



(19)
Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 11 2005 001 808 T5** 2007.09.13

(12)

Veröffentlichung

der internationalen Anmeldung mit der
(87) Veröffentlichungs-Nr.: **WO 2006/014888**
in deutscher Übersetzung (Art. III § 8 Abs. 2 IntPatÜG)
(21) Deutsches Aktenzeichen: **11 2005 001 808.3**
(86) PCT-Aktenzeichen: **PCT/US2005/026375**
(86) PCT-Anmeldetag: **25.07.2005**
(87) PCT-Veröffentlichungstag: **09.02.2006**
(43) Veröffentlichungstag der PCT Anmeldung
in deutscher Übersetzung: **13.09.2007**

(51) Int Cl.⁸: **G05B 11/01** (2006.01)
G05B 9/02 (2006.01)

(30) Unionspriorität:

60/591,286	27.07.2004	US
10/948,085	23.09.2004	US

(71) Anmelder:

MKS Instruments Inc., Andover, Mass., US

(74) Vertreter:

**Grünecker, Kinkeldey, Stockmair &
Schwanhäusser, 80538 München**

(72) Erfinder:

**Khalil, Nidal, San Jose, Calif., US; Sifnatsch,
Guenter, Santa Clara, Calif., US; Lev-Ami, Uzi,
Mountain View, Calif., US; Hadar, Ron, Cupertino,
Calif., US**

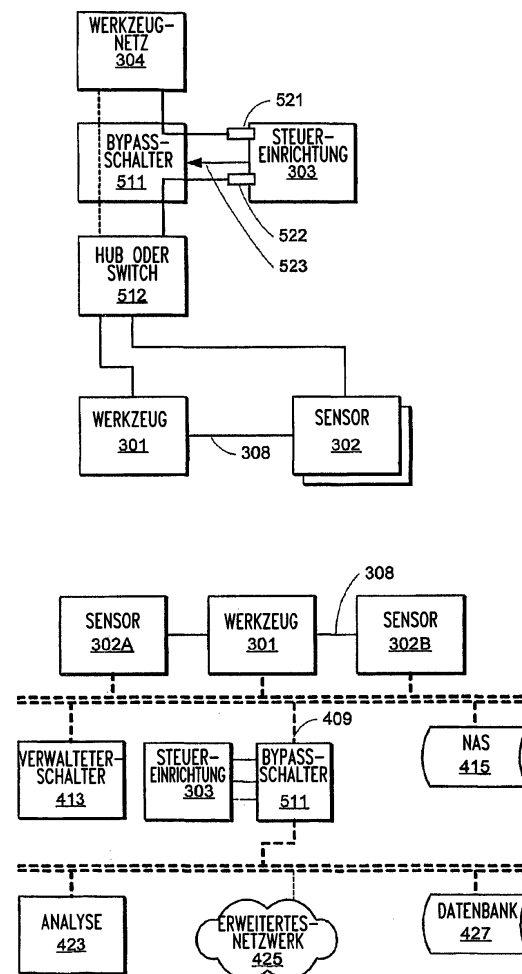
(54) Bezeichnung: **Verfahren und Vorrichtung für das ausfallsichere Schalten einer intelligenten Steuereinrichtung**

(57) Hauptanspruch: Verfahren zum transparenten Herstellen einer Verbindung zwischen einer ersten und einer zweiten Einrichtung im Fall eines Ausfalls einer Zwischeneinrichtung, wobei das Verfahren umfasst:

Verbinden der ersten und der zweiten Einrichtung mit jeweils einer ersten und einer zweiten Netzwerkschnittstelle einer Zwischeneinrichtung, wobei die erste und die zweite Netzwerkschnittstelle Datenverknüpfungsschicht-Kennzeichnungen aufweisen, die sich von denjenigen unterscheiden, die mit der ersten oder der zweiten Einrichtung assoziiert sind,

wobei die Zwischeneinrichtung in einem normalen Modus zwischen der ersten und der zweiten Einrichtung adressierte Mitteilungen handhabt, während sie wiederholt Signale an einen Ausfallsicherungsschalter zu ihrem fortgesetztem korrekten Betrieb sendet, und

wobei der Ausfallsicherungsschalter bei einer Unterbrechung der wiederholten Signale zu dem korrekten Betrieb von der Zwischeneinrichtung zu einem Ausfallsicherungsmodus sichert, indem er die erste und die zweite Einrichtung direkt über eine Datenverbindung verbindet, die die Zwischeneinrichtung umgeht.



Beschreibung**Hintergrund der Erfindung**

[0001] Die vorliegende Erfindung betrifft den ausfallsicheren Betrieb von Steuereinrichtungskomponenten, die zwischen einer steuernden Host bzw. ersten Einrichtung und einem Werkzeug bzw. einer zweiten Einrichtung eingefügt sind. Insbesondere betrifft die vorliegende Erfindung das Herstellen einer direkten Verbindung zwischen der ersten und der zweiten Einrichtung nach dem Ausfall einer Steuereinrichtung, die Datenübertragungen zwischen der ersten und der zweiten Einrichtung vermittelt. Eine Umgebung, in der die vorliegende Erfindung nützlich ist, ist ein Halbleiterproduktionswerk mit einem ein Host und Werkzeugen/Sensoren, zwischen denen eine intelligente Steuereinrichtung eingefügt ist, wobei die Steuereinrichtung zum Vermitteln von Kommunikationen zwischen einem Werkzeug, mit dem Werkzeug assoziierten Sensoren und Datennutzern wie etwa einem Host-System oder verteilten Prozessoren verwendet wird.

[0002] Das Moore-Gesetz sagt ein exponentielles Wachstum der Computerleistung bei sich stets sinkenden Preisen voraus. Aufgrund dieses dynamischen Wachstums der Verarbeitungsleistung könnte man denken, dass die Herstellung von Halbleiterkomponenten ein risikofreudiges Geschäft wie etwa das Spekulieren um Öl ist. Das Gegenteil ist jedoch der Fall. Weil die Fertigung sehr kostspielig ist und die Fertigungsprozesse sehr empfindlich auch gegenüber kleinen Fehlern sind, ist die Herstellung von Halbleiterkomponenten ein eher konservatives Geschäft. Qualifikationszyklen und Standards für neue Maschinen sowie Modifikationen an alten Maschinen sind langwierig und aufwändig. Auch kleinste Änderungen werden ausgiebig geprüft, bevor sie für die Produktion freigegeben werden.

[0003] Zu den wichtigen Einrichtungen in einem Werk für die Halbleiterherstellung gehören Werkzeuge (z.B. Aufdampfungskammern, Reaktoren), Sensoren zum Überwachen der Werkzeuge (z.B. FTIR-Sensoren, Massenspektrographen, Thermoelemente) und Hosts oder verteilte Prozessoren, die Daten aus den Sensoren zu dem Betrieb der Werkzeuge speichern und analysieren.

[0004] Eine ältere Anmeldung beschreibt ein transparentes Verfahren zum Überwachen von Daten aus den Sensoren und zum Weiterleiten derselben zu den Hosts oder verteilten Prozessoren unter Verwendung von mit hoher Geschwindigkeit arbeitenden und fehlerresistenten Technologien wie etwa TCP/IP über Ethernet. Die ältere Anmeldung wurde durch die Erfinder Uzi Lev-Ami und Yossef Ilan Reich unter dem Titel „Method and Apparatus for Monitoring Host to Tool Communications“ und der Anmeldungsnummer 09/935,213 am 22. August 2001 eingereicht und ist hier unter Bezugnahme eingeschlossen. Die ältere Anmeldung beschreibt einen Überwachungsposten, der eine serielle Kommunikation von einem Werkzeug oder Sensor unter Verwendung eines optisch isolierten Steckers überwachen kann. Unter Verwendung des Überwachungsansatzes kann man belegen, dass die Kommunikationen im Werk und die Datensammlungs-Infrastruktur verbessert werden können, ohne dass dazu Modifikationen an Werkzeugen oder Sensoren erforderlich sind, sodass also ein geringes Risiko besteht. Die Verbesserungsmöglichkeiten können demonstriert werden, ohne dass dazu die bestehende Kommunikationsinfrastruktur demontiert werden muss.

[0005] Die nächste Revolution in den Werkseinrichtungen und den nachgeordneten Analysefähigkeiten sehen das Hinzufügen von intelligenten Steuereinrichtungen zur Vermittlung von Kommunikationen zwischen den Werkzeugen und Sensoren auf der einen Seite und den Werkzeug-Hosts oder verteilten Distributoren auf der anderen Seite vor, ohne dass dazu die analytischen Eigenschaften der Sensoren ersetzt oder verändert zu werden brauchen. Die erhöhte Prozessorleistung und die verminderten Speicherkosten ergeben Möglichkeiten für Konfigurationen, die zuvor nicht in einer Werksumgebung realisiert hätten werden können. Eine zweite ältere Anmeldung der Erfinder Uzi Lev-Ami, Guenter Sifnatsch und Mark Attwood mit dem Titel „Controller and Method to Mediate Data Collection from Smart Sensors for Fab Applications“ und der US-Patentanmeldungsnummer 10/819,903 vom 7. April 2004 beschreibt eine intelligente Steuereinrichtung mit verschiedenen Fähigkeiten.

[0006] Dabei ergibt sich die Möglichkeit, die analytischen Fähigkeiten einer intelligenten Steuereinrichtung oder einer anderen über das Netzwerk verbundenen Einrichtung, die Kommunikationen zwischen zwei anderen Einrichtungen vermittelt, die auch zu einer direkten Kommunikation fähig sind, durch einen Ausfallsicherungsschalter zu ergänzen, der die anderen Einrichtungen direkt miteinander verbindet, wenn die Zwischeneinrichtung ausfällt oder blockiert ist. Daraus können zuverlässigere Installationen von Zwischeneinrichtungen resultieren.

Zusammenfassung der Erfindung

[0007] Die vorliegende Erfindung betrifft die Steuerung und Datensammlung von mit Werkzeugen assoziierten Sensoren. Insbesondere betrifft die vorliegende Erfindung die Verwendung einer Steuereinrichtung zum Vermitteln von Kommunikationen zwischen einem Werkzeug, mit dem Werkzeug assoziierten Sensoren und Datennutzern wie etwa dem Host-System oder verteilten Prozessoren. Besondere Aspekte der vorliegenden Erfindung werden in den Ansprüchen, der Beschreibung und den Zeichnungen erläutert.

Kurzbeschreibung der Zeichnungen

[0008] [Fig. 1](#) zeigt eine Umgebung, in der Aspekte der vorliegenden Erfindung besonders nützlich realisiert werden können.

[0009] [Fig. 2](#) ist ein Blockdiagramm einer Steuereinrichtung, die mit Werkzeugen, Sensoren und einem Werkzeug-Host kommuniziert.

[0010] [Fig. 3](#) ist ein Blockdiagramm einer Steuereinrichtung, die einen Kommunikationskanal eines einzelnen Typs verwendet, um mit einem Werkzeug, einem Sensor und einem Werkzeug-Host zu kommunizieren.

[0011] [Fig. 4](#) zeigt die Verwendung von mehreren Typen von Kommunikationskanälen.

[0012] [Fig. 5](#) ist ein Blockdiagramm, in dem ein Ausfallsicherungsschalter zu einem Netzwerk hinzugefügt ist.

[0013] [Fig. 6](#) ist ein Blockdiagramm, in dem ein Ausfallsicherungsschalter zu einem anderen Netzwerk hinzugefügt ist.

Ausführliche Beschreibung

[0014] Die folgende ausführliche Beschreibung nimmt auf die Figuren Bezug. Es werden bevorzugte Ausführungsformen beschrieben, um die vorliegende Erfindung zu erläutern, ohne dadurch den durch die Ansprüche definierten Erfindungsumfang einzuschränken. Der Fachmann kann verschiedene Variationen an den im Folgenden beschriebenen Ausführungsformen vornehmen.

Einführung

[0015] Die SECS-Mitteilungsprotokolle, die Kommunikationsinfrastruktur und die durch die Werkzeuge und andere automatisierte oder halbautomatisierte Einrichtungen in Halbleiterwerken verwendeten Hosting-Modi wurden bereits vor Jahren entwickelt, als die Kommunikations- und Verarbeitungsgeschwindigkeiten ziemlich begrenzt waren. Die SECS-Mitteilungsprotokolle für Werksanwendungen wurden für die Verwendung von langsamen, seriellen Kommunikationen entworfen. Diese Mitteilungsprotokolle enthielten strukturierte Mitteilungen, die auch bei einer langsamen Kommunikation schnell übertragen werden konnten. Strukturierte Mitteilungen waren und bleiben schwierig zu übersetzen und zu verstehen. Die Schwierigkeiten sind noch größer, wenn eine erste Mitteilung einen Kontext für eine Antwort setzt und eine zweite, antwortende Mitteilung den Kontext nicht wiederholt; das heißt, die kontextsensitive Mitteilung ist nur dann bedeutungsvoll, wenn sie mit der entsprechenden den Kontext setzenden Mitteilung gepaart wird. Die Kommunikation erfolgte gewöhnlich über eine RS-232- oder äquivalente serielle Kommunikation entlang von dedizierten Kanälen ähnlich wie bei Modems oder Telefonleitungen für Endgeräte und Computer im Zeitteilungsbetrieb. Die Host-Systeme konnten auf Mainframes, Mini-Computern oder Workstations ausgeführt werden. Die Host-Systeme waren gewöhnlich monolithisch und steuerten bzw. überwachten alle oder einen wesentlichen Satz von Werkzeugen in einem Werk. Die Host-Systeme beruhten auf Adaptern, um eine Schnittstelle zu Werkzeugen und Sensoren herzustellen. Die Host-Systeme empfingen gewöhnlich Daten von den Werkzeugen und Sensoren und gaben Steuerbefehle an die Werkzeuge aus. Die Host-Systeme empfingen und erzeugten häufig ein signifikantes Volumen an seriellen Kommunikationsmitteilungen.

[0016] Unter einem Host sind hier im breiten Sinne sowohl Werkzeugsteuerungs-Hosts als auch begrenzte oder flexiblere verteilte Prozessoren zu verstehen. Die Werkzeug-Hosts umfassen sowohl Hosts mit umfassenden, integrierten Werkzeug-Steuerungsfunktionen als auch Hosts, die auf verteilten Prozessoren mit begrenzteren, aufgabenspezifischen Funktionen ausgeführt werden. Die Werkzeuge umfassen Produkte wie etwa die FAB300 (TM)-Software von Consilium, die ein einzelnes umfassendes Werksverwaltungssystem vorsieht, das durch eine zentralisierte Definition von kundenspezifischen Geschäftsprozessen betrieben wird. Die-

se Kategorie von Werkzeug-Hosts ist ausgebildet, um herkömmliche Fertigungsausführungssysteme zu ersetzen, die vorgesehen sind, um durch verschiedene Hersteller angebotene Werkzeuge zu steuern. An dem zu den herkömmlichen Herstellungsausführungssystemen entgegen gesetzten Ende des Werkzeug-Host-Spektrums können Komponentenprozesse auf verteilten Prozessoren ausgeführt werden, um verschiedene spezifische Funktionen zu handhaben, ohne dass es sich dabei um umfassende Verwaltungssysteme handelt. Entlang des Spektrums kann ein Produkt wie etwa die FAB300 (TM)-Software als ein Werkzeugsteuerungs-Host für bestimmte Zwecke und ein auf einem verteilten Prozessor ausgeführter Prozess für andere Zwecke vorgesehen sein.

[0017] In den vorstehend genannten Anmeldungen wurde eine entfernbare Überwachungseinrichtung beschrieben, die einen verdrahteten Kommunikationskanal zwischen einem oder mehreren Werkzeug-Hosts und einem oder mehreren Werkzeugen überwachen kann. Die Überwachungseinrichtung ist passiv. Sie kann optional eine Standard-Isolationseinrichtung umfassen, um den Kommunikationskanal von durch die Überwachungseinrichtung erzeugten Geräuschen zu schützen. Diese Isolationseinrichtung könnte einen optischen Isolator, einen Verstärker mit hoher Impedanz oder andere Komponenten umfassen, die den verdrahteten Kommunikationskanal effektiv von der Überwachungseinrichtung isolieren. Der verdrahtete Kommunikationskanal kann ein RS-232-, RS-422- oder CAN-konformer Kanal sein, wobei es sich jedoch auch um einen der zuvor genannten Kommunikationskanäle handeln kann.

Steuereinrichtungen und intelligente Sensoren

[0018] Der in einer anderen, älteren Anmeldung beschriebene Ansatz verwendet intelligente Steuereinrichtungen und intelligente, kontextbewusste Sensoren. Eine intelligente Steuereinrichtung kennt den Status des Werkzeugs und/oder der Werkstücke (z.B. der Wafer oder Masken), die das Werkzeug verarbeitet. Diese Typen von Steuereinrichtungen kommunizieren mit intelligenten Sensoren, die auf Werkzeug- und Werkstück-Statusinformationen reagieren. Anstatt von Rekonfigurationsbefehlen wie etwa Werkzeug- und Werkstück-Statusänderungen abzuhängen, überwachen die Sensoren Statusänderungen und reagieren auf diese. Sie reagieren auf vorprogrammierte Weise auf die Statusänderungen und erfordern keine Rekonfigurationsbefehle.

[0019] Die neuen, intelligenten Steuereinrichtungen ändern das Betriebsmodell für Werkzeuge, Sensoren, Steuereinrichtungen und Datennutzer. Die Steuereinrichtungen kennen den Werkzeug- und Werkstück-Status auf die eine oder andere Weise. Eine Steuereinrichtung kann Befehle zum Steuern eines Werkzeugs überwachen und dieselben weiterleiten. Alternativ hierzu kann das Werkzeug seinen Status an die Steuereinrichtung bekannt geben. Die Steuereinrichtung kann den Status des Werkzeugs auch abfragen, und zwar periodisch oder in Reaktion auf Ereignisse, bei denen die Steuereinrichtung einen Bedarf für weitere Abfragen erkennt. Die Steuereinrichtungen kommunizieren die Statusinformationen zu den Sensoren. Die Statusinformationen können sich auf das Werkzeug oder Werkstück beziehen. Die Sensoren sind vorkonfiguriert, um auf die Statusinformationen zu antworten. Als Antwort auf die Statusinformationen können die Sensoren einen Datensammlungsplan verwenden, sich selbst kalibrieren, einen Ausgabebereich setzen oder Daten mit den aktuellen Statusinformationen assoziieren. Die Steuereinrichtungen kommunizieren die von den Sensoren gesammelten Daten zu Datennutzern. Ein Datennutzer kann ein herkömmlicher Werkzeug-Host sein, der auf einem Mainframe ausgeführt wird, oder es kann sich um eine neuere Software handeln, die auf verteilten Prozessoren ausgeführt wird. Ein Datennutzer kann ein monolithisches System sein oder durch verknüpfte Pakete gebildet werden, die unabhängig oder kooperativ betrieben werden. Die Steuereinrichtungen können auch Daten von den Sensoren überwachen, interessante Ereignisse identifizieren und weitere Daten anfordern, die bereits gesammelt wurden, oder den Sammlungsplan für die Sensoren in Reaktion auf die überwachten Daten ändern.

Verschiedene Betriebsumgebungen

[0020] [Fig. 1](#) zeigt eine Umgebung, in der die Aspekte der vorliegenden Erfindung besonders nützlich sind. Es werden eine Verarbeitungskammer **125**, verschiedene Ein- und Ausgänge zu und von der Verarbeitungskammer sowie Sensoren, Steuerkanäle und Steuereinrichtungen gezeigt. Die Kammer **125** kann für verschiedene Reaktionen wie etwa das Aufdampfen, Reinigen, Ätzen, Implantieren, Veraschen usw. verwendet werden. Andere Typen von Werkzeugen, die nicht in dieser Figur gezeigt sind, können auch von den Aspekten der vorliegenden Erfindung profitieren.

[0021] Es ist ein Werksnetzwerk **111** vorgesehen, auf das möglicherweise über das Internet zugegriffen werden kann und das als VPN-Netzwerk oder WAN-Netzwerk über eine Steuereinrichtung, eine Firewall oder ei-

nen andere Verbindung 162 kontrolliert auf ein Werkzeugnetzwerk **112** zugreifen kann. Das Werkzeugnetz ist in dieser Figur mit Steuereinrichtungen und Sensoren verbunden gezeigt, die in einem Ring mit der Verarbeitungskammer **125** verbunden sind. Dem Fachmann sollte jedoch deutlich sein, dass diese Architektur lediglich beispielhaft ist und auch eine serielle Kommunikation, ein Ethernet oder eine geschichtete Kommunikation anstelle eines Rings in einem Werk verwendet werden kann.

[0022] Gasförmige Eingaben zu der Reaktionskammer **125** umfassen Gasse, die durch Gaskastendruckwandler **113** und Massenfluss-Steuereinrichtungen (MFCs) **114** hindurchgehen. Einige Gase können durch einen Ozoneerzeuger **133** hindurchgehen. Andere Gase und Gasmischungen können durch einen Reaktionsgaserzeuger **115** und eine Gaszusammensetzungs-Überwachungseinrichtung **117** hindurchgehen. Der Reaktionsgaserzeuger **115** kann Plasma entweder innerhalb oder außerhalb der Verarbeitungskammer **125** erzeugen. Die Gaszusammensetzungs-Überwachungseinrichtung **117** kann seriell oder parallel mit dem Reaktionsgaserzeuger verbunden sein. Die Massenfluss-Steuereinrichtungen **114** stehen in einer Gaskommunikation mit dem Reaktionsgaserzeuger **115** und der Gaszusammensetzungs-Überwachungseinrichtung **117** und vermittelt oder direkt in einer Gaskommunikation mit der Verarbeitungskammer **125**. Die Gaseingabeeinrichtungen **113**, **114**, **133**, **115** und **117** stehen in einer Kommunikation mit einer oder mehreren digitalen Steuereinrichtungen **142**, Kammersteuereinrichtungen **152** und Verbindungspunkten **162**. Diese Kommunikationen umfassen sowohl eine Steuerung als auch eine Telemetrie. Diese Einrichtungen können sowohl Steuereinrichtungen als auch Sensoren umfassen, die auf den Betrieb der Einrichtungen oder die Ein-/Ausgabe der Gase reagieren.

[0023] Andere Eingänge können eine Materialzufuhr **134**, ein Kühlsystem **145** und verschiedene Leistungseinspritzer **153**, **154** und **155** umfassen. Die Reaktionskammer **125** kann eine Aufdampfkammer, eine Ätzeinrichtung, eine thermische Verarbeitungseinrichtung oder ein anderer Typ von Reaktor sein. Je nach dem Typ der Reaktionskammer kann das Materialzufuhrsystem **134** zum Beispiel Materialien für das Aufdampfen auf einem Werkstück **136** zuführen. Das Kühlsystem **145** kann dabei helfen, die Temperatur innerhalb der Kammer **125** zu regulieren, da die meisten chemischen Reaktionen mit Raten fortschreiten, die temperaturempfindlich sind. Der zu der Kammer zugeführte Strom kann ein Mikrowattstrom **153**, ein Hochfrequenzstrom **154** zum Erzeugen von Plasma, ein Gleichstrom **155** zum Erzeugen von Plasma und zum Erhitzen der Kammer oder Gase oder anderen zu der Kammer zugeführten Materialien sein. Die anderen Eingänge wie etwa die Gaseingänge stehen in Kommunikation mit einer oder mehreren digitalen Steuereinrichtungen **142**, Kammersteuereinrichtungen **152** und Verbindungspunkten **162**. Diese Kommunikation umfasst gewöhnlich eine Steuerung und eine Telemetrie. Diese Einrichtungen können Steuereinrichtungen und Sensoren umfassen, die auf die Steuerung des Betriebs der Einrichtungen oder die Erfassung von Ein-/Ausgaben reagieren.

[0024] Sensoren können entweder auf die Kammerbedingungen oder auf die Abgase aus der Kammer reagieren. Sensoren, die auf Kammerbedingungen reagieren, können umfassen: eine Wafer-Überwachungseinrichtung **116**, die durch ein Fenster **126** in die Kammer **125** blickt, um die Filmdicke, Muster oder andere Eigenschaften zu erfassen (z.B. EPI-Online (TM)); eine Prozess-Überwachungseinrichtung **127** wie etwa eine optische Emissions-Überwachungseinrichtung mit einem Störungsfilter oder Interferometer für die Ätzprozesssteuerung; und einen Druckwandler **137**. Sensoren, die auf Abgase aus der Kammer **125** reagieren, umfassen: einen Leckdetektor **146**, eine Vakuummesseinrichtung **157** und eine Abgas-Überwachungseinrichtung **158**. Diese Sensoren können mit einer Drucksteuereinrichtung **148** und einem Steuerventil **147** sowie mit Vakuumkomponenten und/oder -systemen **156** interagieren. Sie können auch mit einer Pumpe und/oder einer Abgasreinigungseinrichtung interagieren, die nicht in der Zeichnung gezeigt sind. Diese Sensoren stehen in Kommunikation mit einer oder mehreren digitalen Steuereinrichtungen **142**, Kammer-Steuereinrichtungen **152** und Verbindungspunkten **162**. Diese Kommunikation umfasst gewöhnlich eine Steuerung und eine Telemetrie. Die mit den Sensoren (z.B. **147**, **148** und **146**) kommunizierenden Einrichtungen können Steuereinrichtungen und Sensoren sein.

[0025] Nicht in [Fig. 1](#) gezeigt ist ein Ausfallsicherungsschalter, der angewendet werden kann, wenn eine Zwischeneinrichtung zwischen einer ersten Einrichtung bzw. einem ersten Netzwerk wie etwa dem Werksnetzwerk und einer zweiten Einrichtung bzw. einem zweiten Netzwerk wie etwa dem Werkzeugnetzwerk angeordnet ist, die auch ohne die Zwischeneinrichtung miteinander kommunizieren könnten. Ein Beispiel hierfür ist eine Steuereinrichtung, die Lesungen aus einem Werkzeug oder Sensor sammelt, speichert und auf eine Anforderung hin verfügbar macht. Ein anderes Beispiel ist eine Steuereinrichtung, die Daten aus einem Sensor ergänzt. Ein weiteres Beispiel ist eine Steuereinrichtung, die Daten in einem Format wie zum Beispiel SECS zu einem anderen Format wie zum Beispiel einem Tagged-XML-Format wandelt. Dem Fachmann sollten andere Situationen bekannt sein, in denen auf den Ausfall einer Zwischeneinrichtung durch eine ausfallsichere, direkte Verbindung der ersten und zweiten Einrichtung bzw. des ersten und zweiten Netzwerks reagiert werden kann.

[0026] [Fig. 2](#) ist ein Blockdiagramm einer Steuereinrichtung, die mit Werkzeugen, Sensoren und einem Werkzeug-Host in Kommunikation steht. Dieses Blockdiagramm könnte verallgemeinert werden, indem der Host **211** als erste Einrichtung, der Sensor **227** oder das Messinstrument **237** als zweite Einrichtung und die Steuereinrichtung **200** als Zwischeneinrichtung identifiziert werden. In der gezeigten Ausführungsform umfasst die Konfiguration der Steuereinrichtung **200** zwei SEC/GEM-Schnittstellenports **212**, **216** und zwei Netzwerkschnittstellenports **232**, **236**. Die Steuereinrichtung umfasst eine Logik und Ressourcen für die Kommunikation über das SECS-Protokoll einschließlich eines SECS-MUX **215**. Weiterhin umfasst die Steuereinrichtung eine Logik und Ressourcen zum Implementieren einer werkseitigen Schnittstelle **234** für die Kommunikation mit Datennutzern und eine werkzeugseitige Schnittstelle **235** für die Kommunikation mit Werkzeugen, Sensoren und Messinstrumenten. Der SECS-MUX **215** und die Schnittstellen **234**, **235** sind logisch mit Ressourcen **225** zum Sammeln und Veröffentlichen von Daten verbunden. Auf der Werkseite der Steuereinrichtung kann ein herkömmlicher Werkzeug-Host **211** über einen SECS-konformen Kommunikationskanal (SECS-1, HSMS oder ein Nachfolger von SECS), verbunden sein (**212**). Wenn die Erfindung in einer anderen Umgebung als einem Werk angewendet wird, können andere Protokolle verwendet werden, um eine Verbindung zu einem überwachten Werkzeug herzustellen, etwa zu einem medizinischen Werkzeug oder einem numerisch gesteuerten Maschinenwerkzeug. Es kann auch eine Verbindung über ein werkseitiges Protokoll hergestellt werden, das sich von SECS unterscheidet und durch ein Netzwerk **222** getragen wird, um Ressourcen zu speichern (**231**) und zu berichten (**221**). Auf der Werkzeug- und Sensorseite der Steuereinrichtung **200** kann eine SEC/GEM-Werkzeugschnittstelle **217** zu einem Werkzeug oder einer Werkzeuggruppe verbunden sein (**216**). Die Steuereinrichtung kann auch mit einem Netzwerk **226** verbunden sein (**236**), das Sensoren **227**, Messinstrumente **237** und andere Einrichtungen sowie unter Umständen Werkzeuge **217** umfasst. Die Figur stellt die Steuereinrichtung dar, die über ein Netzwerk mit den Sensoren verbunden ist, wobei alternativ hierzu auch SECS-I oder ein anderes seriell-basiertes Protokoll für die Verbindung mit den Sensoren verwendet werden kann.

[0027] [Fig. 3](#) ist ein Blockdiagramm einer Steuereinrichtung, die einen einzelnen Typ von Kommunikationskanal für die Kommunikation mit einem Werkzeug, Sensor und Werkzeug-Host verwendet. [Fig. 4](#) zeigt die Verwendung von mehreren Typen von Kommunikationskanälen. In [Fig. 3](#) ist ein SECS-dominiertes Szenario gezeigt. Die Steuereinrichtung **303** verwendet ein SECS-Protokoll **307**, **309** für die Kommunikation mit dem Werkzeug **301** und dem Sensor **302**. Die Verbindung **308** zwischen dem Werkzeug **301** und dem Sensor **302** kann einen beliebigen Typ von Strom oder Energie leiten, wobei es sich auch um eine der mit Bezug auf [Fig. 1](#) genannten Formen handeln kann. In [Fig. 4](#) ist eine komplexere Kombination aus SECS- und Netzwerkkommunikationen gezeigt. Der nur-SECS-Kommunikationskanal **307** in diesem Szenario erstreckt sich zwischen der Steuereinrichtung **303** und dem Host **301**. Ein werkzeugseitiges Netzwerk **409** verbindet die Steuereinrichtung mit Sensoren **302A-B**, einem verwalteten Schalter **413** und eine netzwerkverbundenen Speicher (NAS) **415**. Ein werkseitiges Netzwerk **419** verbindet die Steuereinrichtung **303** mit einer Analysesoftware **423** in etwa einem herkömmlichen Werkzeug-Host oder verteilten Prozessoren mit einem größeren Netzwerk **425** wie etwa dem Internet, einem VPN oder einem dedizierten internen Netzwerk und mit einer Datenbank **427**, die durch die Steuereinrichtung veröffentlichte Daten aufrechterhält oder speichert. Alternativ hierzu kann die Datenbank **427** auch in der Steuereinrichtung **303** enthalten sein.

Einfügen des Ausfallsicherungsschalters in einem Netzwerk

[0028] [Fig. 5](#) ist ein Blockdiagramm, in dem ein Ausfallsicherungsschalter zu dem in [Fig. 3](#) gezeigten Netzwerk hinzugefügt ist. Es sind zwei neue Komponenten eingefügt: ein Bypass-Schalter **511** und ein Hub oder Switch **512**. Für viele Konfigurationen ist nur der Bypass-Schalter **511** neu. Die Anordnung des Netzwerks nimmt an, dass die Kommunikation mit dem Werkzeug über ein Netzwerkprotokoll erfolgt. Dieses Kommunikationsprotokoll kann vorgesehen werden, wenn das Werkzeug nicht bereits ein Netzwerkprotokoll verwendet, indem ein Protokolladapter zwischen dem Hub oder Switch **512** und dem Werkzeug **501** eingefügt wird. Alternativ hierzu könnten zwei Kommunikationskanäle durch den Bypass-Schalter **511** gesteuert werden, zum Beispiel eine serielle Verbindung für den SECS-Verkehr und eine Ethernet-Verbindung für den restlichen Verkehr. Wie in [Fig. 3](#) gezeigt, kommuniziert eine Steuereinrichtung **303** im normalen Betriebsmodus mit dem Werkzeug **301** und dem Sensor **302**. Der Sensor ist mit dem Werkzeug verbunden, um einen Aspekt des Zustands oder der Leistung des Werkzeugs zu messen oder aufzuzeichnen. Mitteilungen aus dem Werkzeugnetz oder von dem Host **304** werden über den Bypass-Schalter **511** zu der Steuereinrichtung **303** und von der Steuereinrichtung zurück über den Bypass-Schalter zu dem Hub oder Switch **512** gesendet. Der Hub oder Switch ist eine herkömmliche Netzwerkkomponente, die Einrichtungen miteinander verbindet. Die Steuereinrichtung **303** umfasst wenigstens zwei Netzwerkschnittstellen **521**, **522**. Diese Schnittstellen sind effektiv über den By-

pass-Schalter **511** verbunden, der mit dem Werkzeugnetz **304** und dem Werkzeug **301** oder Sensor **302** kommuniziert. Eine zusätzliche Verbindung **523** zwischen der Steuereinrichtung **303** und dem Bypass-Schalter **511** trägt ein Heartbeat-Signal oder anderes Aufrechterhaltungssignal, das den Bypass-Schalter in einem weiter unten beschriebenen normalen (nicht-ausfallsicheren) Modus hält. In der Figur sind zwei Betriebsmodi gezeigt: der normale Betrieb der Steuereinrichtung in durchgezogenen Linien und der Bypass-Betrieb in gestrichelten Linien. Während in der Figur zwei Verbindungen durch den Bypass-Schalter gezeigt sind, kann es sich auch um logische Betriebsmodi handeln, die über einen einzelnen Draht bzw. eine einzelne Verbindung und nicht notwendigerweise über ein Paar von Verbindungen zwischen dem Bypass-Schalter **511** und dem Werkzeugnetz **204** oder dem Hub/Switch **512** ausgeführt werden. Außerdem kann der Bypass-Schalter mehr als eine Verbindung kontrollieren.

[0029] [Fig. 6](#) ist ein Blockdiagramm, in dem ein Ausfallsicherungsschalter zu dem Netzwerk von [Fig. 4](#) hinzugefügt ist. In dieser Figur wird der an dem Bezugszeichen **409** mit dem Bypass-Schalter **511** verbundene Hub/Switch gewöhnlich durch eine Multi-Drop-Netzwerkverbindung von dem Bypass-Schalter zu dem Werkzeug **301** und den Sensoren **301A-B** vorgesehen. In der Figur sind drei Verbindungen zwischen dem Bypass-Schalter und der Steuereinrichtung gezeigt.

Ausfallsicherungsbetrieb

[0030] Mit Bezug auf [Fig. 5](#) wird im Folgenden eine Ausführungsform des Betriebs des Ausfallsicherungsschalters erläutert. Im Fall einer Fehlfunktion der Steuereinrichtung, bei welcher die Steuereinrichtung keine nützliche Rolle mehr zwischen zwei Einrichtungen spielt, die auch ohne die dazwischen geschaltete Steuereinrichtung miteinander kommunizieren könnten, wird eine direkte Verbindung zwischen den Einrichtungen wie etwa dem Host **304** und dem Werkzeug **301** hergestellt. In einer Ausführungsform wird ein Schalter mit einem einfachen eingebetteten Mikrocontroller verwendet. Shore Micro stellt wenigstens einen funktionierenden Schalter her. Dieser umfasst ein Relais, das beim Schalten ein bestätigendes „Klickgeräusch“ ausgibt. Der Mikrocontroller in dem Schalter beobachtet ein Heartbeat-Signal aus der Steuereinrichtung über eine Verbindung **523** wie etwa eine serielle, parallele, USB-, Firewire-, Ethernet- oder andere Verbindung. Es können auch andere Protokolle verwendet werden, je nach der Logik oder den Ressourcen, die an dem Ausfallsicherungsschalter vorgesehen sind. Zum Beispiel kann der Ausfallsicherungsschalter periodische Anfragen an die Steuereinrichtung machen und auf Fehlerbedingungsangaben oder Antwortzeitüberschreitungen antworten. Diese Anfragen können regelmäßig oder adaptiv auf einen hohen Verkehr, einen niedrigen Verkehr und/oder andere interessante Betriebsbedingungen erfolgen. Der Mikrocontroller-gesteuerte Schalter entspricht einem einpoligen Wechselschalter, der die Steuereinrichtung **303** in den Schaltkreis mit dem Host **304** einbindet oder aus demselben ausschließt. Im normalen Betrieb ist die Steuereinrichtung physikalisch mit der Schaltung verbunden. Im Ausfallsicherungsmodus sind der Host und das Werkzeug/die Sensoren direkt miteinander verbunden. Alternativ hierzu kann ein elektronisches Schalten verwendet werden, wobei in diesem Fall jedoch kein bestätigendes Relais-Klickgeräusch erzeugt wird.

[0031] Die Software zum Implementieren eines Heartbeats und einer ausfallsicheren Verbindung kann umfassen: einen Gerätetreiber, der Paketadressen setzt; einen Kernel-Hook zum Abfangen von Paketen, wenn eine Netzwerkschnittstelle im Promiskmodus ausgeführt wird; einen Watchdog-Daemon; und ein Benutzer-raum-Programm. Die folgende Beschreibung orientiert sich an Linux. Es können jedoch auch andere Betriebssysteme wie etwa BSD-Varianten, Unix-Varianten oder Windows verwendet werden. Es kann ein System für die Ausführung auf einer virtuellen Maschine wie etwa eine Echtzeitversion von Java geschrieben werden, so dass nur kleine Änderungen an der Software für die Steuerung von Netzwerkfunktionen der niedrigen Ebene erforderlich sind, um die Software von einem Betriebssystem auf ein anderes zu übertragen.

[0032] Der Gerätetreiber könnte den TCP/IP-Stack abfangen und die Steuereinrichtung transparent machen, so als ob die Steuereinrichtung nicht verbunden wäre. Dazu ändert er die Quelladressen und die Informationen in den Paketen, damit diese so aussehen, als ob sie von dem Werkzeug oder dem Host und nicht von der Zwischensteuereinrichtung kämen. Der Gerätetreiber kopiert Daten aus dem Benutzerraum zu TCP/IP-Hooks im Kernel-Raum.

[0033] Die Steuereinrichtung kann ausgewählte Pakete handhaben, die nicht an einen HSMS-Port adressiert sind, ohne dass die Pakete durch die Steuereinrichtung verarbeitet werden, indem diese von einer Netzwerkschnittstelle zu der nächsten überbrückt werden. Zum Beispiel kann ein Ping oder ICMP-Paket ohne eine Verarbeitung durch die Steuereinrichtung durchgelassen werden. Das wahlweise Überbrücken kann in Abhängigkeit von dem Pakettyp und/oder Port erfolgen.

[0034] Der Kernel-Hook umfasst einige Codezeilen, die wenigstens bestimmte Pakete retten, wenn die Netzwerkschnittstelle im Promiskmodus betrieben wird, insbesondere Sniffing-Pakete, die nicht für die Adresse bestimmt sind, an der die Netzwerkschnittstelle erscheint. Ein nicht modifizierter Linux-Kernel wie zum Beispiel 4.2.26 fängt keine Pakete ab, die nicht an ihn adressiert sind (Layer 2 oder MAC-Layer), auch wenn die Schnittstellen im Promiskmodus betrieben werden. Er verwirft den Inhalt in der `Ip rev-Funktion`. Der Kernel-Hook gibt bestimmte Pakete zu einer Funktion, die nicht Teil des zu handhabenden, nicht modifizierten Kernels ist.

[0035] Watchdog-Daemons kommunizieren mit dem Schalter und senden einen Heartbeat aus. Der Schalter sichert die Verbindung (schaltet das Relais), wenn er den Heartbeat von diesem Daemon nicht empfängt. Die Standardverbindung nach dem Hochfahren für den Schalter ist die ausfallsichere. Der Heartbeat-Daemon schreibt an `syslog`.

[0036] Ein Benutzerraum-Programm setzt IP- oder andere Adressen für den eigenen Port der Steuereinrichtung und für die erste und die zweite Einrichtung, zwischen denen die Steuereinrichtung vorgesehen ist, zum Beispiel für ein Werkzeug/einen Sensor und für einen Host.

[0037] In Linux binden Benutzer-Scripts für Konfigurationsinformationen und den Start die anderen Komponenten zusammen. Die Software ist mit einer Sample-Konfigurationsdatei gebündelt. Die Konfigurationsdatei enthält die Host-IP, die Werkzeug-IP, ein Zeitintervall zum Triggern des Watchdog-Daemon-Timers, ein Com-Portnummer für die Kommunikation zwischen dem Watchdog-Daemon und dem Ausfallsicherungsschalter und einen optionalen Modus für eine zukünftige Verbesserung. Ein Start-Script wird bei einer Implementierung mit Linux 4.2.26 vorzugsweise nach `syslog` und vor `easl` ausgeführt. Das Script startet und stoppt den Daemon-Betrieb wie es für Start-Scripts typisch ist. Es kann zum Beispiel „`hsmfsd start`“ genannt werden. Das Script kann etwas länger dauern als andere Scripts, was einfach darauf zurückzuführen ist, dass es die MAC-Adressen des Werkzeugs und des Hosts erkennen und ggf. die entsprechenden Routen hinzufügen muss. Damit die Erkennung erfolgreich ist, werden die erste und die zweite Einrichtung, also zum Beispiel das Werkzeug und der Host, beim Start mit der Steuereinrichtung verbunden. Alternativ hierzu können vorbestimmte IP-Adressen geladen und ohne Erkennung verwendet werden. Das Start-Script fügt auch eine Route hinzu, um dem TCP/IP-Stack zu zeigen, wie die IP-Adressen der Steuereinrichtung auf die Netzwerkschnittstellen `eth0` und `eth1` bezogen sind.

[0038] Die einfachste Konfiguration, zu der wahrscheinlich eine Steuereinrichtung oder eine andere Zwischeneinrichtung hinzugefügt werden kann, umfasst ein Werkzeug und einen Host. In diesem einfachen Fall sind die IP-Adressen des Werkzeugs und des Hosts bekannt und in der Konfigurationstabelle enthalten. Wenn die Steuereinrichtung das `hsmfsd-Start-Script` ausführt, startet sie den Schalter-Watchdog-Daemon. Der Daemon weiß nichts über den Rest des Ausfallsicherungsmechanismus, sondern veranlasst einfach, dass der Schalter (Shore-Mikroschalter) zu dem Ausfallsicherungsmodus wechselt (in dem der Host physikalisch mit dem Werkzeug verbunden ist), wenn die Bluebox keine Heartbeats oder Befehle für den Online-Betrieb mehr sendet.

[0039] Solange die Steuereinrichtung normal funktioniert, bleibt der Schalter online und verbindet das Werkzeug über die Bluebox mit dem Host. Das Start-Script kann ein Standard-ARP-Protokoll verwenden, um die MRC-Adressen des Werkzeugs und des Hosts zu erkennen und eine lokale ARP-Tabelle zu aktualisieren. Weitere Details zu den ARP-Protokollen werden durch die folgenden RFCs erläutert, wobei die ARP-Protokolle allgemein #826, PROXY ARP #1027, DHCP ARP #2131 und UNARP #1868 verwenden. Wenn der Host oder das Werkzeug auf die zweite Netzwerkschnittstelle, z.B. auf `eth1`, antwortet, wird eine Host-Route zu der zweiten Schnittstelle mit dieser IP-Adresse hinzugefügt.

[0040] In dieser Ausführungsform befinden sich das Werkzeug und der Host in demselben Netzwerk-Subnetz, ebenso wie die Netzwerkschnittstellen der Steuereinrichtung. Die Steuereinrichtung erkennt oder weiß, welche Schnittstelle eine Verbindung zu dem Host und dem Werkzeug herstellt, sodass sie Mitteilungen routen kann. Ansonsten würde eine Standardroute für den TCP/IP-Stack verwendet werden, was jedoch nicht funktioniert, weil alle Mitteilungen für dasselbe Netzwerk-Subnetz, die sowohl den Host als auch das Werkzeug umfasst, zu derselben Netzwerkschnittstelle geroutet würden. Die Module werden geladen, wobei dann die Anwendung mit den aus der Konfigurationsdatei erhaltenen IP-Adressen und den MAC-Adressen für diese IP-Adressen aus der lokalen ARP-Tabelle erhalten wird. Daraufhin werden der Host und das Werkzeug über die Bluebox verbunden. Die Bluebox-Konfiguration unter EMX-Setup ist einerseits passiv und nimmt die Verbindung von dem Host an und andererseits aktiv und verbindet das Werkzeug mit der IP-Adresse des Werkzeugs. Der passive und der aktive HSMS-Setup müssen sich den gleichen Port teilen.

[0041] Eine durch den Gerätetreiber aufrechterhaltene Tabelle, die mit TCP/IP-Stack-Hooks in dem Kernel assoziiert ist, enthält einen Eintrag für das Werkzeug und einen anderen Eintrag für den Host. Für die zweite Einrichtung, d.h. zum Beispiel das Werkzeug/den Sensor, können die Tabelleneinträge wie folgt sein:

Eintragsnummer	Sequenz der Anwendung
Protokoll	0 × 6 für TCP
Flags	1 bedeutet, dass die MAC-Adresse gültig ist
Ziel-MAC-Adresse	Aus dem Start-Script genommen
Ziel-IP-Adresse	Aus dem Start-Script genommen
Ziel-Port	Aus der Konfiguration genommen
Quell-IP-Rdresse	Unbekannt
Quell-Port	Unbekannt

[0042] Für die erste Einrichtung, d.h. zum Beispiel den Host, können die Tabelleneinträge wie folgt sein:

Eintragsnummer	Sequenz der Anwendung
Protokoll	0 × 6 für TCP
Flags	1 bedeutet, dass die MAC-Adresse gültig ist
Ziel-MAC-Adresse	Aus dem Start-Script genommen
Ziel-IP-Adresse	Aus dem Start-Script genommen
Ziel-Port	Unbekannt
Quell-IP-Rdresse	Aus der Konfiguration genommen
Quell-Port	Aus der Konfiguration genommen

[0043] Für TCP/IP wird gewöhnlich eine eindeutige Verbindung durch ein Quadrupel identifiziert, das die Quell-IP, den Quell-Port, die Ziel-IP und den Ziel-Port enthält. Dies macht die Verbindung universell im Netzwerk und eindeutig – Netzwerkprotokolle unterstützen nur eine Verbindung unter Verwendung dieser Quadrupel. Ebenfalls verfügbar ist die so genannte Halbassoziaton, die die Ziel-IP und den Port umfasst, wobei der Port auf den Dienst verweist und die IP der Maschine entspricht, zu der die Verbindung hergestellt wird. Zum Beispiel sind www.mksinst.com als Port 80 und eine IP-Adresse, die der Domain-Name-Server aus dem Namen www.misinst.com erhält, vorgesehen. Für einen ISP-Benutzer würde der Server an dem Ende des ISP die IP beibehalten und einen lokalen Port zuweisen, um das eindeutige Quadrupel zu bilden. Immer wenn jemand ein weiteres Fenster des Browsers öffnet, wird ein weiteres eindeutiges Quadrupel mit derselben Ziel-IP, demselben Ziel-Port, derselben Quell-IP und einem anderen zugewiesenen Quell-Port erzeugt, um die Anforderung der Eindeutigkeit zu erfüllen.

[0044] Bei einem praktischen Betrieb versucht der Host zum Beispiel das Werkzeug oder einen Sensor zu verbinden, wobei die Steuerung eine oder mehrere Mitteilungen von dem Host abfängt, während die Netzwerkschnittstelle im Promiskmodus betrieben wird. Es wird ein erstes mit einem Eingangs-Hook verbundenes Filter angewendet, das bestimmt, ob das Paket zu einer der Netzwerkschnittstellen oder der Steuereinrichtung gehört. Das erste Filter gibt ein zu einer Schnittstelle gehöriges Paket zu dieser Schnittstelle und beendet seinen Betrieb. Wenn das Paket nicht zu den Netzwerkschnittstellen der Steuereinrichtung gehört, schlägt das Filter den Ziel-Port und die Ziel-IP in den oben beschriebenen Tabellen des Gerätetreibers nach. Wenn das Ziel in den Tabellen des Gerätetreibers gefunden wird, ändert das Filter das Ziel des Pakets zu einer auf die Steuereinrichtung bezogenen Adresse und gibt sie an den TCP/IP-Stack. Nachdem das Paket durch den TCP/IP-Stack gehandhabt wird, stellt ein zweites mit einem Ausgangs-Hook assoziiertes Filter das Ziel wieder her, sodass eine Bestätigung oder Antwort von dem ursprünglichen Ziel zu kommen scheint. Dieser Prozess wird gelegentlich als Einmaskierung bezeichnet. Dieser Ansatz unterstützt gleichzeitige Sitzungen. Je nach dem Typ des Pakets und dem Verlauf der Sitzung verarbeitet die Steuereinrichtung das Paket direkt oder leitet das Paket an das ursprüngliche Ziel weiter.

[0045] Während des praktischen Betriebs kann ein Werkzeug/ein Sensor versuchen, eine Verbindung zu dem Host herzustellen. Die als Zwischeneinrichtung dienende Steuereinrichtung versucht, das Paket an den Host zu senden. Die IP-Sendefunktion schlägt das Ziel-Paket und den Ziel-Port nach. Wenn das Ziel gefunden wird, modifiziert die Funktion die Paket-Quell-IP, die die Steuereinrichtungs-IP zu der Werkzeug-IP in der Tabelle ist, und kopiert den Ziel-Port (der zufällig der Quell-Port der Steuereinrichtung ist in die Tabelle. Das Werkzeug antwortet auf das Paket, und die Empfangsfunktion erhält die Antwort. Weil jedoch die Tabelle jetzt vollständig ist, ist das Nachschlagen erfolgreich und wird das Paket zu dem Stack zurückgeleitet. Dieser Prozess wird gelegentlich als Ausmaskierung bezeichnet.

[0046] Entweder das Werkzeug oder der Host fragt nach der MAC-Adresse, wenn die ARP-Einträge älter wer-

den. Das Werkzeug fragt zum Beispiel nach der MAC-Adresse der Host-IP, wobei aber das Werkzeug nicht mit dem Host, sondern mit der Steuereinrichtung verbunden ist. Die Steuereinrichtung schlägt die IP-Adresse des Hosts in ihren Tabelleneinträgen nach und antwortet auf die ARP-Anforderungsmittelung mit der entsprechenden MAC-Adresse für den Host. Dabei handelt es sich um den ARP-Hook in dem Gerätetreiber. Die durch die Steuereinrichtung ausgegebene MAC-Adresse ist die echte MAC-Adresse des Hosts oder in Antwort auf eine ARP-Anforderung aus dem Host die echte MAC-Adresse des Werkzeugs. Der Paketverkehr findet innerhalb des Moduls (msmfs.o Gerätetreiber) statt, das eine Verbindung zu dem TCP/IP-Stack herstellt.

[0047] Wenn die Steuereinrichtung aus irgend einem Grund blockiert wird, kann die Ausfallsicherungsfunktion aktiviert werden. Solange der Serienschalter-Daemon das System betreibt und das System korrekte betriebsfähigen erscheint, bleibt die Steuereinrichtung online und werden der Host und das Werkzeug über die Steuereinrichtung verbunden. Wenn der Daemon ausfällt, geht der Schalter zu dem Ausfallsicherungsmodus über, in dem der Host und das Werkzeug direkt miteinander verbunden sind. Optional kann der Daemon die Korrektheit des Betriebs der Steuereinrichtung bewerten, einen Ausfall voraussagen bzw. erfassen und entsprechend reagieren. Im Fall eines vorausgesagten Ausfalls kann der Host benachrichtigt werden und kann optional das Erfassen der Korrektheit des Betriebs der Steuereinrichtung modifiziert werden. Wenn der Ausfallsicherungsschalter geschaltet wird, versuchen die Teilnehmer der jetzt direkt verbundenen Sitzung die Verbindung von dem Host zu dem Werkzeug wiederherzustellen. In einer Ausführungsform eines mechanischen Relais veranlasst eine Unterbrechung der Stromversorgung zu dem Schalter, dass das Relais die Ausfallsicherungsstellung annimmt und den Host direkt mit dem Werkzeug verbindet.

[0048] Wenn ein Host eine Verbindung verliert, sollte er versuchen, eine Sitzung neu zu starten. Weil die ARP-Tabelle aktuell ist, kann eine direkte Verbindung einfach hergestellt werden. Das erneute Starten einer Sitzung wird gelegentlich als robuste Mitteilungsübertragung bezeichnet.

[0049] Die Ausführungsform des Ausfallsicherungsmodus sieht verschiedene interessante Merkmale vor, von denen einigen auch in anderen Ausführungsformen vorgesehen sind. Es muss keine Software zu der ersten oder zweiten Einrichtung (zu dem Host oder Werkzeug) hinzugefügt werden. Der Host und das Werkzeug befinden sich im selben Subnetz, sodass sie im Fall einer direkten Ausfallsicherungsverbindung miteinander kommunizieren können. Die als Zwischeneinrichtung dienende Steuereinrichtung befindet sich im selben Subnetz wie das Werkzeug und der Host. Der Host und das Werkzeug „können einander sehen“, wenn die Steuereinrichtung im Ausfallsicherungsmodus gestartet wird. Eine aktive Sitzung wird automatisch durch das Werkzeug, den Host oder beide wiederhergestellt, wenn der Betrieb von dem normalen Modus zu dem Ausfallsicherungsmodus wechselt.

Zweite Betriebsausführung

[0050] In einer zweiten Ausführungsform wird eine wahlweise Überbrückung implementiert, ohne dass die Steuereinrichtung auf ARP-Anforderungsmittelungen zwischen dem Host und dem Werkzeug antwortet. ARP-Mittelungen und andere ausgewählte Mittelungen von dem Host an das Werkzeug oder umgekehrt, werden von einer Seite der Steuereinrichtung zu der anderen überbrückt, von einer Netzwerkschnittstelle im Promiskmodus zu einer anderen Netzwerkschnittstelle gegeben und zurück gesendet. Das Werkzeug antwortet auf weitergeleitete ARP-Anforderungsmittelungen von dem Host und umgekehrt. Die Steuereinrichtung überbrückt und leitet die ARP-Anforderungsmittelungen und anderen Mittelungen wahlweise mit einer erkannten Quelle und einem erkannten Ziel zum Beispiel auf der Basis eines Nachschlagens in einer Tabelle weiter. Eine nützliche Tabelle ist weiter oben beschrieben, und die Überbrückung erfolgt wahlweise. Ein Paket mit einem nicht erkannten Ziel wird nicht durch den Kernel-Hook gehandhabt, sondern wird durch den gewöhnlichen TCP/IP-Stackprozess gelassen, der dann das Paket fallen lassen kann. Durch das Herausfiltern von bestimmten Mittelungen werden Zyklen im Netzwerk reduziert. Wenn der Host zum Beispiel über fünf Steuereinrichtungen mit fünf Werkzeugen verbunden ist, kann die erste Steuereinrichtung gefahrlos einige oder alle Mittelungen an das zweite bis fünfte Werkzeug herausfiltern. Der Verkehr in dem werkzeugseitigen Netzwerk kann wesentlich reduziert werden. Als weiteres Beispiel kann die Steuereinrichtung Daten aus dem Werkzeug abrufen und speichern, die der Host erwartet oder anfordern kann, aber noch nicht angefordert hat. Die Steuereinrichtung kann gefahrlos den Datenverkehr für die Steuereinrichtung herausfiltern und den Verkehr in dem hostseitigen Netzwerk reduzieren. Eine Regel, die auf die wahlweise Überbrückung angewendet werden kann, besagt, dass nur Pakete zwischen einem Host und einem Ziel weitergeleitet werden, die durch die Steuereinrichtung erkannt werden und mit derselben kommunizieren. Außerdem können ausgewählte Typen von Rundmittelungen überbrückt werden. Die weiter oben beschriebenen Kernel-Hooks sind ausgebildet um die erforderliche Unterstützung für das Weiterleiten von Paketen zwischen Netzwerkschnittstellen und für das Überbrücken von Paketen vorzusehen.

[0051] Bei der Handhabung von Paketen wird dem HSMS-konfigurierten Port Priorität eingeräumt, sodass die Verbindung durch den lokalen Prozess in der Bluebox gehandhabt wird. ICMP-, UDP-, ARP-, TCP-Pakete (andere Ports als MSMS) werden zwischen zwei Netzwerkschnittstellen weitergeleitet, sofern die Ziel-IP in der lokalen Tabelle enthalten ist. Dieses Verhalten ist demjenigen einer Brücke ähnlich, aber wahlweise auf die IP-Adressen in der Tabelle beschränkt, um Zyklen im Netzwerk zu vermeiden. Die ARP-Einschränkung ist sogar noch strenger, wobei sowohl die Quell- als auch die Ziel-IP in der Tabelle enthalten sein müssen, bevor sie weitergeleitet werden, was bedeutet, dass nur das Werkzeug und der Host eine ARP-Verbindung über die Netzwerkschnittstellen der Steuereinrichtung herstellen können.

Dritte Betriebsausführung

[0052] Alternativ hierzu kann die Steuer- oder Zwischeneinrichtung die IP-Adressen der Einrichtungen, die direkt miteinander kommunizieren könnten, annehmen und die Pakete entsprechend neu packen und weiterleiten. Dieser Ansatz unterscheidet sich stark von den herkömmlichen Funktionen der anderen Typen von Geräten, weil die Netzwerkschnittstelle der Steuereinrichtung eine eigene Hardwareschicht-Kennzeichnung oder MAC-Adresse aufweist. Eine MAC-Adresse ist Teil des Paketadressierungsschemas, das gewöhnlich für Netzwerke implementiert wird. Für eine typische Netzwerkschnittstelle ist die Netzwerkschicht (z.B. IP) mit der Datenverknüpfungsschicht (z.B. MAC) verknüpft und in dem sieben-schichtigen OSI-Modell angegeben. Netzwerkprotokolle wie zum Beispiel ARP gestatten, dass Einrichtungen im Netzwerk IP- und MAC-Adressen miteinander korrelieren. Datenredundanzmerkmale des Pakettransports enthalten Prüfcodes, die teilweise unter Verwendung von Informationen aus der Datenverknüpfungsschicht des Pakets codiert werden. Wenn zwei Netzwerkschnittstellen, die zum Beispiel mit separaten Netzwerksegmenten verbunden sind, beide dieselbe IP-Adresse verwenden, weisen sie dennoch unterschiedliche MAC-Adressen auf. Damit die Steuereinrichtung ein Paket von dem Host zu dem Werkzeug oder umgekehrt weiterleitet, wenn sie sich die IP-Adressidentität des Werkzeugs borgt, muss sie das Paket mit den korrigierten Prüfcodes neu packen, die unter Verwendung der MAC-Adresse des Werkzeugs und nicht der MAC-Adresse der Steuereinrichtung codiert werden. Dies reicht jedoch nicht für eine ausfallsichere Implementierung aus. Die Geräte, die direkt miteinander kommunizieren könnten, müssen ihre Netzwerkschicht zu Datenverknüpfungsschicht-Tabellen wie zum Beispiel ihren ARP-Tabellen aktualisieren, um die effektive MAC-Adresse nach einem Ausfall zu korrigieren. Wenn der weiter oben beschriebene Ausfallsicherungsschalter den Host und das Werkzeug direkt miteinander verbindet, gehen die Pakete in dem Ausfallsicherungsmodus nicht direkt von dem Host zu dem Werkzeug, weil die MAC-Adressen, die der Host und das Werkzeug füreinander haben, die MAC-Adressen der Steuereinrichtung enthalten. Um dies zu überwinden, müssen der Host und/oder das Werkzeug ihre Netzwerkschicht zu den Datenverknüpfungsschichttabellen aktualisieren. Der Host und/oder das Werkzeug können für eine häufige Aktualisierung ihrer Tabellen oder derart angepasst werden, dass sie auf eine fallen gelassene Sitzung antworten, indem sie ihre Tabellen aktualisieren. Mit einer aktualisierten Tabelle kann eine unterbrochene Sitzung wiederhergestellt werden oder es kann eine neue, direkte Sitzung begonnen werden.

Weitere Erläuterungen zu den Ausführungsformen

[0053] Die vorliegende Erfindung kann als ein Verfahren oder eine Vorrichtung zum Ausführen des Verfahrens realisiert werden. Dasselbe Verfahren kann aus der Perspektive eines intelligenten Sensors oder Adapter wie etwa einem SenseLink oder aus der Perspektive einer Steuereinrichtung wie etwa einer Bluebox betrachtet werden. Die Erfindung kann ein Produkt wie etwa ein Medium mit einer Logik sein, um eine computergestützte Sensorsteuerung auszuführen.

[0054] Das Verfahren der ersten Ausführungsform ist ein Verfahren zum transparenten Herstellen einer direkten Verbindung zwischen einer ersten und einer zweiten Einrichtung für den Fall, dass eine Zwischeneinrichtung ausfallen sollte. Dieses Verfahren umfasst das Verbinden der ersten und der zweiten Einrichtung mit einer ersten und einer zweiten Netzwerkschnittstelle einer Zwischeneinrichtung. Die erste und die zweite Netzwerkschnittstelle weisen Datenverknüpfungsschichten-Kennzeichnungen auf, die sich von denjenigen unterscheiden, die mit der ersten und der zweiten Einrichtung assoziiert sind. In einem normalen Betriebsmodus umfasst das Verfahren weiterhin das Handhaben von Mitteilungen, die zwischen der ersten und der zweiten Einrichtung adressiert sind, wobei die Zwischeneinrichtung wiederholt Signale an einen Ausfallsicherungsschalter sendet, die ihren fortgesetzten korrekten Betrieb signalisieren. An dem Ausfallsicherungsschalter umfasst das Verfahren bei einem Ausbleiben der wiederholten Signale zu dem korrekten Betrieb von der Zwischeneinrichtung das Schalten zu einem Ausfallsicherungsmodus durch das direkte Verbinden der ersten und der zweiten Einrichtung über eine Datenverbindung, die die Zwischeneinrichtung umgeht. Diese Datenverbindung kann die erste und die zweite Netzwerkschnittstelle umgehen. Die Wiederholung der Signale zu dem korrekten Betrieb kann durch kontinuierliche Signale oder diskrete periodische Signale bewerkstelligt werden.

[0055] Ein Aspekt der ersten Ausführungsform besteht darin, dass das Wechseln zu einem Ausfallsicherungsmodus ein hörbares Signal wie etwa ein Relaisklicken erzeugen kann. Gemäß einem anderen Aspekt können die erste und die zweite Netzwerkschnittstelle angepasst werden, um alle empfangenen Pakete zu einem Filter zu geben, das an die erste oder die zweite Einrichtung oder an die Zwischeneinrichtung adressierte Pakete handhabt. Die Handhabung der Pakete kann für wenigstens einige Pakete das Weiterleiten der Pakete von der ersten oder zweiten Einrichtung entsprechend zu der zweiten oder ersten Einrichtung und das Spezifizieren einer Datenverknüpfungsschicht-Kennzeichnung der tatsächlichen Quelle anstelle einer Datenverknüpfungs-Kennzeichnung der ersten oder zweiten Netzwerkschnittstelle in einem Quellenkennzeichnungsfeld der weitergeleiteten Pakete umfassen.

[0056] Ein weiterer Aspekt besteht darin, wie die wiederholte Signalisierung implementiert wird. Diese kann durch einen Daemon implementiert werden, der auf der Zwischeneinrichtung ausgeführt wird und wiederholt eine Mitteilung zu dem Ausfallsicherungsschalter sendet oder auf Anfragen von dem Ausfallsicherungsschalter wartet und diese beantwortet. Alternativ hierzu kann der Daemon einen kontinuierlichen Betrieb vorsehen.

[0057] Die Ausführungsformen können weiterhin mehrere zweite Einrichtungen umfassen, die auf die erste Einrichtung reagieren, indem sie entweder eine physikalische Kommunikationsverknüpfung oder zwei oder mehrere physikalische Kommunikationsverknüpfungen verwenden. Wenn zwei oder mehr physikalische Kommunikationsverknüpfungen verwendet werden, kann es sich einerseits um ein Ethernet-Segment und andererseits um eine serielle Verbindung handeln. Die serielle Verbindung kann einem IEEE-Standard wie etwa RS-232 oder RS-422 entsprechen.

[0058] Während des Betriebs kann das Herstellen einer direkten Kommunikationssitzung zwischen der ersten und der zweiten Einrichtung erfordern, dass in der ersten oder zweiten Einrichtung Tabellen aktualisiert werden, die Netzwerkadressen mit Datenverknüpfungsschicht-Adressen korrelieren. Das heißt, die ARP-Tabellen müssen unter Umständen nicht aktualisiert werden. Es kann dagegen erforderlich sein, die Tabellen zu aktualisieren, die IP- und MAC-Adressen korrelieren. Die erste und die zweite Einrichtung sowie die Zwischeneinrichtungen können alle innerhalb desselben Netzwerk-Subnetzes betrieben werden.

[0059] Eine weitere Ausführung des Verfahrens ist ein Ausfallsicherungsverfahren zum Herstellen einer Kommunikationsverknüpfung zwischen einem Host und einem Werkzeug, nachdem eine zwischen dem Host und dem Werkzeug verbundene intelligente Steuereinrichtung ausgefallen ist. Dieses Verfahren umfasst das Übernehmen einer ersten Hardwareebenen-Kennzeichnung, die ansonsten durch das Werkzeug verwendet wird, an einem ersten Port der intelligenten Steuereinrichtung und das Bekanntmachen des ersten Ports an dem Host als unter Verwendung der ersten Hardwareebenen-Kennzeichnung adressiert. Das Verfahren umfasst weiterhin das Übernehmen einer zweiten Hardwareebenen-Kennzeichnung, die ansonsten durch den Host verwendet wird, an einem zweiten Port der intelligenten Steuereinrichtung und das Bekanntmachen des zweiten Ports an dem Werkzeug als unter Verwendung der zweiten Hardwareebenen-Kennzeichnung adressiert. Während des Betriebs signalisiert die intelligente Steuereinrichtung wiederholt gegenüber einem Ausfallsicherungsschalter, dass die Steuereinrichtung zuverlässig ist. Der Ausfallsicherungsschalter wird bei einem Ausbleiben der wiederholten Signalisierung verwendet, um den Host und das Werkzeug direkt mit einer Kommunikationsverknüpfung zu verbinden, die die intelligente Steuereinrichtung umgeht. Danach befinden sich der Host und das Werkzeug in einer direkten Bekanntmachungs-Verbindung, wobei durch die Bekanntmachungen der ersten und zweiten Hardwareebenen-Kennzeichnungen die Herstellung einer Kommunikationsverbindung zwischen dem Host und dem Werkzeug bewerkstelligt wird.

[0060] Es werden mehrere Aspekte dieser anderen Ausführungsformen beschrieben. Gemäß einem Aspekt können sich ein erste logische Adresse zum Identifizieren des ersten Ports, eine zweite logische Adresse, die durch das Werkzeug verwendet wird, eine dritte logische Adresse zum Identifizieren des zweiten Ports und eine vierte logische Adresse, die durch den Host verwendet wird, jeweils unterscheiden. Diese logischen Adressen können IP-Adressen oder andere Netzwerkschichtadressen sein. Diese Hardwareebenen-Kennzeichnung kann eine MAC-Adresse sein. Die Bekanntmachungen der Hardwareebenen-Kennzeichnung können über standardkonforme ARP-Mitteilungen erfolgen.

[0061] Die andere Ausführungsform kann weiterhin auf einen Sensor angewendet werden, der das Werkzeug überwacht, wobei die intelligente Steuereinrichtung zwischen dem Host und dem Sensor verbunden ist. Diese Anwendung kann das Übernehmen einer dritten Hardwareebenen-Kennzeichnung, die ansonsten durch den Sensor verwendet wird, an dem ersten Port der intelligenten Steuereinrichtung und das Bekanntmachen des ersten Ports an den Host als unter Verwendung der dritten Hardwareebenen-Kennzeichnung umfassen. Sie kann weiterhin das Bekanntmachen des zweiten Ports an den Sensor als unter Verwendung der zweiten Hard-

wareebenen-Kennzeichnung adressiert und das Abfangen der dritten Hardwareebenen-Kennzeichnung an den Bekanntmachungen der intelligenten Steuereinrichtung umfassen, sodass der Host und der Sensor nicht in einer direkten Bekanntmachungs-Kommunikation stehen. Bei dieser Anwendung stellt der Ausfallsicherungsschalter bei Beendigung der wiederholten Signalisierung eine direkte Kommunikationsverbindung zwischen dem Host und dem Sensor her, die die intelligente Steuereinrichtung umgeht. Diese direkte Verbindung kann den ersten und den zweiten Port umgehen. Die Aspekte der distinkten logischen IP-Adresse, der distinkten Netzwerkschichtadresse, der Hardwarekennzeichnung und der Konformität zu dem ARP-Standard können alle auf diese Anwendung angepasst werden.

[0062] Eine weitere Verfahrensausführungsform fügt eine gegenüber einem Ausfall geschützte intelligente Steuereinrichtung und einen Schalter in eine Kommunikationsverknüpfung zwischen einem Host und wenigstens einem Werkzeug oder Sensor ein. Dieses Verfahren umfasst das Verbinden des Schalters mit dem Host, der intelligenten Steuereinrichtung und dem Werkzeug, wobei der Host und das Werkzeug mit der intelligenten Steuereinrichtung und nicht direkt miteinander kommunizieren, wenn sich der Schalter in einem ersten Zustand befindet, und wobei der Host und das Werkzeug direkt miteinander kommunizieren, wenn sich der Schalter in einem zweiten Zustand befindet. In dem ersten Zustand fängt die intelligente Steuereinrichtung Mitteilungen zwischen dem Host und dem Werkzeug ab, modifiziert wenigstens eine Hardwareebenen-Quellkennzeichnung und wenigstens eine Hardwareebenen-Zielkennzeichnung in der abgefangenen Mitteilung, modifiziert wenigstens einen Fehlerkorrekturcode in der abgefangenen Mitteilung, sodass dieser den Hardwareebenen-Kennzeichnungen entspricht, und leitet die abgefangenen Mitteilungen mit den modifizierten Hardwareebenen-Kennzeichnungen und dem modifizierten Korrekturcode weiter. In dem zweiten Zustand umgeht der Schalter die intelligente Steuereinrichtung und stellt eine direkte Verbindung zwischen dem Host und dem Werkzeug her.

[0063] Gemäß einem Aspekt des Verfahrens der weiteren Ausführungsform umfasst die intelligente Steuereinrichtung wenigstens einen ersten Port und einen zweiten Port, wobei der erste Port mit dem Host kommuniziert und der zweite Port mit dem Werkzeug kommuniziert. Gemäß diesem Aspekt identifiziert eine erste logische Adresse den ersten Port, wird eine zweite logische Adresse durch das Werkzeug verwendet, identifiziert eine dritte logische Adresse den zweiten Port und wird eine vierte logische Adresse durch den Host verwendet. Diese vier logischen Adressen sind jeweils verschieden. Es kann sich um IP-Adressen oder andere Netzwerkschichtadressen handeln. Dies Hardwareebenen-Kennzeichnungen der weiteren Verfahrensausführung können MAC-Adressen sein.

[0064] Das Verfahren der weiteren Ausführungsform kann auch auf einen Sensor angewendet werden, der das Werkzeug überwacht. Die weitere Anwendung umfasst das Verbinden des Ausfallsicherungsschalters mit dem Sensor, wobei der Host und der Sensor mit der intelligenten Steuereinrichtung und nicht direkt miteinander kommunizieren, wenn sich der Ausfallsicherungsschalter in dem ersten Zustand befindet, und wobei der Host und der Sensor direkt miteinander kommunizieren, wenn sich der Ausfallsicherungsschalter in dem zweiten Zustand befindet. In dem ersten Zustand operiert die Steuereinrichtung auf Mitteilungen zwischen dem Host und dem Sensor wie oben für den Host und das Werkzeug beschrieben. In dem zweiten Zustand umgeht der Ausfallsicherungsschalter die intelligente Steuereinrichtung, wobei der Host direkt mit dem Sensor kommuniziert. Andere Aspekte der weiteren Ausführungsform werden auf Kommunikationen zwischen dem Host, dem Werkzeug und dem Sensor angewendet.

[0065] Die intelligente Steuereinrichtung kann mehrere Ports für die Verbindung mit dem Werkzeug und dem Sensor umfassen, wobei die logischen Adressen der Ports, des Hosts, des Werkzeugs und des Sensors alle verschieden sind. Wie weiter oben erläutert, können diese logischen Adressen IP-Adressen oder Hardwareebenen-Kennzeichnungen sein.

[0066] Alle oben beschriebenen Verfahren können durch eine Zwischeneinrichtung und einen Ausfallsicherungsschalter realisiert werden, der eine direkte Verbindung zwischen der ersten und der zweiten Einrichtung für den Fall herzustellen, dass die Zwischeneinrichtung ausfallen sollte. Eine Ausführungsform umfasst eine Zwischeneinrichtung mit einer ersten und einer zweiten Netzwerkschnittstelle, die in einer Kommunikation jeweils mit der ersten und der zweiten Einrichtung verknüpft werden können, wobei die erste und die zweite Netzwerkschnittstelle jeweils Datenverknüpfungsschicht-Kennzeichnungen aufweisen, die sich von den Datenverknüpfungsschicht-Kennzeichnungen unterscheiden, die mit der ersten oder der zweiten Einrichtung verknüpft sind. Weiterhin umfasst die Ausführungsform einen Ausfallsicherungsschalter, der mit der Zwischeneinrichtung kommuniziert und unter Umständen mit der ersten und der zweiten Einrichtung kommuniziert. Der Ausfallsicherungsschalter weist wenigstens zwei Modi auf: einen normalen Betriebsmodus und einen Ausfallsicherungsmodus. In dem normalen Betriebsmodus verbindet der Ausfallsicherungsschalter die erste und die zweite

Einrichtung mit der ersten und der zweiten Netzwerkschnittstelle. In dem Ausfallsicherungsmodus verbindet der Schalter die erste und die zweite Einrichtung direkt miteinander und umgeht dabei die Zwischeneinrichtung. Die Verbindung kann elektrisch oder über einen Isolator erfolgen. Die Zwischeneinrichtung kann weiterhin eine Logik und Ressourcen umfassen, die für das wiederholte Senden von Signalen an den Ausfallsicherungsschalter ausgebildet sind, um einen korrekten Betrieb zu signalisieren. Der Ausfallsicherungsschalter umfasst weiterhin eine Logik und Ressourcen, die ausgebildet sind, um auf ein Ausbleiben der wiederholten Signale zu dem korrekten Betrieb zu reagieren, indem sie einen Wechsel zu einem Ausfallsicherungsmodus veranlassen.

[0067] Ein Aspekt der Erfindung kann darin bestehen, dass das Schalten zu dem Ausfallsicherungsmodus das Erzeugen eines hörbaren Signals wie etwa des Klicken eines Relais umfassen kann. Die Zwischeneinrichtung kann weiterhin in ihrer Logik und ihren Ressourcen ein Filter umfassen, das an die erste oder die zweite Einrichtung oder an die Zwischeneinrichtung adressierte Pakete für eine Handhabung behält, wobei das Filter mit der ersten und der zweiten Netzwerkschnittstelle verbunden ist. Das Filter gestattet, dass die Netzwerkschnittstellen in einem Promiskmodus betrieben werden. Die Logik und die Ressourcen des Filters können in einem Prozessor in der Zwischeneinrichtung oder aber in der Nähe von oder in den Netzwerkschnittstellen der Zwischeneinrichtung vorgesehen sein. Ein weiterer Aspekt besteht darin, dass die Logik und die Ressourcen der Zwischenschicht weiterhin einen Daemon umfassen, der eine Signalisierung für den Ausfallsicherungsschalter vorsieht. Dieser Daemon kann in jedem der für die vorstehenden Ausführungsformen beschriebenen Modi betrieben werden.

[0068] Die vorliegende Erfindung wurde mit Bezug auf die oben erläuterten bevorzugten Ausführungsformen und Beispiele beschrieben, wobei zu beachten ist, dass diese Ausführungsformen beispielhaft und nicht einschränkend beschrieben werden. Eine computergestützte Verarbeitung ist in den beschriebenen Ausführungsformen impliziert. Dementsprechend kann die vorliegende Erfindung in Verfahren für das computergestützte Erfassen, in Systemen mit einer Logik zum Ausführen einer Sensorsteuerung, in Systemen mit einer computergestützten Sensorsteuerung, in Medien mit einer Logik zum Ausführen einer computergestützten Sensorsteuerung, in Datenströmen mit einer Logik zum Ausführen einer computergestützten Sensorsteuerung oder in computergestützten Diensten zum Ausführen einer computergestützten Sensorsteuerung ausgeführt werden. Der Fachmann kann zahlreiche Modifikationen vorsehen und Kombinationen bilden, ohne dass deshalb der Erfindungsumfang verlassen wird.

Zusammenfassung

[0069] Die vorliegende Erfindung betrifft das Steuern und Sammeln von Daten von Sensoren, die mit Werkzeugen assoziiert sind. Insbesondere betrifft die vorliegende Erfindung die Verwendung einer Steuereinrichtung, um Kommunikationen zwischen einem Werkzeug, mit dem Werkzeug assoziierten Sensoren und Datenutzern wie etwa einem Host-System oder verteilten Prozessoren zu vermitteln. Besondere Aspekte der vorliegenden Erfindung werden in den Ansprüchen, in der Beschreibung und in den Zeichnungen beschrieben bzw. gezeigt.

Patentansprüche

1. Verfahren zum transparenten Herstellen einer Verbindung zwischen einer ersten und einer zweiten Einrichtung im Fall eines Ausfalls einer Zwischeneinrichtung, wobei das Verfahren umfasst:
Verbinden der ersten und der zweiten Einrichtung mit jeweils einer ersten und einer zweiten Netzwerkschnittstelle einer Zwischeneinrichtung, wobei die erste und die zweite Netzwerkschnittstelle Datenverknüpfungsschicht-Kennzeichnungen aufweisen, die sich von denjenigen unterscheiden, die mit der ersten oder der zweiten Einrichtung assoziiert sind,
wobei die Zwischeneinrichtung in einem normalen Modus zwischen der ersten und der zweiten Einrichtung adressierte Mitteilungen handhabt, während sie wiederholt Signale an einen Ausfallsicherungsschalter zu ihrem fortgesetztem korrekten Betrieb sendet, und
wobei der Ausfallsicherungsschalter bei einer Unterbrechung der wiederholten Signale zu dem korrekten Betrieb von der Zwischeneinrichtung zu einem Ausfallsicherungsmodus sichert, indem er die erste und die zweite Einrichtung direkt über eine Datenverbindung verbindet, die die Zwischeneinrichtung umgeht.

2. Verfahren nach Anspruch 1, wobei das Schalten des Ausfallsicherungsschalters zu dem Ausfallsicherungsmodus das Erzeugen eines hörbaren Signals umfasst.

3. Verfahren nach Anspruch 2, wobei das hörbare Signal ein Relaisklicken ist.

4. Verfahren nach Anspruch 1, wobei die erste und die zweite Netzwerkschnittstelle ausgebildet sind, um alle empfangenen Pakete zu einem Filter weiterzuleiten, das an die Zwischeneinrichtung adressierte Pakete für eine Verarbeitung zurückhält.

5. Verfahren nach Anspruch 1, wobei die Handhabung der Pakete für wenigstens einige Pakete das Weiterleiten der Pakete von der ersten oder zweiten Einrichtung zu entsprechend der zweiten oder ersten Einrichtung und das Spezifizieren einer Datenverknüpfungsschicht-Kennzeichnung der tatsächlichen Quelle in einem Quellenidentifikationsfeld der weitergeleiteten Pakete anstelle einer Datenverknüpfungs-Kennzeichnung der ersten oder zweiten Netzwerkschnittstelle umfasst.

6. Verfahren nach Anspruch 1, wobei das wiederholte Senden von Signalen zu dem fortgesetzten korrekten Betrieb durch einen Daemon implementiert wird, der auf der Zwischeneinrichtung ausgeführt wird und eine Mitteilung an den Ausfallsicherungsschalter sendet.

7. Verfahren nach Anspruch 1, wobei das wiederholte Senden von Signalen zu dem fortgesetzten korrekten Betrieb durch einen Daemon implementiert wird, der auf der Zwischeneinrichtung ausgeführt wird und auf Anfragen von dem Ausfallsicherungsschalter wartet und antwortet.

8. Verfahren nach Anspruch 1, das weiterhin eine Vielzahl von zweiten Einrichtungen umfasst, die mit der ersten Einrichtung unter Verwendung einer einzelnen physikalischen Kommunikationsverbindung verbunden ist.

9. Verfahren nach Anspruch 8, wobei die einzelne physikalische Kommunikationsverbindung ein Ethernet-Segment ist.

10. Verfahren nach Anspruch 1, die weiterhin eine Vielzahl von zweiten Einrichtungen umfasst, die unter Verwendung von zwei oder mehr physikalischen Kommunikationsverbindungen mit der ersten Einrichtung verbunden ist.

11. Verfahren nach Anspruch 10, wobei eine der physikalischen Kommunikationsverbindungen ein Ethernet-Segment und die andere eine serielle Verbindung ist.

12. Verfahren nach Anspruch 11, wobei die serielle Verbindung dem RS-232 oder RS-422-Standard entspricht.

13. Verfahren nach Anspruch 1, wobei das Herstellen einer direkten Kommunikationssitzung zwischen der ersten und der zweiten Einrichtung keine Aktualisierung von Tabellen, die Netzwerkadressen und Datenverknüpfungsschicht-Adressen miteinander korrelieren, in der ersten oder zweiten Einrichtung erfordert.

14. Verfahren nach Anspruch 1, wobei sich die Netzwerkadressen der ersten und der zweiten Einrichtung sowie der Zwischeneinrichtung alle innerhalb desselben Netzwerk-Subnetzes befinden.

15. Verfahren nach Anspruch 1, wobei das Herstellen einer direkten Kommunikationssitzung zwischen der ersten und der zweiten Einrichtung keine Aktualisierung von Tabellen, die IP- und MAC-Adressen miteinander korrelieren, in der ersten oder zweiten Einrichtung erfordert.

16. Ausfallsicherungsverfahren zum Herstellen einer Kommunikationsverbindung zwischen einem Host und einem Werkzeug nach einem Ausfall einer intelligenten Steuereinrichtung, die zwischen dem Host und dem Werkzeug verbunden ist, wobei das Verfahren umfasst:

Übernehmen einer ersten Hardwareebenen-Kennzeichnung, die ansonsten durch das Werkzeug verwendet wird, an einem ersten Port der intelligenten Steuereinrichtung und Bekanntmachen des ersten Ports an den Host als unter Verwendung der ersten Hardwareebenen-Kennzeichnung adressiert,

Übernehmen einer zweiten Hardwareebenen-Kennzeichnung, die ansonsten durch den Host verwendet wird, an einem zweiten Port der intelligenten Steuereinrichtung und Bekanntmachen des zweiten Ports an das Werkzeug als unter Verwendung der zweiten Hardwareebenen-Kennzeichnung adressiert,

Abfangen von Bekanntmachungen der ersten und zweiten Hardwareebenen-Kennzeichnungen an der intelligenten Steuereinrichtung, sodass der Host und das Werkzeug nicht in einer direkten Bekanntmachungs-Kommunikation stehen,

wiederholtes Senden von Signalen an einen Ausfallsicherungsschalter, um demselben zu signalisieren, dass die intelligente Steuereinrichtung zuverlässig ist, wobei der Ausfallsicherungsschalter ausgebildet ist, um bei

einem Ausbleiben des wiederholten Sendens von Signalen den Host direkt über eine Kommunikationsverbindung, die die intelligente Steuereinrichtung umgibt, mit dem Werkzeug zu verbinden, wobei der Host und das Werkzeug in einer direkten Bekanntmachungs-Kommunikation stehen und die Bekanntmachungen der ersten und zweiten Hardwareebenen-Kennzeichnungen die Herstellung der Kommunikationsverbindung zwischen dem Host und dem Werkzeug bewerkstelligen.

17. Verfahren nach Anspruch 16, wobei eine erste logische IP-Adresse, die den ersten Port identifiziert, eine zweite logische IP-Adresse, die durch das Werkzeug verwendet wird, eine dritte logische IP-Adresse, die den zweiten Port identifiziert, und eine vierte logische IP-Adresse, die durch das Werkzeug verwendet wird, jeweils verschieden sind.

18. Verfahren nach Anspruch 16, wobei eine erste logische Netzwerkschichtadresse, die den ersten Port identifiziert, eine zweite logische Netzwerkschichtadresse, die durch das Werkzeug verwendet wird, eine dritte logische Netzwerkschichtadresse, die den zweiten Port identifiziert, und eine vierte logische Netzwerkschichtadresse, die durch den Host verwendet wird, jeweils verschieden sind.

19. Verfahren nach Anspruch 16, wobei die Hardwareebenen-Kennzeichnung eine MAC-Adresse ist.

20. Verfahren nach Anspruch 16, wobei die Bekanntmachungen der Hardwareebenen-Kennzeichnungen durch standardkonforme ARP-Mitteilungen erfolgen.

21. Verfahren nach Anspruch 16, das weiterhin auf einen Sensor angewendet wird, der das Werkzeug überwacht, wobei die intelligente Steuereinrichtung zwischen dem Host und dem Sensor verbunden ist, wobei das Verfahren weiterhin umfasst:

Übernehmen einer dritten Hardwareebenen-Kennzeichnung, die ansonsten durch den Sensor verwendet wird, an dem ersten Port der intelligenten Steuereinrichtung und Bekanntmachen des ersten Ports an den Host als unter Verwendung der dritten Hardwareebenen-Kennzeichnung adressiert,

Bekanntmachen des zweiten Ports an den Sensor als unter Verwendung der zweiten Hardwareebenen-Kennzeichnung adressiert, und

Abfangen der Bekanntmachungen der dritten Hardwareebenen-Kennzeichnung an der intelligenten Steuereinrichtung, sodass der Host und der Sensor nicht in einer direkten Bekanntmachungs-Kommunikation stehen, wobei der Ausfallsicherungsschalter bei einem Ausbleiben des wiederholten Sendens von Signalen eine direkte Kommunikationsverbindung zwischen dem Host und dem Sensor herstellt, die die intelligente Steuereinrichtung umgeht.

22. Verfahren nach Anspruch 21, wobei eine erste logische IP-Adresse, die den ersten Port identifiziert, eine zweite logische IP-Adresse, die durch das Werkzeug verwendet wird, eine dritte logische IP-Adresse, die den zweiten Port identifiziert, eine vierte logische IP-Adresse, die durch den Host verwendet wird, und eine fünfte logische IP-Adresse, die durch den Sensor verwendet wird, jeweils verschieden sind.

23. Verfahren nach Anspruch 21, wobei eine erste logische Netzwerkschichtadresse, die den ersten Port identifiziert, eine zweite logische Netzwerkschichtadresse, die durch das Werkzeug verwendet wird, eine dritte logische Netzwerkschichtadresse, die den zweiten Port identifiziert, eine vierte logische Netzwerkschichtadresse, die durch den Host verwendet wird, und eine fünfte logische Netzwerkschichtadresse, die durch den Sensor verwendet wird, jeweils verschieden sind.

24. Verfahren nach Anspruch 21, wobei die Hardwareebenen-Kennzeichnung eine MAC-Adresse ist.

25. Verfahren nach Anspruch 21, wobei die Bekanntmachungen der Hardwareebenen-Kennzeichnungen durch standardkonforme ARP-Mitteilungen erfolgen.

26. Verfahren zum Einfügen einer gegenüber einem Ausfall geschützten intelligenten Steuereinrichtung und eines Schalters in eine Kommunikationsverbindung zwischen einem Host und wenigstens einem damit verbundenen Werkzeug, wobei das Verfahren umfasst:

Verbinden des Schalters mit dem Host, der intelligenten Steuereinrichtung und dem Werkzeug, wobei der Host und das Werkzeug mit der intelligenten Steuereinrichtung und nicht direkt miteinander kommunizieren, wenn sich der Schalter in einem ersten Zustand befindet, und wobei der Host und das Werkzeug direkt miteinander kommunizieren, wenn sich der Schalter in einem zweiten Zustand befindet, wobei die intelligente Steuereinrichtung in dem ersten Zustand:

Mitteilungen zwischen dem Host und dem Werkzeug abfängt,

wenigstens eine Hardwareebenen-Quellkennzeichnung und wenigstens eine Hardwareebenen-Zielkennzeichnung in den abgefangenen Mitteilungen modifiziert,
 wenigstens einen Fehlerkorrekturcode in den abgefangenen Mitteilungen modifiziert, damit dieser den modifizierten Hardwareebenen-Kennzeichnungen entspricht, und
 die abgefangenen Mitteilungen mit den modifizierten Hardwareebenen-Kennzeichnungen und dem modifizierten Korrekturcode weiterleitet, und
 der Schalter in dem zweiten Zustand die intelligente Steuereinrichtung umgeht, sodass der Host direkt mit dem Werkzeug kommuniziert.

27. Verfahren nach Anspruch 26, wobei die intelligente Steuereinrichtung wenigstens einen ersten Port und einen zweiten Port umfasst, wobei der erste Port mit dem Host kommuniziert und der zweite Port mit dem Werkzeug kommuniziert, und eine erste logische IP-Adresse, die den ersten Port identifiziert, eine zweite logische IP-Adresse, die durch das Werkzeug verwendet wird, eine dritte logische IP-Adresse, die den zweiten Port identifiziert, und eine vierte logische IP-Adresse, die durch den Host verwendet wird, jeweils verschieden sind.

28. Verfahren nach Anspruch 26, wobei die intelligente Steuereinrichtung wenigstens einen ersten Port und einen zweiten Port umfasst, wobei der erste Port über den Schalter mit dem Host kommuniziert und der zweite Port über den Schalter mit dem Werkzeug kommuniziert, und eine erste logische Netzwerkschichtadresse, die den ersten Port identifiziert, eine zweite logische Netzwerkschichtadresse, die durch das Werkzeug verwendet wird, eine dritte logische Netzwerkschichtadresse, die den zweiten Port identifiziert, und eine vierte logische Netzwerkschichtadresse, die durch den Host verwendet wird, jeweils verschieden sind.

29. Verfahren nach Anspruch 26, wobei die Hardwareebenen-Kennzeichnung eine MAC-Adresse ist.

30. Verfahren nach Anspruch 26, das weiterhin auf wenigstens einen Sensor angewendet wird, der das Werkzeug überwacht, wobei das Verfahren weiterhin umfasst:
 Verbinden des Ausfallsicherungsschalters mit dem Sensor, wobei der Host und der Sensor mit der intelligenten Steuereinrichtung und nicht direkt miteinander kommunizieren, wenn sich der Ausfallsicherungsschalter in dem ersten Zustand befindet, und wobei der Host und der Sensor direkt miteinander kommunizieren, wenn sich der Ausfallsicherungsschalter in dem zweiten Zustand befindet, wobei die intelligente Steuereinrichtung in dem ersten Zustand:
 Mitteilungen zwischen dem Host und dem Werkzeug abfängt,
 wenigstens eine Hardwareebenen-Quellkennzeichnung und wenigstens eine Hardwareebenen-Zielkennzeichnung in den abgefangenen Mitteilungen modifiziert,
 wenigstens einen Fehlerkorrekturcode in den abgefangenen Mitteilungen modifiziert, damit dieser den modifizierten Hardwareebenen-Kennzeichnungen entspricht, und
 die abgefangenen Mitteilungen mit den modifizierten Hardwareebenen-Kennzeichnungen und dem modifizierten Korrekturcode weiterleitet, und
 der Ausfallsicherungsschalter in dem zweiten Zustand die intelligente Steuereinrichtung umgeht, sodass der Host direkt mit dem Werkzeug kommuniziert.

31. Verfahren nach Anspruch 30, wobei die intelligente Steuereinrichtung wenigstens einen ersten Port und einen zweiten Port umfasst, wobei der erste Port über den Ausfallsicherungsschalter mit dem Host kommuniziert und der zweite Port über den Ausfallsicherungsschalter mit dem Werkzeug und dem Sensor kommuniziert, und eine erste logische IP-Adresse, die den ersten Port identifiziert, eine zweite logische IP-Adresse, die durch das Werkzeug verwendet wird, eine dritte logische IP-Adresse, die den zweiten Port identifiziert, eine vierte logische IP-Adresse, die durch den Host verwendet wird, und eine fünfte logische IP-Adresse, die durch den Sensor verwendet wird, jeweils verschieden sind.

32. Verfahren nach Anspruch 30, wobei die intelligente Steuereinrichtung wenigstens einen ersten Port und einen zweiten Port umfasst, wobei der erste Port über den Ausfallsicherungsschalter mit dem Host kommuniziert und der zweite Port über den Ausfallsicherungsschalter mit dem Werkzeug und dem Sensor kommuniziert, und eine erste logische Netzwerkschichtadresse, die den ersten Port identifiziert, eine zweite logische Netzwerkschichtadresse, die durch das Werkzeug verwendet wird, eine dritte logische Netzwerkschichtadresse, die den zweiten Port identifiziert, eine vierte logische Netzwerkschichtadresse, die durch den Host verwendet wird, und

eine fünfte logische Netzwerkschichtadresse, die durch den Sensor verwendet wird, jeweils verschieden sind.

33. Verfahren nach Anspruch 30, wobei die intelligente Steuereinrichtung wenigstens einen ersten Port, einen zweiten Port und einen dritten Port umfasst, wobei der erste Port über den Ausfallsicherungsschalter mit dem Host kommuniziert, der zweite Port über den Ausfallsicherungsschalter mit dem Werkzeug kommuniziert und der dritte Port über den Ausfallsicherungsschalter mit dem Sensor kommuniziert, und eine erste logische IP-Adresse, die den ersten Port identifiziert, eine zweite logische IP-Adresse, die durch das Werkzeug verwendet wird, eine dritte logische IP-Adresse, die den zweiten Port identifiziert, eine vierte logische IP-Adresse, die durch den Host verwendet wird, und eine fünfte logische IP-Adresse, die durch den Sensor verwendet wird, jeweils verschieden sind.

34. Verfahren nach Anspruch 30, wobei die intelligente Steuereinrichtung wenigstens einen ersten Port, einen zweiten Port und einen dritten Port umfasst, wobei der erste Port über den Ausfallsicherungsschalter mit dem Host kommuniziert, der zweite Port über den Ausfallsicherungsschalter mit dem Werkzeug kommuniziert und der dritte Port über den Ausfallsicherungsschalter mit dem Sensor kommuniziert, und eine erste logische Netzwerkschichtadresse, die den ersten Port identifiziert, eine zweite logische Netzwerkschichtadresse, die durch das Werkzeug verwendet wird, eine dritte logische Netzwerkschichtadresse, die den zweiten Port identifiziert, eine vierte logische Netzwerkschichtadresse, die durch den Host verwendet wird, und eine fünfte logische Netzwerkschichtadresse, die durch den Sensor verwendet wird, jeweils verschieden sind.

35. Zwischeneinrichtung mit einem Ausfallsicherungsschalter, der ausgebildet ist, um im Fall eines Ausfalls der Zwischeneinrichtung eine direkte Verbindung zwischen einer ersten und einer zweiten Einrichtung sicherzustellen, mit:
die Zwischeneinrichtung, die eine erste und eine zweite Netzwerkschnittstelle aufweist, die jeweils mit der ersten und der zweiten Einrichtung verbunden sind, wobei die erste und die zweite Netzwerkschnittstelle Datenverbindungsschicht-Kennzeichnungen aufweisen, die sich von den mit der ersten oder zweiten Einrichtung assoziierten Datenverbindungsschicht-Kennzeichnungen unterscheiden,
den Ausfallsicherungsschalter, der mit der Zwischeneinrichtung kommuniziert und gegebenenfalls mit der ersten und der zweiten Einrichtung verbunden wird, wobei der Ausfallsicherungsschalter in einem normalen Betriebsmodus betrieben werden kann, in dem die erste und die zweite Einrichtung jeweils mit der ersten und der zweiten Netzwerkschnittstelle kommunizieren, und in einem Ausfallsicherungsmodus, in dem die ersten und die zweite Einrichtung direkt miteinander kommunizieren und die Zwischeneinrichtung umgehen, wobei die Logik und die Ressourcen der Zwischeneinrichtung ausgebildet sind, um wiederholt Signale zu einem korrekten Betrieb der Zwischeneinrichtung an den Ausfallsicherungsschalter zu senden, und die Logik und die Ressourcen des Ausfallsicherungsschalters ausgebildet sind, um bei einem Ausbleiben des wiederholten Sendens der Signale zu dem korrekten Betrieb von der Zwischeneinrichtung zu reagieren, indem der Ausfallsicherungsschalter zu einem Ausfallsicherungsmodus geschaltet wird.

36. Zwischeneinrichtung und Ausfallsicherungsschalter nach Anspruch 35, wobei das Schalten des Ausfallsicherungsschalters zu dem Ausfallsicherungsmodus weiterhin das Erzeugen eines hörbaren Signals umfasst.

37. Zwischeneinrichtung und Ausfallsicherungsschalter nach Anspruch 36, wobei das hörbare Signal ein Relais-Klicken ist.

38. Zwischeneinrichtung und Ausfallsicherungsschalter nach Anspruch 35, wobei die Logik und die Ressourcen der Zwischeneinrichtung weiterhin ein Filter umfassen, das an die Zwischeneinrichtung adressierte Pakete für eine Verarbeitung zurückhält, wobei das Filter mit der ersten und der zweiten Netzwerkschnittstelle verbunden ist.

39. Zwischeneinrichtung und Ausfallsicherungsschalter nach Anspruch 35, wobei die Logik und die Ressourcen der Zwischeneinrichtung weiterhin einen Daemon umfassen, der auf der Zwischeneinrichtung ausgeführt wird und eine Mitteilung an den Ausfallsicherungsschalter sendet.

40. Zwischeneinrichtung und Ausfallsicherungsschalter nach Anspruch 35, wobei die Logik und die Ressourcen der Zwischeneinrichtung weiterhin einen Daemon umfassen, der auf der Zwischeneinrichtung ausgeführt wird und auf Anfragen von dem Ausfallsicherungsschalter wartet und antwortet.

Es folgen 4 Blatt Zeichnungen

Anhängende Zeichnungen

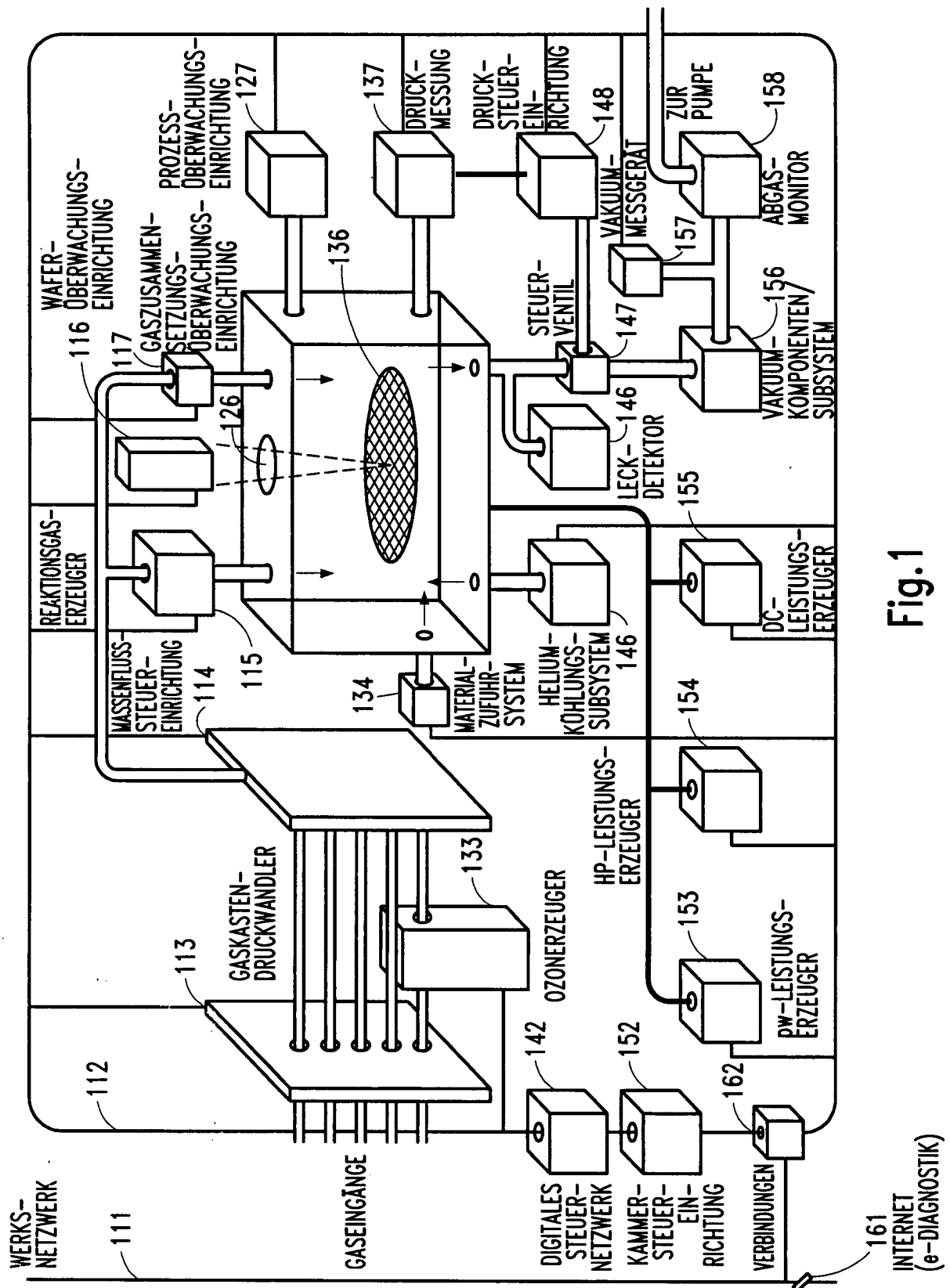


Fig. 1

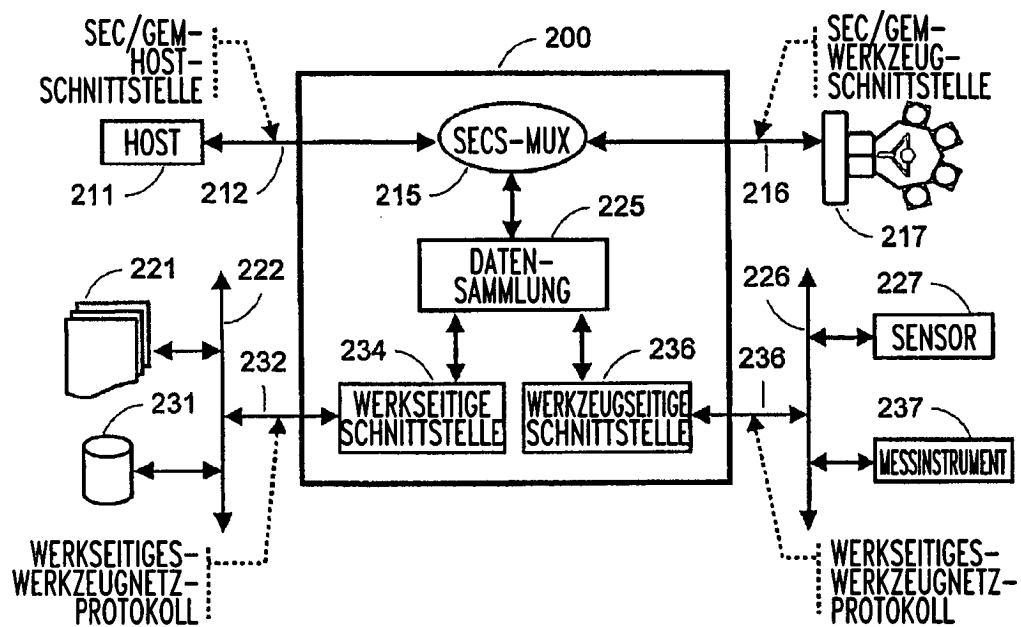


Fig.2

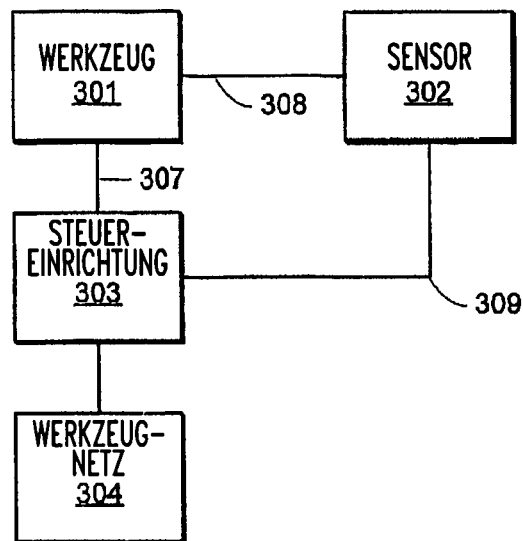


Fig.3

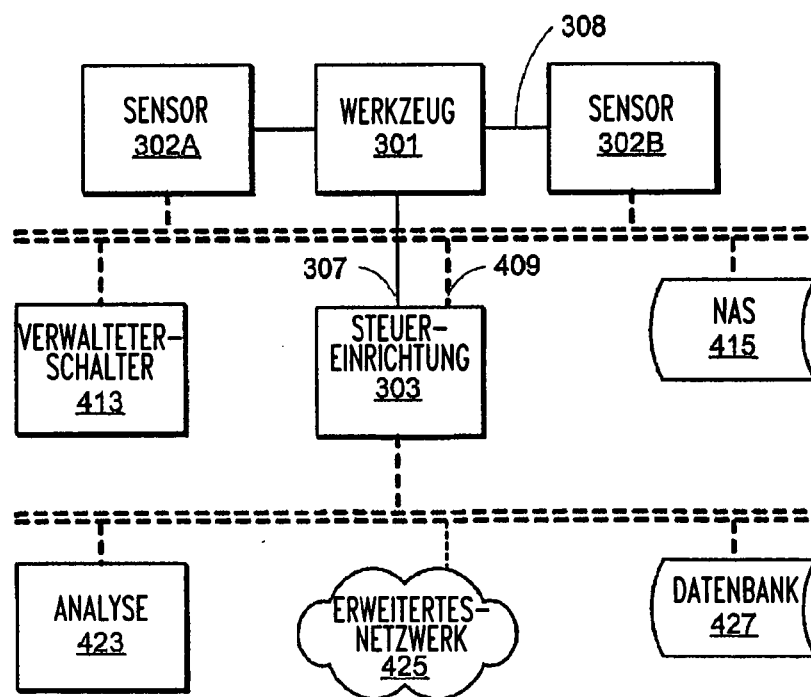


Fig.4

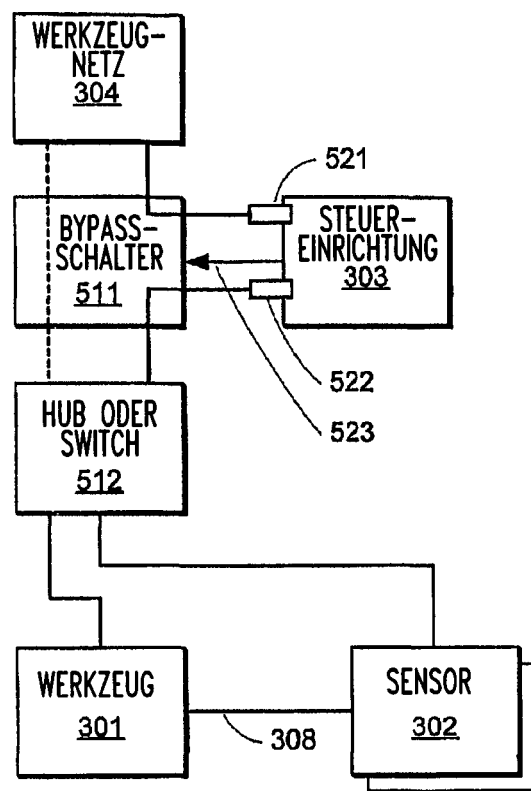


Fig.5

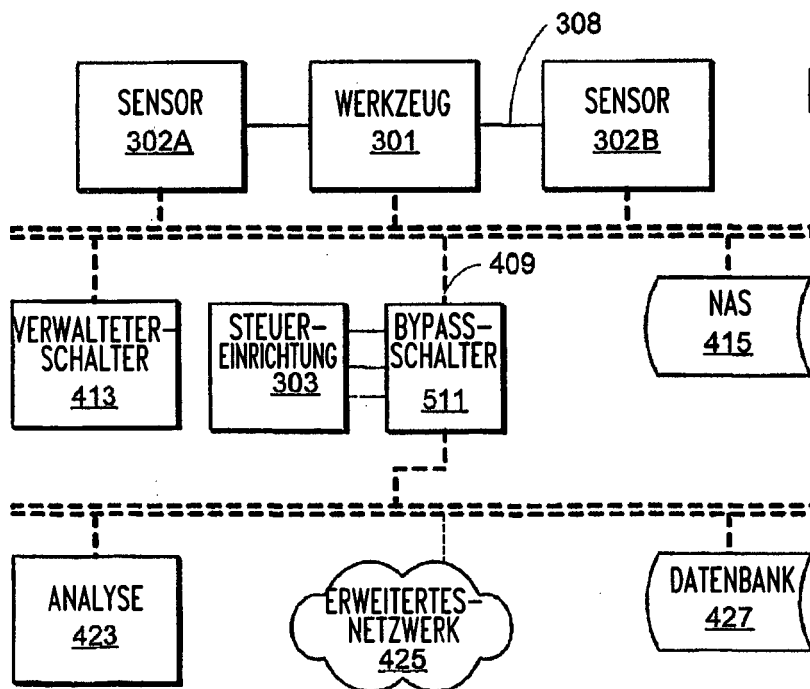


Fig.6