



(19)
Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 10 2004 059 630 A1 2006.06.14**

(12)

Offenlegungsschrift

(21) Aktenzeichen: **10 2004 059 630.1**

(22) Anmeldetag: **10.12.2004**

(43) Offenlegungstag: **14.06.2006**

(51) Int Cl.⁸: **G07D 7/00 (2006.01)**

(71) Anmelder:
Bundesdruckerei GmbH, 10969 Berlin, DE

(74) Vertreter:
FROHWITTER Patent- und Rechtsanwälte, 81679 München

(72) Erfinder:
Demanowski, Hans, 10117 Berlin, DE

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

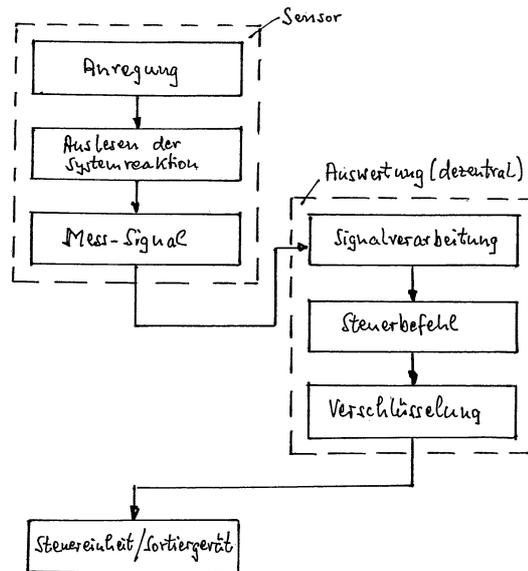
DE 102 24 256 A1
US2002/00 26 422 A1
US 64 18 358 B1
US 60 26 175
US 59 09 502

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gemäß § 44 PatG ist gestellt.

(54) Bezeichnung: **Verfahren zur Echtheitsüberprüfung und Sortierung von Wertdokumenten und Hochsicherheitssensoren zur Durchführung des Verfahrens**

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren zur Echtheitsüberprüfung und Sortierung von Wertdokumenten mittels eines Hochsicherheitssensors, wobei ein Messsignal durch Abgabe eines Testsignals erzeugt und die resultierende Systemreaktion durch den Sensor ausgelesen sowie ein Messsignal erzeugt wird. Das Messsignal wird nach einem vorgegebenen Algorithmus in einer Signalverarbeitungseinrichtung mit Mitteln initiiert und/oder ausgewertet, die in getrennten Sicherheitsbereichen geführt werden. Das Verfahren sieht danach das Ausgeben eines Steuerbefehls zur Steuerung einer Sortiereinheit vor. Die Erfindung betrifft des Weiteren einen Hochsicherheitssensor zur Durchführung des Verfahrens.



Beschreibung

Stand der Technik

[0001] Die Erfindung betrifft ein Verfahren zur Echtheitsüberprüfung und Sortierung von Wertdokumenten mittels eines Hochsicherheitssensors, der ein sensoreigenes Testsignal abgibt, die Systemreaktion ausliest und ein dementsprechendes Messsignal abgibt, sowie einen Hochsicherheitssensor zur Durchführung des Verfahrens.

[0002] Wertdokumente wie Banknoten sind mit diversen Sicherheitsmerkmalen ausgestattet, die eine missbräuchliche Nachahmung erschweren oder unmöglich machen sollen. Moderne Hochsicherheitsmerkmale sind dabei nicht nur per se schwer nachzuahmen, vielmehr ist auch nicht ohne weiteres feststellbar, was bei einer Überprüfung genau analysiert und in welcher Weise es ausgewertet wird. Zum Gebiet der Hochsicherheitsmerkmale gehören beispielsweise elektrolumineszierende Substanzen, die in einem geeigneten elektromagnetischen Wechselfeld zum Leuchten in einem charakteristischen Spektrum angeregt werden (DE 197 58 587 C2; DE 197 35 293 C2, DE 199 53 924 A1).

[0003] Zur Echtheitsüberprüfung werden spezielle Sensoren eingesetzt, die herkömmlich eine Einrichtung zur Abgabe des Anregungssignals sowie eine Empfangseinrichtung aufweisen, mit der die Systemreaktion ausgelesen wird. Das hiervon abgegebene Messsignal wird anschließend in einer Signalverarbeitungseinrichtung ausgewertet, die letztlich einen Steuerbefehl an die Sortiereinrichtung abgibt, wonach die als nicht echt erkannten Dokumente ausgeworfen werden.

[0004] Derartige Sensoren unterliegen besonderen Sicherheitsmaßnahmen und werden nur von wenigen autorisierten Institutionen in streng abgesicherten Bereichen eingesetzt, um so mit hoher Wahrscheinlichkeit auszuschließen, dass Unbefugte in den Besitz des Sensors gelangen, seine Funktionsweise analysieren und sich so das nötige Wissen für Fälschungen aneignen können. Es muss also verhindert werden, dass Unbefugte Hochsicherheitssensoren testen, um Hinweise zur Optimierung ihrer illegalen Tätigkeit zu gewinnen. Dies bedingt einen hohen Aufwand an Sicherheitsmaßnahmen und schließt eine breitere kommerzielle Anwendung der Hochsicherheitssensoren aus.

Aufgabenstellung

[0005] Der Erfindung liegt deshalb die Aufgabe zugrunde, eine verbesserte Absicherung von Hochsicherheitssensoren anzugeben, um diese ohne erhöhtes Risiko flächendeckend einsetzen zu können. Dies wird erfindungsgemäß mit einem Verfahren zur

Echtheitsüberprüfung und Sortierung von Wertdokumenten mittels eines Hochsicherheitssensors, erreicht, das die Schritte aufweist:

Erzeugen eines Messsignals durch Abgabe eines Testsignals und Lesen der resultierenden Systemreaktion durch den Sensor;

Auswerten des Messsignals nach einem vorgegebenen Algorithmus in einer Signalverarbeitungseinrichtung mit Mitteln, die in einem getrennten Sicherheitsbereich geführt werden und

Ausgeben eines Steuerbefehls zur Steuerung einer Sortiereinheit.

[0006] Erfindungsgemäß werden also Signalerzeugung und Signalverarbeitung zumindest teilweise getrennt und in getrennten Sicherheitsbereichen, beispielsweise in einem Trustcenter, geführt, so dass sich ein potenzieller Angreifer alle Systemteile beschaffen muss, weil ein Teil alleine keine auswertbaren Daten liefert.

[0007] Vorzugsweise wird dem Sensor zumindest ein externes Führungssignal zugeführt, welches die ordnungsgemäße Funktion des Sensors sicherstellt. Dies geschieht insbesondere durch Erzeugung eines verschlüsselten ersten Führungssignals in einem räumlich vom eigentlichen Hochsicherheitssensor getrennten Bereich. Erst die nachfolgende verschlüsselte Interaktion zwischen dem ersten Führungssignal und dem Hochsicherheitssensor versetzt diesen in die Lage, das vorbestimmte Testsignals auszusenden. Das Führungssignal kann dem Sensor bspw. in der Weise zugeführt werden, dass es die Sensoreinstellungen selbst steuert. So lassen sich zum angegebenen Zweck bei einem Elektrolumineszenz-Sensor Frequenz, Spannung und/oder spektrale Auswertung des Lumineszenzsignals steuern. In anderer bevorzugter Ausführung wird das Führungssignal in Gestalt eines zweiten Führungssignals der Signalverarbeitung im Sensor zugeführt und zusammen mit dem Messsignal verarbeitet. Mit Vorteil lassen sich erstes und zweites Führungssignal auch zusammen einsetzen, um so eine besonders hohe Absicherung zu gewährleisten.

[0008] In vorteilhaften Ausführungen wird das Führungssignal dem Sensor über eine Datenleitung, insbesondere über eine Standleitung oder per Funk, zugeführt. Ebenso kann das Messsignal über eine solche Verbindung an den getrennten Sicherheitsbereich übertragen werden. Für Test- und Messsignale können insbesondere unterschiedliche Führungssignale und unterschiedliche Verschlüsselungen verwendet werden. Das erste und/oder zweite Führungssignal umfasst bevorzugt einen on-line übermittelten Rechenalgorithmus, mit dem Test- und/oder Messsignal verarbeitet werden. Das Ergebnis der Messsignalverarbeitung wird an den getrennten Sicherheitsbereich zurückgemeldet. Dort wird es wieder zurückgewandelt, worauf das Messsignal ausgewertet und

ein Steuerbefehl ermittelt werden, der wiederum an den Sensor zurückgeleitet wird.

[0009] In einer anderen vorteilhaften Variante wird das Führungssignal dem Sensor off-line zugeführt. Dies kann mittels eines Datenträgers, insbesondere mittels einer Chip-Karte, erfolgen. Dieser Datenträger kann nach der Arbeitszeit durch einen Verantwortlichen entfernt werden. Nach dem Vier-Augen-Prinzip oder Sechs-Augen-Prinzip ist auch der Einsatz mehrerer Chip-Karten möglich.

[0010] Das Führungssignal wird vorzugsweise in vorbestimmten Intervallen verändert. Dies erschwert zusätzlich ein Ausspionieren der Sensorfunktionen und kann weiter dadurch ergänzt werden, dass dem Sensor ein weiteres, drittes Führungssignal in vorbestimmten – idealerweise kürzeren – Intervallen zugeführt wird, das einen im Sensor vorgesehenen Selbstzerstörungsmechanismus blockiert. Fällt diese Signal über einen festgelegten Zeitraum hinweg aus, z. B. weil der Originalsensor entwendet wurde, tritt die Selbstzerstörung ein, und der Sensor wird unbrauchbar. Ein solches zweites Führungssignal wird sinnvollerweise lokal, aber in einem räumlich getrennten Sicherheitsbereich erzeugt. Der Sensor kann dabei alleine schon durch dieses dritte, die Selbstzerstörung verhindernde Führungssignal gesichert werden. Selbstzerstörung bedeutet dabei, dass der Sensor unbrauchbar gemacht wird, was bspw. auch durch Entfernen bzw. Löschen der in einem Speicher abgelegten Daten erreicht werden kann.

[0011] Eine andere bevorzugte Ausführung besteht darin, das vom Sensor ermittelte Messsignal an eine räumlich getrennte Auswertestation zu übertragen, die in einem eigenen Sicherheitsbereich vorgesehen ist, in dem die Signalverarbeitung nach dem vorgegebenen Algorithmus erfolgt und ein Steuerbefehl erzeugt wird, der nach Verschlüsselung nicht mehr dem Sensor sondern der Sortiereinheit zugeführt wird. In diesem Fall wird das Messsignal breitbandig übertragen, wobei insbesondere Tarnsignale zugemischt werden können, die bei der Signalverarbeitung unberücksichtigt bleiben, ein Ausspionieren des realen Messsignals aber erschweren.

[0012] Die Auswertung wird mittels einer Zeitschaltung außerhalb der überwachten Zeiten, insbesondere außerhalb der Dienstzeit der Sortiereinrichtung mit Vorteil ausgeschaltet, um unbefugte Versuche der Signalanalyse vor Ort, z. B. während der Nachtstunden, zu unterbinden.

[0013] Erfindungsgemäß wird die Aufgabe ferner gelöst durch einen Hochsicherheitssensor zur Durchführung des vorgenannten Verfahrens, wobei dieser Sensor eine Einrichtung zur Abgabe eines Testsignals, eine Leseeinrichtung zum Lesen der resultierenden Systemreaktion und zur Erzeugung eines

Messsignals aufweist. Des Weiteren besitzt er eine Empfangseinrichtung zum Empfang eines externen Führungssignals. Eine Signalverarbeitungseinrichtung verarbeitet das Messsignal zusammen mit dem Führungssignal nach einem vorgegebenen Algorithmus. Außerdem ist eine Einrichtung zum Ausgeben eines Steuerbefehls, mit dem eine Sortiereinheit steuerbar ist, vorgesehen.

[0014] In einer besonders vorteilhaften Ausführung umfasst die Empfangseinrichtung zum Empfang des externen Führungssignals eine Lesestation für einen Datenträger, insbesondere für eine Chip-Karte, die fallweise entfernt und in vorbestimmten Intervallen mit geändertem Führungssignal erneuert werden kann.

[0015] In einer anderen Ausführungsform der Erfindung umfasst der Hochsicherheitssensor eine Einrichtung zur Abgabe eines Testsignals, eine Leseeinrichtung zum Lesen der resultierenden Systemreaktion und zur Erzeugung eines Messsignals und besitzt eine Einrichtung zur Übertragung des Messsignals an eine Signalverarbeitungseinrichtung in einem räumlich getrennten Sicherheitsbereich. Hierbei ist bevorzugt eine Einrichtung zur Erzeugung von Tarnsignalen vorgesehen, die dem Messsignal breitbandig überlagerbar sind und bei der späteren Signalverarbeitung unberücksichtigt bleiben. Der Hochsicherheitssensor ist dabei bevorzugt ebenfalls mit einer Einrichtung zum Empfang eines Führungssignals ausgestattet, das seinen ordnungsgemäßen Betrieb sicherstellt.

Ausführungsbeispiel

[0016] Weitere Merkmale und Vorteile der Erfindung ergeben sich aus der nachfolgenden Beschreibung der Figuren.

[0017] Es zeigen:

[0018] [Fig. 1](#): ein erstes Ausführungsbeispiel mit Signalverarbeitung mittels erster und zweiter Führungssignale;

[0019] [Fig. 2](#): ein Ausführungsbeispiel mit dezentraler Signalverarbeitung;

[0020] [Fig. 1](#) zeigt das Prinzip der Trennung von Signalerzeugung und Signalverarbeitung unter Einbeziehung eines externer Führungssignale. Im Sensor befindet sich eine Anregungseinrichtung, beispielsweise eine Elektrodenanordnung, mit der ein elektromagnetisches Wechselfeld an das zu prüfende Wertdokument angelegt wird. Im Dokument befindliche elektrolumineszierende Pigmente werden damit zum Leuchten mit einem charakteristischen Spektrum angeregt, das von einem Empfänger ausgelesen wird. Das resultierende Messsignal wird einer Signalverar-

beutungseinrichtung zugeführt, die das Lumineszenzspektrum nach vorgegebenen Kriterien auswertet. Der Sensor gibt zuletzt einen Steuerbefehl an die Steuereinheit eines Sortiergeräts, mit dessen Hilfe die als falsch erkannten Dokumente ausgesondert werden.

[0021] Um aktiv werden zu können benötigt der Sensor ein externes erstes Führungssignal, das im gezeigten Beispiel von einem Trustcenter geliefert wird, aber auch von einem anderen Sicherheitsbereich kommen kann.

[0022] Der Sensor arbeitet auch bezüglich der Signalverarbeitung nicht autonom, sondern bedarf zusätzlicher Information. Im gezeigten Beispiel erhält der Sensor, beispielsweise über eine Standleitung, ein zweites Führungssignal, das ebenfalls aus einem räumlich getrennten Sicherheitsbereich wie dem gezeigten Trustcenter geliefert wird. Die im Sensor befindliche Signalverarbeitungseinrichtung verarbeitet das Messsignal zusammen mit dem Führungssignal und ist erst damit in der Lage, ersteres ordnungsgemäß nach einem vorgegebenen Algorithmus auszuwerten und einen zutreffenden Steuerbefehl abzugeben. Der Sensor alleine liefert damit potentiellen Fälschern keine relevanten Informationen, die sie missbräuchlich verwerten könnten, weil der Sensor für sich alleine nichts Verwertbares offenbart.

[0023] Das Führungssignal kann auch auf andere Sensorkomponenten, steuernd einwirken, was jeweils zu internen Situationen führt, die nur dem Absender der Signale selbst verständlich sind. Die Systemdaten können dabei variabel gestaltet werden. Außerdem kann das System auf mehr als zwei getrennte Bereiche verteilt werden. Die Anzahl der Systembausteine kann durch das Hinzufügen zusätzlicher Ver- und Entschlüsselungsschritte in jeweils getrennten Bereichen, beispielsweise verschiedene Hierarchieebenen, beliebig erhöht werden. Die Funktionsfähigkeit des Gesamtsystems setzt die konzentrierte Aktion aller Ebenen voraus; der Verlust einzelner Komponenten führt nicht zum Verlust der Systemsicherheit insgesamt. Mit diesen Maßnahmen läßt sich vermeiden, dass aktuelle Sensoreinstellungen oder der Algorithmus der Signalverarbeitung analysiert werden. Ebenso wenig können aus dem Sortierergebnis Rückschlüsse gezogen werden, wie sich bestimmte Sicherheitselemente und zugehörige Prüfmethode umgehbar sein könnten.

[0024] Ein weiteres Ausführungsbeispiel zeigt [Fig. 2](#). Im Sensor selbst befinden sich wiederum die Einrichtungen zur Anregung der Sicherheitselemente, zum Auslesen der Systemreaktion und zur Ermittlung des Messsignals. Das vom Sensor erzeugte Signal wird aber nicht im Sensor selbst ausgewertet sondern einer dezentralen Auswertung zugeführt, die sich in einem getrennten Sicherheitsbereich, bei-

spielsweise in einem anderen Raum, Schaltzentrale, Panzerschrank oder dergleichen befindet. Das vom Sensor übertragene Signal ist breitbandig und enthält Daten, die für die spätere Auswertung nicht notwendig sind, oder ist aktiv durch zusätzliche Tarnsignale angereichert, was einen potenziellen Angriff auf das System zusätzlich erschwert. Zusätzlich kann auch hier der Sensor wie in [Fig. 1](#) so gestaltet sein, dass er erst bei Empfang eines Führungssignals aktiviert wird.

[0025] Der in der Auswerteeinrichtung ermittelte Steuerbefehl geht verschlüsselt direkt an das Sortiergerät, beispielsweise an eine gesonderte dort installierte Empfangseinrichtung, wo er nach entsprechender Dekodierung die Aussortierung der als falsch erkannten Dokumente steuert. Auch in diesem Fall ist die unmittelbare Rückkopplung bezüglich des Sortierergebnisses weitgehend unmöglich gemacht, weil der Steuerbefehl nicht zurück an den Sensor sondern unmittelbar an die Sortiermaschine geht.

Patentansprüche

1. Verfahren zur Echtheitsüberprüfung und Sortierung von Wertdokumenten mittels eines Hochsicherheitssensors, mit den Schritten:

- Erzeugen eines Messsignals durch Abgabe eines Testsignals und Lesen der resultierenden Systemreaktion durch den Sensor,
- Auswerten des Messsignals nach einem vorgegebenen Algorithmus in einer Signalverarbeitungseinrichtung mit Mitteln, die in getrennten Sicherheitsbereichen geführt werden, und
- Ausgeben eines Steuerbefehls zur Steuerung einer Sortiereinheit.

2. Verfahren nach Anspruch 1, wobei dem Sensor zumindest ein externes Führungssignal zugeführt wird, welches einen vorbestimmten, ordnungsgemäßen Betrieb des Sensors sicherstellt.

3. Verfahren nach Anspruch 2, wobei das zumindest ein Führungssignal durch ein erstes Führungssignal gebildet wird, das den Sensor zur Abgabe eines vorbestimmten Testsignals veranlasst.

4. Verfahren nach Anspruch 2 oder 3, wobei ein zweites Führungssignal vorgesehen ist, das der Signalverarbeitungseinrichtung zugeführt und zusammen mit dem Messsignal verarbeitet wird.

5. Verfahren nach Anspruch 4, wobei das erste und/oder zweite Führungssignal einen on-line übermittelten Rechenalgorithmus umfasst, mit dem das Messsignal verarbeitet wird.

6. Verfahren nach Anspruch 5, wobei das Ergebnis der Messsignalverarbeitung an den getrennten Sicherheitsbereich zurückgemeldet und dort wieder

zurückgewandelt wird, worauf das Messsignal ausgewertet und ein Steuerbefehl ermittelt wird, der dem Sensor zugeführt wird.

7. Verfahren nach einem der Ansprüche 2 bis 6, wobei das zumindest eine Führungssignal dem Sensor über eine Datenleitung, insbesondere Standleitung zugeführt wird.

8. Verfahren nach einem der Ansprüche 2 bis 6, wobei das Führungssignal per Funk übertragen wird.

9. Verfahren nach einem der Ansprüche 1 bis 8, wobei die getrennten Sicherheitsbereiche ein Trustcenter umfassen.

10. Verfahren nach einem der Ansprüche 2 bis 5, wobei das Führungssignal dem Sensor off-line zugeführt wird.

11. Verfahren nach Anspruch 10, wobei das Führungssignal mittels eines Datenträgers, insbesondere mittels einer Chip-Karte, zugeführt wird.

12. Verfahren nach einem der Ansprüche 2 bis 11, wobei das Führungssignal in vorbestimmten Intervallen verändert wird.

13. Verfahren nach einem der Ansprüche 1 bis 12, wobei dem Sensor ein drittes Führungssignal in vorbestimmten Intervallen zugeführt wird, das einen im Sensor vorgesehenen Selbstzerstörungsmechanismus blockiert.

14. Verfahren nach Anspruch 1, wobei das vom Sensor ermittelte Messsignal an eine räumlich getrennte Auswertestation in dem getrennten Sicherheitsbereich übertragen wird, in der räumlich getrennten Auswertestation die Signalverarbeitung nach dem vorgegebenen Algorithmus erfolgt und ein Steuerbefehl erzeugt wird, der nach Verschlüsselung der Sortiereinheit zugeführt wird.

15. Verfahren nach Anspruch 14, wobei dem Messsignal breitbandig Tarnsignale zugemischt werden, die bei der späteren Signalverarbeitung unberücksichtigt bleiben.

16. Verfahren nach einem der Ansprüche 1 bis 15, wobei die Auswertung mittels einer Zeitschaltung außerhalb überwachter Zeiten, insbesondere außerhalb der Dienstzeit der Sortiereinrichtung, ausgeschaltet wird.

17. Hochsicherheitssensor zur Durchführung des Verfahrens nach einem der Ansprüche 1 bis 16 mit einer Einrichtung zur Abgabe eines Testsignals, einer Leseeinrichtung zum Lesen der resultierenden Systemreaktion und zur Erzeugung eines Messsignals sowie mit einer Empfangseinrichtung zum Empfang

eines externen Führungssignals und mit einer Signalverarbeitungseinrichtung zum Verarbeiten des Messsignals zusammen mit dem Führungssignal nach einem vorgegebenen Algorithmus sowie mit einer Einrichtung zum Ausgeben eines Steuerbefehls zur Steuerung einer Sortiereinheit.

18. Hochsicherheitssensor nach Anspruch 17, wobei die Empfangseinrichtung zum Empfang des externen Führungssignals eine Lesestation für einen Datenträger, insbesondere für eine Chip-Karte, aufweist.

19. Hochsicherheitssensor zur Durchführung des Verfahrens nach einem der Ansprüche 14 bis 16, mit einer Einrichtung zur Abgabe eines Testsignals, einer Leseeinrichtung zum Lesen der resultierenden Systemreaktion und zur Erzeugung eines Messsignals sowie mit einer Einrichtung zur Übertragung des Messsignals an eine räumlich getrennte Signalverarbeitungseinrichtung in einem getrennten Sicherheitsbereich.

20. Hochsicherheitssensor nach Anspruch 19, wobei der Sensor eine Einrichtung zum Empfang eines Führungssignals umfasst, das einen vorbestimmten, ordnungsgemäßen Betrieb des Sensors sicherstellt.

21. Hochsicherheitssensor nach Anspruch 19 oder 20, wobei die Einrichtung zur Übertragung des Messsignals mit einer Einrichtung zur Erzeugung von Tarnsignalen ausgestattet ist, die dem Messsignal überlagerbar sind und bei der späteren Signalverarbeitung unberücksichtigt bleiben können.

Es folgen 2 Blatt Zeichnungen

Anhängende Zeichnungen

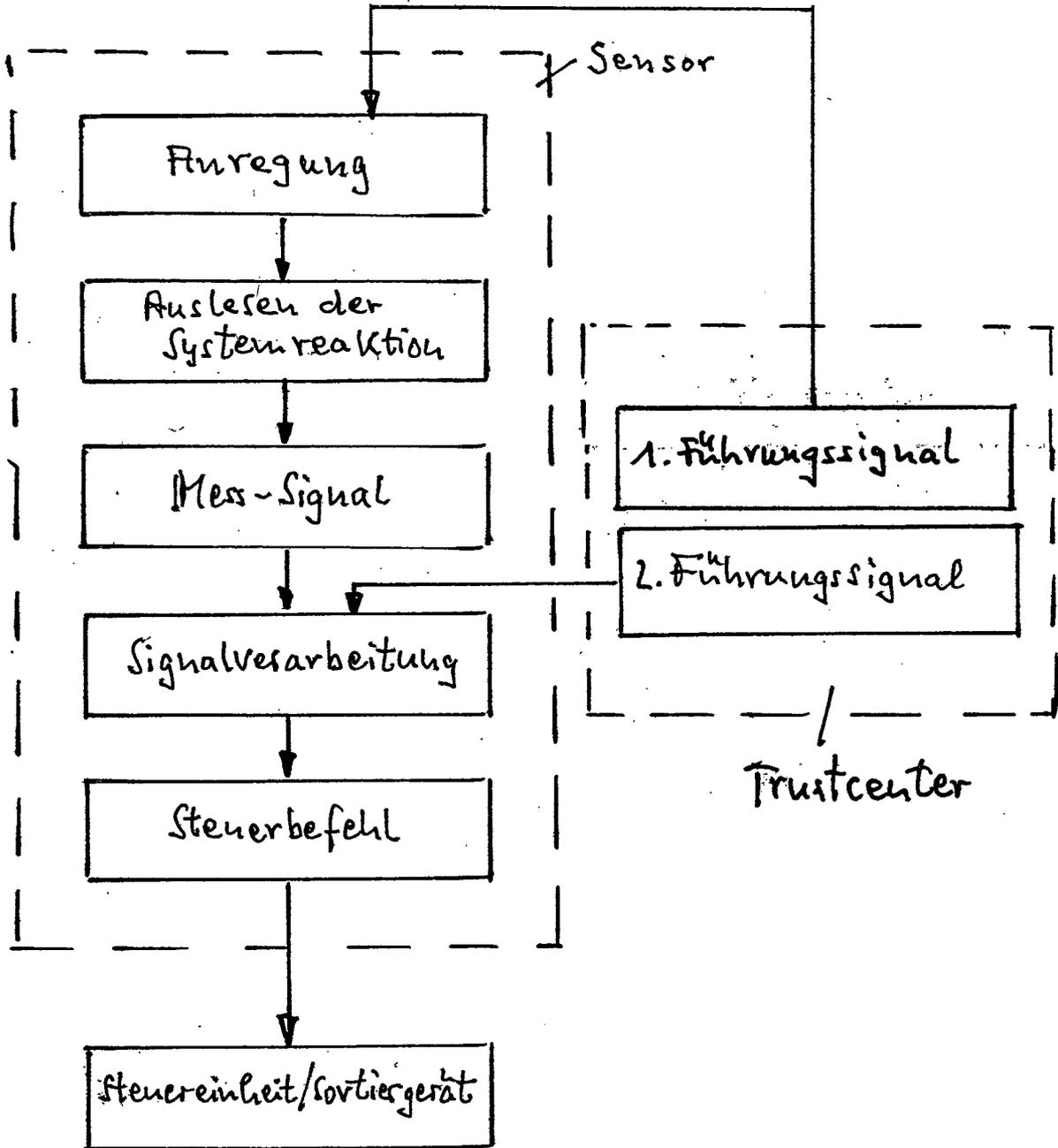


Fig. 1

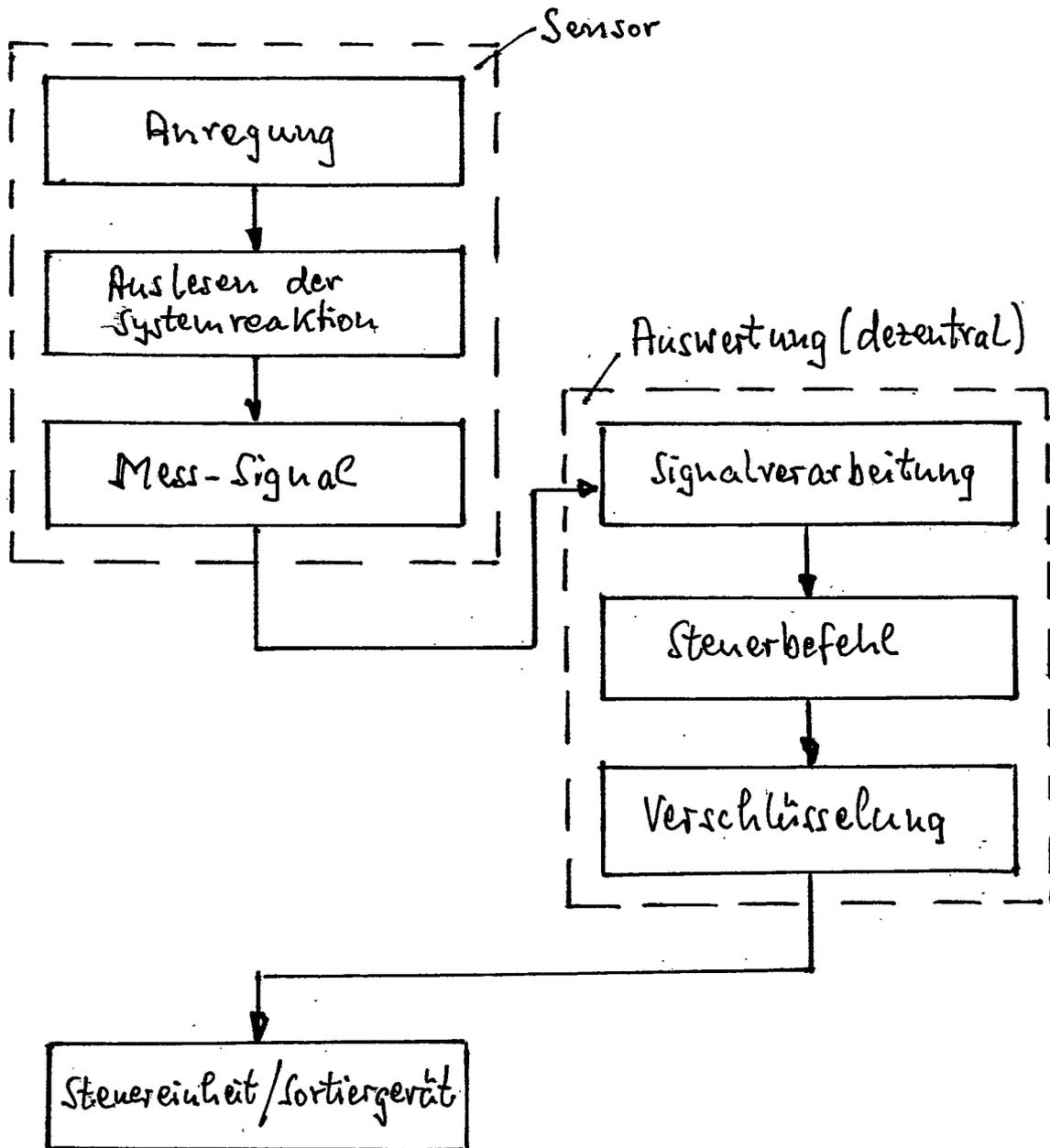


Fig. 2