(19) **Bundesrepublik Deutschland**
Deutsches Patent- und Markenamt

(10) **DE 103 14 721 A1** 2004.11.11

(12) # Offenlegungsschrift

(21) Aktenzeichen: **103 14 721.7**
(22) Anmeldetag: **31.03.2003**
(43) Offenlegungstag: **11.11.2004**

(51) Int Cl.[7]: **H04L 12/40**
H04L 9/00

(71) Anmelder:
Endress + Hauser GmbH + Co. KG, 79689 Maulburg, DE

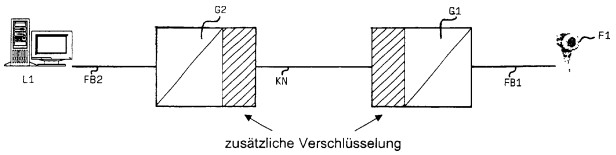
(74) Vertreter:
Andres, A., Pat.-Anw., 79576 Weil am Rhein

(72) Erfinder:
Kilian, Markus, 79100 Freiburg, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Verfahren zur sicheren Datenübertragung über einen Feldbus**

(57) Zusammenfassung: Bei einem Verfahren zur sicheren Datenübertragung über einen Feldbus FB1 der Prozessautomatisierungstechnik werden die Daten verschlüsselt über den Feldbus FB1 übertragen.



Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zur sicheren Datenübertragung über einen Feldbus gemäß dem Oberbegriff des Anspruchs 1.

[0002] In der Prozessautomatisierungstechnik werden häufig Feldbusse zur Übertragung von Daten zwischen Feldgeräten und Steuereinheiten eingesetzt. Die Datenübertragung erfolgt nach den bekannten Standards (Profibus, FF bzw. HART). Bisher werden die Daten unverschlüsselt übertragen, d.h. sie können von jedermann, der Zugriff zum Feldbus hat, mitgelesen werden. Ebenso können Daten in unbefugter Weise an Feldgeräte übertragen werden um Einstellungen (z.B. Parameter) dieser Feldgeräte zu ändern.

[0003] Aus Sicherheitsgründen sollte der Zugriff auf die Daten eines Feldbusses daher gesichert werden.

[0004] Aufgabe der vorliegenden Erfindung ist es deshalb, ein Verfahren zur sicheren Datenübertragung über einen Feldbus der Prozessautomatisierungstechnik anzugeben, das zum einen eine sichere Datenübertragung erlaubt, und zum anderen einfach und kostengünstig einsetzbar ist.

[0005] Gelöst wird diese Aufgabe durch das im Anspruch 1 angegebene Verfahren.

[0006] Vorteilhafte Weiterentwicklungen der Erfindungen sind in den Unteransprüchen angegeben.

[0007] Die wesentliche Idee der Erfindung besteht darin, Daten, die über einen Feldbus der Prozessautomatisierungstechnik übertragen werden, zu verschlüsseln.

[0008] In vorteilhafter Weise erfolgt die Verschlüsselung im Feldgerät selbst d.h. direkt bei der Datenquelle.

[0009] Häufig sind Feldbusse nicht mehr abgeschlossene Systeme, sondern über Gateways mit anderen Kommunikationsnetzen verbunden. Dadurch können die Daten auch über zusätzliche, eventuell öffentliche Kommunikationsnetze übertragen werden.

[0010] In vorteilhafter Weise kann im Gateway daher noch eine zusätzliche Verschlüsselung erfolgen.

[0011] Das erfindungsgemäße Verfahren ist für alle bekannten Feldbusse (z. B. Profibus, FF, HART, etc.) einsetzbar.

[0012] Der zur Verschlüsselung notwendige Schlüssel kann entweder über den Feldbus selbst oder aber vor Ort über die Vor-Ort-Bedienung oder über die Service-Schnittstelle ins Feldgerät übertragen werden, sowie aufgrund einer Geräteeigenschaft (z.B. der Seriennummer oder eines eingegebenen Wertes) generiert werden.

[0013] Der Schlüssel kann zur symmetrischen bzw. asymmetrischen Verschlüsselung der Daten dienen.

[0014] Nachfolgend ist die Erfindung anhand eines in der Zeichnung dargestellten Ausführungsbeispiels näher erläutert.

[0015] In der einzigen Figur ist ein Feldgerät F1 über einen Feldbus FB1, ein öffentliches Kommunikationsnetz KN und einen weiteren Feldbus FB2 mit einem Leitsystem L1 verbunden. Dadurch dass die Verschlüsselung der Daten bereits im Feldgerät F1 erfolgt, ist ein unberechtigtes Abhören der Daten auch auf dieser Teilstrecke der gesamten Datenübertragungsstrecke nicht möglich, zusätzlich ist die sichere Datenübertragung nicht auf in externen Komponenten eventuell integrierte Mechanismen angewiesen.

[0016] Der Feldbus FB1 ist über ein Gateway G1 mit einem öffentlichen Kommunikationsnetz KN verbunden. Die weitere Datenübertragung erfolgt über einen Gateway G2 und einen Feldbus FB2 zum Leitsystem L1. Im Gateway G1 kann eine zusätzliche Verschlüsselung der Daten stattfinden. Bei dem erfindungsgemäßen Verfahren ist die gesamte Datenübertragungsstrecke vom Feldbus F1 über das öffentliche Kommunikationsnetz KN sowie dem Feldbus FB2 verschlüsselt. In gleicher Weise kann die Datenübertragung vom Leitsystem L1 zum Feldgerät F1 hin in verschlüsselter bzw. signierter Form erfolgen.

[0017] Um Daten im Feldgerät F1 verschlüsseln zu können, muss der Schlüssel in diesem abgespeichert werden. Eine Möglichkeit den Schlüssel zum Feldgerät F1 zu übertragen, ist vom Leitsystem L1 aus. Der Schlüssel kann aber auch direkt am Feldgerät z. B. über die Service-Schnittstelle bzw. die Vor-Ort-Bedienung eingegeben werden oder auf einem anderen Weg dorthin gelangen.

[0018] Bei der vorliegenden Erfindung werden die Daten die über einen Feldbus der Prozessautomatisierungstechnik übertragen werden verschlüsselt, um einen unbefugten Zugriff auf die Daten bzw. auf die an dem Feldbus angeschlossenen Feldgeräte zu verhindern.

Patentansprüche

1. Verfahren zur sicheren Datenübertragung über einen Feldbus der Prozessautomatisierungstechnik, **dadurch gekennzeichnet**, dass die Daten verschlüsselt sind.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Verschlüsselung im Feldgerät z. B. F1 erfolgt.

3. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der Feldbus FB1 über ein Gateway G1 mit einem öffentlichen Kommunikationsnetz KN verbunden ist.

4. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der Feldbus entsprechend dem Profibus, Foundation Fieldbus bzw. HART Standard ausgelegt ist.

5. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der Schlüssel über den Feldbus FB1 zum Feldgerät F1 übertragen wird.

6. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der Schlüssel vor Ort ins Feldgerät z.B. F1 übertragen wird.

7. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der Schlüssel aufgrund einer Geräteeigenschaft im Feldgerät z.B. F1 generiert wird.

8. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der Schlüssel zur symmetrischen bzw. asymmetrischen Verschlüsselung der über den Feldbus FB1 übertragenen Daten dient.

Es folgt ein Blatt Zeichnungen

Anhängende Zeichnungen

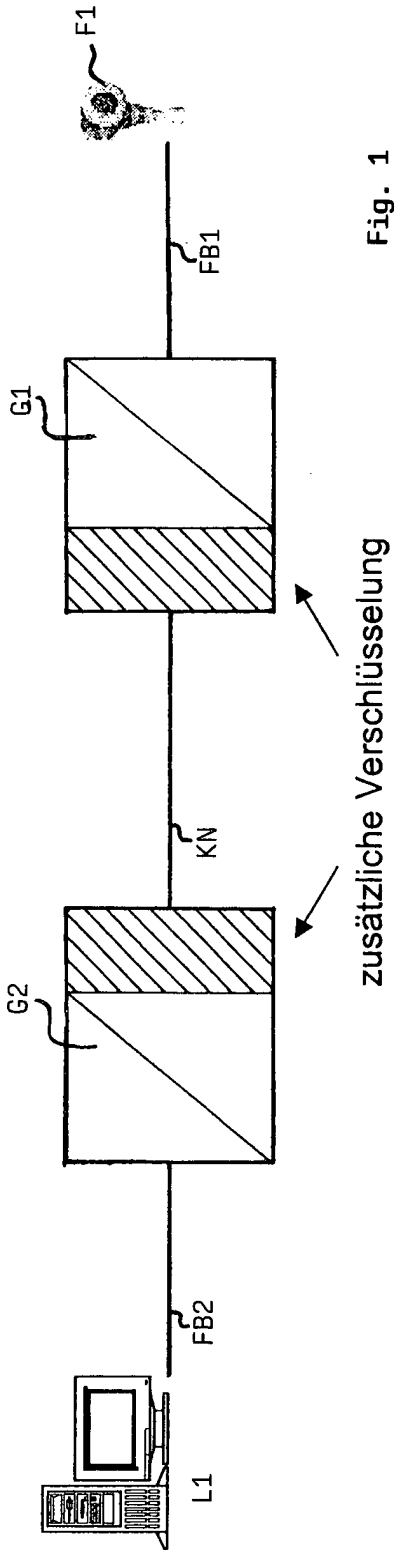


Fig. 1