alle m
Hamming-Distanz:
Polynomial 12A23h / 188A9h:
Deterministische Analyse für m=1...16
min. Hamming-Distanz HD
Anzahl der Informationsbits m
SIL 3: Generatorpolynom 0x12A23
Restfehlerwahrscheinlichkeit:
Polynomial 12A23h / 188A9h:
Restfehlerwahrscheinlichkeit für m=16
Restfehlerwahrscheinlichkeit Pre
0<p<=0,5

Fig. 3A

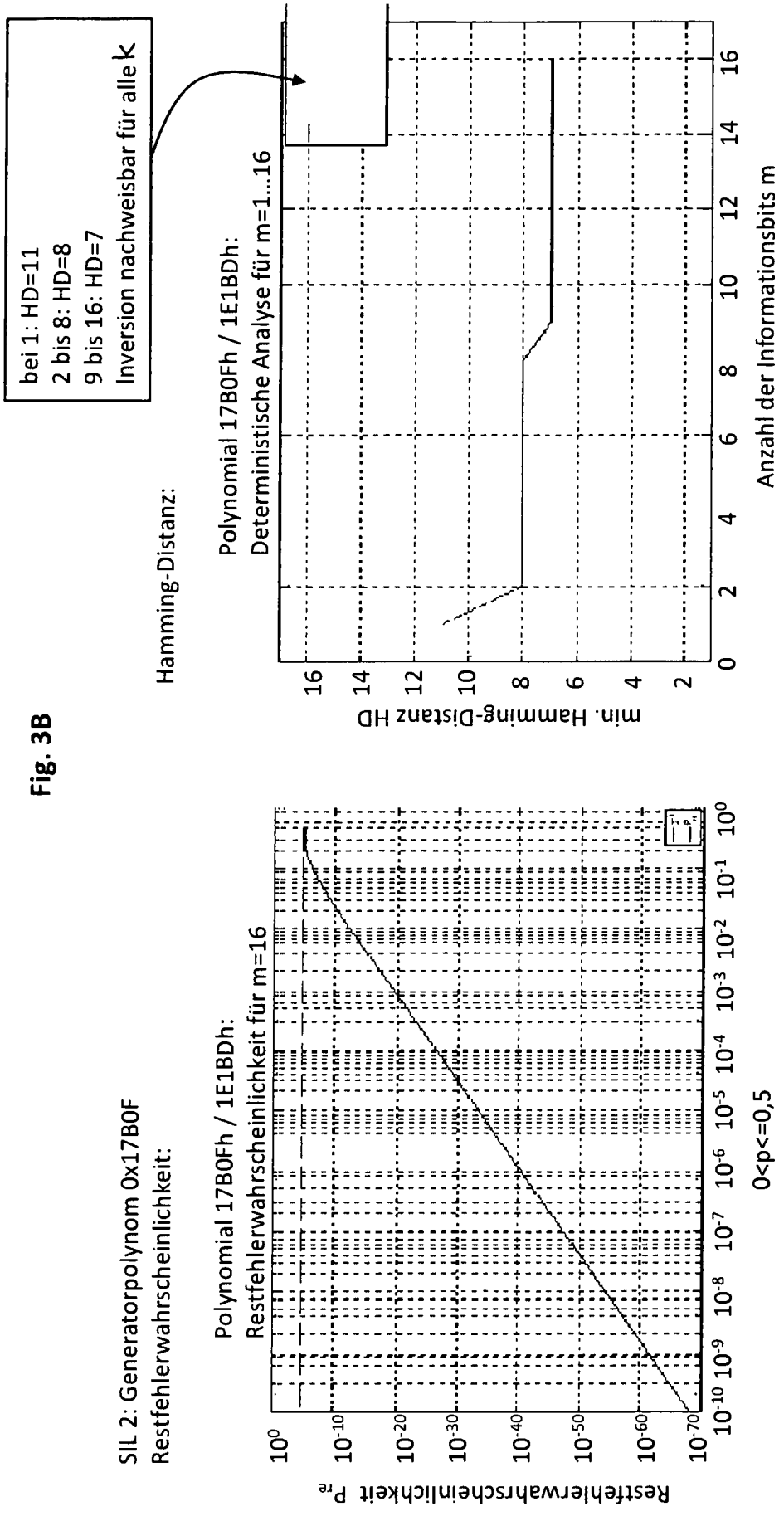

bei 1: HD=11
2 bis 8: HD=8
9 bis 16: HD=7
Inversion nachweisbar für alle k
Hamming-Distanz:
Polynomial 17B0Fh / 1E1BDh:
Deterministische Analyse für m=1..16
min. Hamming-Distanz HD
Anzahl der Informationsbits m
SIL 2: Generatorpolynom 0x17B0F
Restfehlerwahrscheinlichkeit:
Polynomial 17B0Fh / 1E1BDh:
Restfehlerwahrscheinlichkeit für m=16
Restfehlerwahrscheinlichkeit Pre
0<p<=0,5

Fig. 3B

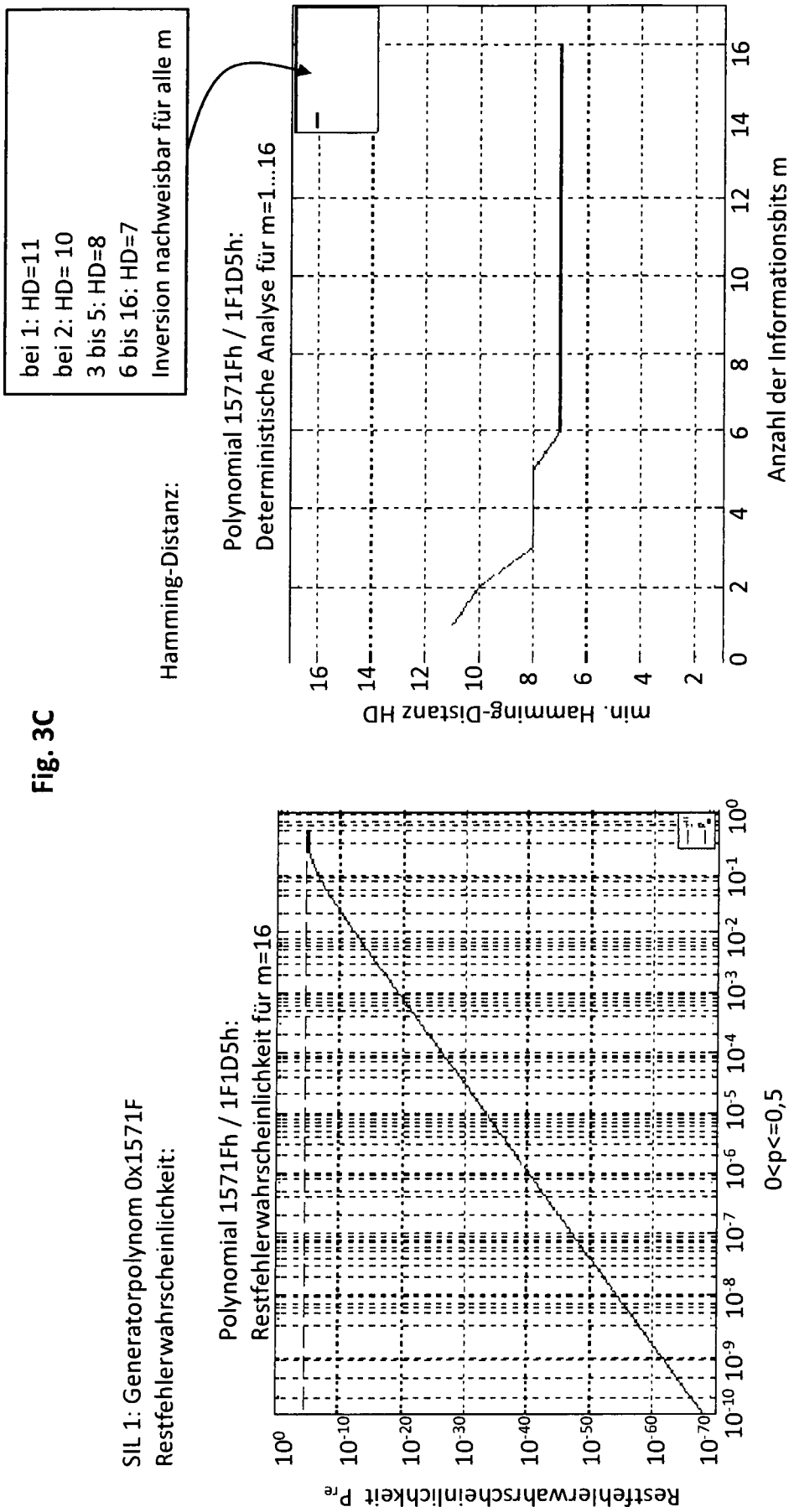

bei 1: HD=11
bei 2: HD= 10
3 bis 5: HD=8
6 bis 16: HD=7
Inversion nachweisbar für alle m
Hamming-Distanz:
Polynomial 1571Fh / 1F1D5h:
Deterministische Analyse für m=1...16
min. Hamming-Distanz HD
Anzahl der Informationsbits m
SIL 1: Generatorpolynom 0x1571F
Restfehlerwahrscheinlichkeit:
Polynomial 1571Fh / 1F1D5h:
Restfehlerwahrscheinlichkeit für m=16
Restfehlerwahrscheinlichkeit P_re
0<p<=0,5

Fig. 3C