(19) Deutsches Patent- und Markenamt

(10) **DE 10 2015 103 740 A1** 2016.09.15

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2015 103 740.8**
(22) Anmeldetag: **13.03.2015**
(43) Offenlegungstag: **15.09.2016**

(51) Int Cl.: ***G06F 21/54*** (2013.01)

(71) Anmelder:
Phoenix Contact GmbH & Co. KG, 32825 Blomberg, DE

(74) Vertreter:
Blumbach Zinngrebe, 64283 Darmstadt, DE

(72) Erfinder:
Salzmann, Rolf, 32657 Lemgo, DE; Frank, Tobias, Dr., 32657 Lemgo, DE

(56) Ermittelter Stand der Technik:

US 2014 / 0 283 107 A1
US 5 596 718 A

Prüfungsantrag gemäß § 44 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Verfahren und Vorrichtung zum Verarbeiten und Übertragen von Daten innerhalb eines funktional sicheren elektrischen, elektronischen oder programmierbar elektronischen Systems**

(57) Zusammenfassung: Die Erfindung betrifft das Verarbeiten und Übertragen von Daten innerhalb eines funktional sicheren elektrischen, elektronischen und/oder programmierbar elektronischen Systems, welches aus wenigstens zwei Sub-Systemen aufgebaut wird, welche jeweils wenigstens eine sichere Hardware- und/oder Software-Komponente umfassen und jeweils einem bestimmten Sicherheitslevel für eine funktional sichere Datenverarbeitung genügen. Vorgesehen ist das Verarbeiten von Daten mittels der sicheren Hardware- und/oder Software-Komponente eines ersten der Sub-Systeme zu funktional sicheren Daten eines ersten Sicherheitslevels und Hinzufügen zu diesen Daten durch dieses erste Sub-System wenigstens ein Kennzeichnungsattribut, welches die Eignung dieser Daten für den Einsatz dieses ersten Sicherheitslevels kennzeichnet; das Übertragen dieser Daten einschließlich des hinzugefügten Kennzeichnungsattributs von diesem ersten Sub-System an ein zweites dieser Sub-Systeme, und Empfangen dieser Daten einschließlich des hinzugefügten Kennzeichnungsattributs durch dieses zweite Sub-System; und das Prüfen des empfangenen Kennzeichnungsattributs durch das zweite Sub-System mittels dessen sicherer Hardware- und/oder Software-Komponente dahingehend, ob der Sicherheitslevel, den dieses Kennzeichnungsattribut kennzeichnet gegenüber dem Sicherheitslevel, welchem das zweite Sub-System genügt, gleich oder ungleich ist, und, wenn die Prüfung ungleiche Sicherheitslevel ergibt, das funktional sichere Weiterverarbeiten der Daten basierend auf dem geringeren Sicherheitslevel.

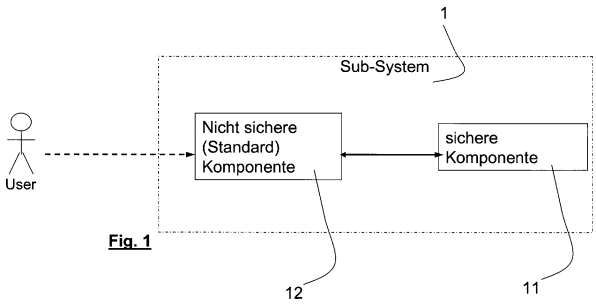

Fig. 1

Beschreibung

[0001] Die Erfindung betrifft Verfahren und Vorrichtungen zum Verarbeiten und Übertragen von Daten innerhalb eines funktional sicheren elektrischen, elektronischen und/oder programmierbar elektronischen Systems, welches aus wenigstens zwei Sub-Systemen aufgebaut wird.

[0002] Bekanntermaßen werden funktional sichere elektrische, elektronische und programmierbar elektronische Systeme in der internationalen Norm IEC 61508 bzw. in der im Wesentlichen inhaltsgleichen Europäischen Norm EN 61508 unter anderem auch hinsichtlich deren Entwicklung beschrieben. Die darin vorgegebenen Anforderungen an den Entwicklungsprozess von sicheren Systemen führen zu signifikant höherem Aufwand und benötigtem Entwicklungsbudget im Vergleich zur Entwicklung von Standardsystemen. Dabei nehmen die Anforderungen mit zunehmendem Sicherheitsintegritätslevel („SIL“; SIL1 bis SIL4) zu.

[0003] Auch der Einsatz von Komponenten, die nicht den Anforderungen der IEC 61508 für sichere Systeme genügen, ist normativ geregelt.

[0004] So ist z.B. im Teil 3 "Anforderungen an Software" der IEC 61508 in der Fassung von 2010 (IEC 61508-3:2010) unter dem Absatz 7.4.2.8 definiert:
"Wenn die Software sowohl Sicherheitsfunktionen als auch Nichtsicherheitsfunktionen umsetzt, muss die gesamte Software als sicherheitsbezogen behandelt werden, sofern nicht angemessene Maßnahmen sicherstellen, dass Versagen von Nichtsicherheitsfunktionen Sicherheitsfunktionen nicht nachteilig beeinflussen können",
sowie unter dem Absatz 7.4.2.9:
"Wenn die Software Sicherheitsfunktionen verschiedener Sicherheitsintegritätslevel umsetzt, muss die gesamte Software so behandelt werden, als ob sie zum höchsten Sicherheitsintegritätslevel gehört, sofern nicht ausreichende Unabhängigkeit zwischen den Sicherheitsfunktionen der verschiedenen Sicherheitsintegritätslevel im Entwurf gezeigt werden kann. Es muss dargelegt werden, dass entweder (1) die Unabhängigkeit sowohl im räumlichen und zeitlichen Bereich erreicht wird, oder (2) jede Verletzung der Unabhängigkeit beherrscht wird. Die Rechtfertigung für diese Unabhängigkeit muss dokumentiert werden."

[0005] Mit dem Begriff „Sicherheitsintegritätslevel“ (SIL; oder auch Sicherheitsanforderungsstufe) wird somit über den jeweiligen Level ein bestimmtes Maß für die notwendige bzw. erreichte Wirksamkeit von Sicherheitsfunktionen zur Risikominderung definiert. Wenn keine sicherheitsgerichteten (auch als sicherheitsbezogen oder sicherheitsrelevant im Rahmen der Erfindung bezeichnet) Anforderungen gelten, so ist die Entwicklung nach den normalen Standards des betrieblichen Qualitätsmanagements durchzuführen. Darüber hinaus stellt der Sicherheitsintegritätslevel SIL1 die geringsten Anforderungen. Je höher der Sicherheitsintegritätslevel, desto höher sind auch die Anforderungen an die Sicherheit.

[0006] Hierbei betrifft der Begriff „Sicherheit“ im Rahmen der Erfindung sowie in der Beschreibung und den Ansprüchen, soweit nicht anderes angegeben ist, die funktionale Sicherheit.

[0007] Die funktionale Sicherheit gemäß der Normreihe IEC 61508 umfasst hierbei ferner die Anwendung diverser Methoden zur Beherrschung von Fehlern, wie bspw. die Vermeidung systematischer Fehler in der Entwicklung, die Überwachung im laufenden Betrieb zur Erkennung von zufälligen Fehlern und/oder die sichere Beherrschung von erkannten Fehlern und der Übergang in einen vorher als sicher definierten Zustand. Alle diese Maßnahmen können Teil von bestimmten, vorher festgelegten Sicherheitsfunktionen sein. Allgemein kann gesagt werden, dass zwei- oder mehrkanalige Systeme, bei denen jeder Kanal für sich allein eine Sicherheitsfunktion auslösen kann, mit weniger technischem Aufwand eine höhere SIL erreichen können als solche, die nur einen Kanal besitzen. Als Kanal wird dabei der Informationsfluss durch eine Sicherheitskette (Safety-Loop) bezeichnet, angefangen z.B. von der Anforderung einer Sicherheitsfunktion (z. B. durch einen Sensor, Näherungsmelder, Lichtschranke oder Taster), endend mit dem Aktor bzw. Stellglied, welches den sicheren Zustand einer Maschine einleitet.

[0008] Nicht zu dieser funktionalen Sicherheit gehört demnach die elektrische Sicherheit.

[0009] Ist durch geeignete Maßnahmen somit gewährleistet, dass ein elektrisches, elektronisches und/oder programmierbar elektronisches System, aber auch eine einzelne Hardware- und/oder Software-Komponente eine bestimmte Sicherheitsfunktion wirksam erfüllt, gilt dieses System bzw. die jeweilige Komponente im Rahmen der nachfolgenden Beschreibung und der Ansprüche als sicher. Gelten für ein System, aber auch für eine einzelne Hardware- und/oder Software-Komponente keine sicherheitsgerichteten Anforderungen und ist somit für das System oder die einzelne Hardware- und/oder Software-Komponente nicht das Erfüllen einer bestimmten Sicherheitsfunktion durch geeignete Maßnahmen gewährleistet, gilt dieses System bzw. die jeweilige Komponente im Rahmen der nachfolgenden Beschreibung und der Ansprüche als nicht-sicher oder auch als Standard-System bzw. Standard-Komponente.

[0010] Aus der DE 10 2004 020 994 B4 ist ein Verfahren und eine Vorrichtung zum computergestütz-

ten Konstruieren einer sicherheitsgerichteten elektrischen Schaltung bekannt.

[0011] Dementsprechend werden eine Vielzahl von Schaltungskomponenten bereitgestellt, ausgewählt und verknüpft, wobei ferner eine Vielzahl von Regelsätzen bereitgestellt wird und jeder Regelsatz wiederum eine Vielzahl von sicherheitstechnischen Konstruktionsregeln beinhaltet, wobei zumindest einer der Regelsätze eine Konstruktionsregel beinhaltet, die mehrkanalig-redundante Ausgangssignale der Schaltungskomponenten und/oder einen Rückführkreis für jedes Ausgangssignal erfordert. Die elektrische Schaltung ist ferner in Teilbereiche unterteilt und für jeden der Teilbereiche wird vor dem Auswählen und Verknüpfen der Schaltungskomponenten ein Regelsatz festgelegt und der hierdurch definierte Regelsatz ausgewählt und es wird geprüft, ob die ausgewählten und verknüpften Schaltungskomponenten den Konstruktionsregeln dieses definierten Regelsatzes vollständig entsprechen, so dass jede nachfolgende Auswahl und/oder Verknüpfung von Schaltungskomponenten in Abhängigkeit von dem ausgewählten definierten Regelsatz freigegeben oder verhindert wird, wobei der definierte Regelsatz angezeigt wird.

[0012] Hierdurch soll das Konstruieren von sicherheitsgerichteten Schaltungen einfacher und schneller möglich sein, ohne dass die Fehlersicherheit der konstruierten Schaltung beeinträchtigt wird, wobei sich das Konstruieren hierbei auf das Konstruieren einer bestimmten Schaltung als Gesamtsystem bezieht. Denn zunächst werden einzelne Regelsätze, die jeweils eine Vielzahl von sicherheitstechnischen Konstruktionsregeln beinhalten, für diese Schaltung definiert und ausgewählt und anschließend die Schaltungskomponenten ausgewählt und verknüpft, die den Konstruktionsregeln der jeweiligen Regelsätze entsprechen.

[0013] Eine Aufgabe der vorliegenden Erfindung besteht darin, ein Verfahren und eine Vorrichtung auszubilden, mit welchen basierend auf sicheren Komponenten und gegebenenfalls auch auf Standard-Komponenten ein System aufgebaut und betrieben werden kann, derart dass die normativen Anforderungen an ein sicheres System erfüllt sind, und also das zu entwickelnde System eine Verletzung der Unabhängigkeit für dessen Beherrschung, insbesondere auch die Verletzung der Unabhängigkeit zwischen Standard und sicheren Sub-Systemen, sicher erkennen kann.

[0014] Die Aufgabe wird gemäß der Erfindung durch ein Verfahren und eine Vorrichtung gemäß den anhängigen unabhängigen Ansprüchen gelöst. Vorteilhafte und zweckmäßige Weiterbildungen sind Gegenstand der jeweiligen Unteransprüche.

[0015] Erfindungsgemäß ist somit ein Verfahren zum Verarbeiten und Übertragen von Daten innerhalb eines funktional sicheren elektrischen, elektronischen und/oder programmierbar elektronischen Systems vorgeschlagen, welches aus wenigstens zwei Sub-Systemen aufgebaut wird, welche jeweils wenigstens eine sichere Hardware- und/oder Software-Komponente umfassen und jeweils einem bestimmten Sicherheitslevels für eine funktional sichere Datenverarbeitung genügen. Das Verfahren sieht ferner vor, dass die Daten mittels der sicheren Hardware- und/oder Software-Komponente eines ersten der Sub-Systeme zu funktional sicheren Daten eines ersten Sicherheitslevels verarbeitet werden und durch dieses erste Sub-System wenigstens ein Kennzeichnungsattribut zu diesen Daten hinzugefügt wird, welches die Eignung dieser Daten für den Einsatz dieses ersten Sicherheitslevels kennzeichnet. Diese Daten einschließlich des hinzugefügten Kennzeichnungsattributs werden dann von diesem ersten Sub-System an ein zweites dieser Sub-Systeme übertragen und durch dieses zweite Sub-System folglich empfangen.

[0016] Das empfangene Kennzeichnungsattribut wird anschließend durch das zweite Sub-System mittels dessen sicherer Hardware- und/oder Software-Komponente dahingehend geprüft, ob der Sicherheitslevel, den dieses Kennzeichnungsattribut kennzeichnet, gegenüber dem Sicherheitslevel, welchem das zweite Sub-System genügt, gleich oder ungleich ist. Wenn die Prüfung ungleiche Sicherheitslevel ergibt, werden die Daten anschließend basierend auf dem geringeren Sicherheitslevel funktional sicher weiterverarbeitet.

[0017] Ein wesentlicher Vorteil hierbei ist, dass jedes Sub-System und folglich im Wesentlichen jedes Bauteil oder Gerät einem eigenen, auch jeweils unterschiedlichem Sicherheitslevel genügen kann und dennoch aus diesen Sub-Systemen wiederum ein System zusammensetzbar ist, welches auch in dessen Gesamtheit wiederum einem Sicherheitslevel genügt. Da hierbei das aus verschiedenen Sub-Systemen aufgebaute System unterschiedliche Sicherheitslevel erkennt und eine Weiterverarbeitung von Daten stets auf dem geringeren von zwei unterschiedlichen Sicherheitsleveln durchgeführt wird, können durch die Erfindung die Anforderung an ein funktional sicheres Systems erfüllt werden, obgleich dieses Baukasten-artig aus Sub-Systemen unterschiedlicher Sicherheitslevel aufgebaut ist.

[0018] Zur Durchführung des Verfahrens schlägt die Erfindung ferner eine Vorrichtung vor, die eine sichere Hardware- und/oder Software-Komponente umfasst, die einem bestimmten Sicherheitslevels für eine funktional sichere Datenverarbeitung genügt.

[0019] Die sichere Hardware- und/oder Software-Komponente ist hierbei dazu eingerichtet, Daten zu funktional sicheren Daten eines bestimmten Sicherheitslevels zu verarbeiten und diesen Daten anschließend ein Kennzeichnungsattribut hinzu zu fügen, welches die Eignung dieser Daten für den Einsatz dieses bestimmten Sicherheitslevels kennzeichnet.

[0020] Ergänzend oder alternativ ist die sichere Hardware- und/oder Software-Komponente dazu eingerichtet, nach Erhalt von Daten, welche zu funktional sicheren Daten eines bestimmten Sicherheitslevels verarbeit sind und denen ein Kennzeichnungsattribut hinzugefügt ist, welches die Eignung dieser Daten für den Einsatz dieses bestimmten Sicherheitslevels kennzeichnet, das diesen Daten hinzugefügte Kennzeichnungsattribut dahingehend zu prüfen, ob der Sicherheitslevel, den dieses Kennzeichnungsattribut kennzeichnet gegenüber dem Sicherheitslevel, welchem die Hardware- und/oder Software-Komponente genügt, gleich oder ungleich ist, und, wenn die Prüfung ungleiche Sicherheitslevel ergibt, eine Weiterverarbeitung der Daten auf dem geringeren Sicherheitslevel basierend durchzuführen

[0021] Die vorstehend genannten und weiteren Merkmale der Erfindung werden anhand der nachfolgenden Beschreibung von Ausführungsbeispielen unter Bezugnahme auf die beigefügte Zeichnung näher erläutert und/oder ersichtlich, wobei es sich versteht, dass diese Merkmale nicht nur in der jeweils beschriebenen Kombination sondern auch in anderen Kombinationen oder in Alleinstellung verwendbar sind ohne den Rahmen der Erfindung zu verlassen.

[0022] In den in Bezug genommenen Zeichnungen zeigen:

[0023] Fig. 1 eine stark vereinfachte Prinzipskizze eines Ausführungsbeispiels eines Sub-Systems mit wenigstens einer sicheren Hardware- und/oder Software-Komponente,

[0024] Fig. 2 eine stark vereinfachte Prinzipskizze eines Ausführungsbeispiels eines aus Sub-Systemen aufgebauten Systems, wobei das System gemäß Ausführungsbeispiel aus zwei, jeweils wenigstens eine sichere Hardware- und/oder Software-Komponente umfassenden Sub-Systeme aufgebaut ist, und

[0025] Fig. 3 eine stark vereinfachte Prinzipskizze einer Verarbeitung und Übertragung von Daten innerhalb eines Systems, welches beispielhaft aus drei Sub-Systemen mit jeweils wenigstens einer sicheren Hardware- und/oder Software-Komponente aufgebaut wird oder ist.

[0026] Fig. 1 zeigt eine stark vereinfachte Prinzipskizze eines Ausführungsbeispiels eines Sub-Systems **1** mit wenigstens einer sicheren Hardware- und/oder Software-Komponente **11**, wobei die sichere Hardware- und/oder Software-Komponente **11** einem bestimmten Sicherheitslevel für eine funktional sichere Datenverarbeitung genügt. Eine solche sichere Komponente wird in der nachfolgenden Beschreibung und auch in den Zeichnungen auch als „Safety Context“ bezeichnet.

[0027] Die sichere Hardware- und/oder Software-Komponente **11** ist Teil einer in den Zeichnungen nicht weiter dargestellten Vorrichtung, insbesondere einer elektrischen, elektronischen und/oder programmierbar elektronischen Vorrichtung eines elektrischen, elektronischen und/oder programmierbar elektronischen Systems, welches aus wenigstens zwei Sub-Systemen aufgebaut wird oder ist, welche jeweils wenigstens eine sichere Hardware- und/oder Software-Komponente umfassen und jeweils einem bestimmten Sicherheitslevel für eine funktional sichere Datenverarbeitung genügen. Ein elektrisches, elektronisches und/oder programmierbar elektronisches Systems, welches aus wenigstens zwei Sub-Systemen aufgebaut ist, ist der stark vereinfachten Prinzipskizze eines Ausführungsbeispiels eines aus zwei Sub-Systemen **2** und **3** aufgebauten Systems gemäß **Fig.** 2 zu entnehmen, die jeweils wenigstens eine sichere Hardware- und/oder Software-Komponente **21a** bis **21c** bzw. **31a** und **31b** umfassen.

[0028] Gemäß einer Ausführungsform ist die sichere Hardware- und/oder Software-Komponente, z.B. die sichere Hardware- und/oder Software-Komponente **11**, dazu eingerichtet, Daten zu funktional sicheren Daten eines bestimmten Sicherheitslevels zu verarbeiten und diesen Daten anschließend ein Kennzeichnungsattribut hinzu zu fügen, welches die Eignung dieser Daten für den Einsatz dieses bestimmten Sicherheitslevels kennzeichnet. Eine solche sichere Komponente produziert folglich funktional sichere Daten. Eine Vorrichtung oder ein Sub-System mit einer oder einer Mehrzahl von solchen sicheren Komponenten, die funktional sichere Daten produzieren, wird nachfolgend auch als „Safety Server“ bezeichnet.

[0029] Gemäß einer weiteren Ausführungsform kann die sichere Hardware- und/oder Software-Komponente, z.B. die sichere Hardware- und/oder Software-Komponente **11**, jedoch auch dazu eingerichtet sein, nach Erhalt von Daten, welche zu funktional sicheren Daten eines bestimmten Sicherheitslevels verarbeitet sind und denen ein Kennzeichnungsattribut hinzugefügt ist, welches die Eignung dieser Daten für den Einsatz dieses bestimmten Sicherheitslevels kennzeichnet, das diesen Daten hinzugefügte Kennzeichnungsattribut dahingehend zu prüfen, ob der Sicherheitslevel, den dieses Kennzeichnungsattribut kennzeichnet gegenüber dem Sicherheitslevel, welchem die Hardware- und/oder Software-Komponente genügt, gleich oder ungleich ist, und, wenn

die Prüfung ungleiche Sicherheitslevel ergibt, eine Weiterverarbeitung der Daten auf dem geringeren Sicherheitslevel basierend durchzuführen. Eine solche sichere Komponente konsumiert folglich zunächst funktional sichere Daten und wertet diese hierbei aus. Eine Vorrichtung oder ein Sub-System mit einer oder einer Mehrzahl von solchen sicheren Komponenten, die funktional sichere Daten konsumieren, wird nachfolgend auch als „Safety Client“ bezeichnet.

[0030] Im Rahmen der Erfindung kann eine sichere Komponente, wie z.B. die mit „Safety-Context B“ bezeichnete sichere Komponente innerhalb eines Sub-Systems **5** der **Fig.** 3, auch zunächst funktional sichere Daten konsumieren und hierbei auswerten und anschließend wiederum funktional sichere Daten produzieren. Eine Vorrichtung oder ein Sub-System mit einer oder einer Mehrzahl von sicheren Komponenten sowohl zum Auswerten von funktional sicheren Daten als auch zum Verändern oder erneutem Produzieren von funktional sicheren Daten, kann demnach, wie beispielsweise das Sub-System **5** der **Fig.** 3, sowohl die Rolle als Safety Server und als Safety Client annehmen.

[0031] Auch das Sub-System **1** der **Fig.** 1 ist somit im Rahmen der Erfindung zweckmäßig ferner Teil eines in **Fig.** 1 nicht weiter dargestellten übergeordneten Systems. Das Sub-System kann ferner zusätzlich zu der wenigstens einen sicheren Hardware- und/oder Software-Komponente **11** auch aus wenigstens einer nicht-sicheren Hardware- und/oder Software-Komponente **12** aufgebaut sein. Das Sub-System **1** kann beispielsweise ein Programmiersystem sein, mittels welchem ein Benutzer „user“, insbesondere ein Programmierer, ein sicheres Steuerungsprogramm mittels dazu geeigneter Software-komponenten erstellt. In einem solchen Fall, d.h., wenn ein Sub-System, wie z.B. das Sub-system **1** zusätzlich zu der wenigstens einen sicheren Hardware- und/oder Software-Komponente **11** auch aus wenigstens einer nicht-sicheren Hardware- und/oder Software-Komponente **12** aufgebaut ist, wird eine Verarbeitung von Daten durch die nicht-sichere Hardware- und/oder Software-Komponente **12** von der sicheren Hardware- und/oder Software-Komponente **11** des Sub-Systems dahingehend überwacht, dass die Daten während der Verarbeitung nicht korrumpiert werden, wie nachfolgend noch näher beschrieben wird. Durch die Überwachung der Standard Komponenten durch die sicheren Komponenten ergibt sich folglich wiederum ein funktional sicheres Sub-System.

[0032] Im Rahmen der Erfindung werden nunmehr innerhalb eines aus wenigstens zwei funktional sicheren Sub-Systemen aufgebauten Systems Daten mittels sicherer Hardware- und/oder Software-Komponente eines ersten Subsystems zunächst zu funktional sicheren Daten eines ersten Sicherheitslevels verarbeitet. Anschließend fügt das erste Sub-System diesen Daten noch wenigstens ein Kennzeichnungsattribut hinzu, welches die Eignung dieser Daten für den Einsatz dieses ersten Sicherheitslevels kennzeichnet.

[0033] Werden anschließend diese Daten einschließlich des hinzugefügten Kennzeichnungsattributs von diesem ersten Sub-System an ein zweites dieser Sub-Systeme übertragen und von diesem einschließlich des hinzugefügten Kennzeichnungsattributs empfangen, prüft das zweite Sub-System das empfangene Kennzeichnungsattribut mittels dessen sicherer Hardware- und/oder Software-Komponente dahingehend, ob der Sicherheitslevel, den dieses Kennzeichnungsattribut kennzeichnet gegenüber dem Sicherheitslevel, welchem das zweite Sub-System genügt, gleich oder ungleich ist. Ergibt die Prüfung ungleiche Sicherheitslevel, erfolgt ein funktional sicheres Weiterverarbeiten der Daten durch das zweite Sub-System in jedem Fall basierend auf dem geringeren Sicherheitslevel.

[0034] Wie vorstehend bereits erwähnt, ist ein solches funktional sicheres elektrisches, elektronisches und/oder programmierbar elektronisches System, welches aus wenigstens zwei Sub-Systemen aufgebaut wird oder ist, welche jeweils wenigstens eine sichere Hardware- und/oder Software-Komponente umfassen und jeweils einem bestimmten Sicherheitslevel für eine funktional sichere Datenverarbeitung genügen, beispielhaft der **Fig.** 2 zu entnehmen. Ein erstes Sub-System **2** stellt hier z.B. eine Benutzeroberfläche bereit, auf welches ein Benutzer „user“ zugreifen kann, um ein Steuerungsprogram zu generieren, welches anschließend an ein zweites Sub-System **3** übertragen werden soll. Die sicheren Hardware- und/oder Software-Komponenten **21a**, **21b**, **21c** des ersten Sub-Systems **2** können somit z.B. eine sichere Programeditor-Komponente **21a**, eine sichere Datenliste-Komponente **21b** und/oder z.B. eine sichere Netzwerk-Konfigurationskomponente **21c** beinhalten.

[0035] Das Sub-System kann hierbei nur derartige sichere Komponenten beinhalten oder aber, wie bei der Ausführungsform nach **Fig.** 2 zusätzlich aus nicht-sicheren Hardware- und/oder Software-Komponente **22a**, **22b** und/oder **22c**, wie z.B. einer nicht-sicheren Programeditor-Komponente **22a**, einer nicht-sicheren Datenliste-Komponente **22b** und/oder z.B. einer nicht-sicheren Netzwerk-Konfigurationskomponente **22c** aufgebaut sein.

[0036] Ein zweites Sub-System **3** stellt hier dann z.B. eine Compilerumgebung bereit, an welches das mittels des Sub-Systems **2** generierte Steuerprogramm übertragen wird. Die sicheren Hardware- und/oder Software-Komponenten **31a** und **31b** des zweiten Sub-Systems **3** können somit z.B. sichere Komponenten unterschiedlicher Compiler beinhalten. Das

Sub-System **3** kann zusätzlich z.B. auch aus einer nicht-sicheren Hardware- und/oder Software-Komponente **32a** aufgebaut sein, die z.B. eine nicht-sichere Compiler-Infrastruktur mit abstraktem Syntaxbaum beinhaltet.

[0037] Auch beim System gemäß **Fig.** 2 werden somit Produzenten von funktional sichereren Daten von Konsumenten von funktional sicheren Daten unterschieden.

[0038] Das Sub-System **2** stellt in diesem Beispiel demnach einen Produzenten oder „Safety Server" und das Sub-System **3** einen Konsumenten oder „Safety Client" dar, wobei im Beispiel gemäß **Fig.** 2 sowohl der „Safety Server" (das Sub-System **2**) als auch der „Safety Client" (das Sub-System **3**) gemischt aus Standard Komponenten und sicheren Komponenten bestehen. Wie vorstehend aufgezeigt, überwacht der Safety Server in einem solchen Fall die Daten, welche mithilfe von Standard Komponenten entstehen. Zweckmäßig überwacht auch der Safety Client in einem solchen Fall die Daten, welche mithilfe von Standard Komponenten ausgewertet werden. Eine solche Überwachung durch den Safety Server und den Safety Client ist bei **Fig.** 2 durch die jeweiligen Doppelpfeile zwischen den Standard Komponenten und sicheren Komponenten angedeutet.

[0039] Dabei wird sichergestellt, dass die Daten durch die Standard Komponenten nicht korrumpiert werden. Diese Überwachung findet zweckmäßig während und außerhalb von Datenänderungen statt. Bevorzugt werden hierzu vor der Verarbeitung von Daten durch eine nicht-sichere Hardware- und/oder Software-Komponente, Daten, welche nicht geändert werden sollen, von den übrigen Daten separiert und separat gesichert und/oder separat mit einer Prüfsumme belegt. Die Daten werden somit zweckmäßig segmentiert und also in Daten aufgeteilt, welche geändert werden sollen und in Daten, welche nicht geändert werden sollen. Die Daten welche geändert werden, sei es durch Löschen, Hinzufügen oder Modifizieren von Daten sind für die Änderung freigegeben. Die Daten welche nicht geändert werden dürfen, werden während der Änderung der zu ändernden Daten bevorzugt im RAM und/oder auf einer sonderten Festplatte mittels entsprechenden Verfahren wie z.B. Prüfsummen einschl. Hash-Werte gesichert. Dabei ist zweckmäßig zu beachten, den Bereich der geschützten Daten, das also sind die Daten, welche nicht geändert werden, möglichst groß zu gestalten.

[0040] Die korrekte Funktionalität der Datenüberwachung kann mittels geeigneter, auch an und für sich bekannter Methoden wie einer logischen Programmablaufüberwachung sichergestellt werden. Wenn, dann berechnet folglich nur eine sichere Komponente bzw. der Safety Context eines Safety Servers eine Prüfsumme und weitere Attribute, die die Datenkonsistenz und Datenintegrität belegt. Damit werden sowohl Datenänderungen außerhalb der sicheren Komponente bzw. des Safety Contexts als auch eine Fehlfunktion des Safety Servers sicher erkannt.

[0041] Abgesehen von der Prüfsumme zum Nachweis der Datenkonsistenz und Integrität generiert der Safety Context des Safety Servers, wie z.B. beim Safety Context **21a** der **Fig.** 2 angedeutet, in jedem Fall für die vom ihm kommende Daten ein vorerwähntes Kennzeichnungsattribut **101** und qualifiziert dann diese Daten mit dem Kennzeichnungsattribut **101**, so dass die vom Safety Server (z.B. Sub-System **2** der **Fig.** 2) letztendlich an den Safety Client (z.B. Sub-System **3** der **Fig.** 2) zu übertragenen Daten **100** auch das Kennzeichnungsattribut **101** enthalten.

[0042] Ein solches Kennzeichnungsattribut **101**, welches die Eignung von Daten für den Einsatz eines bestimmten Sicherheitslevels kennzeichnet, identifiziert somit insbesondere auch die systematische Eignung des Safety Servers. Beispiele dieser Kennzeichnungsattribute sind ein maximal erreichbarer SIL (Sicherheitsintegritäts-Level), ein maximal erreichbarer PL (Performance Level) und/oder der Einsatz eines vordefinierten Sprachumfangs, bspw. gemäß LVL (Limited Variability Languages), oder FVL (Full Variability Language), welches hierdurch hinsichtlich einer nachfolgenden Weiterverarbeitung definiert ist.

[0043] Alle vorgenannten Prüfsummen und (erweiterten) Attribute, welche zur Datenqualifizierung eingesetzt werden, werden dann im weiteren Verlauf von einem die Daten empfangenen Safety Client (z.B. Sub-System **3** der **Fig.** 2) ausgewertet. Wie vorstehend aufgezeigt, sind auch Safety Clients häufig zusammengesetzte Sub-Systeme, welche somit nicht nur aus sicheren Komponenten bestehen sondern auch aus Standard Komponenten bestehen, jedoch funktional sicher qualifizierte Daten insbesondere auch mittels der sicheren Komponenten sicherheitsgerichtet auswerten. Dazu verifiziert der Safety Client zweckmäßig sowohl eine gegebenenfalls mit den empfangenen Daten mit empfangene Prüfsumme zum Nachweis der Datenkonsistenz und Datenintegrität sowie die Kennzeichnungsattribute, welche die systematische Eignung der funktional sicheren Daten beschreiben. Stellt der Safety Client einen Verstoß der Dateninkonsistenz oder Datenintegrität fest oder die systematische Eignung der Daten ist inkompatibel zu der systematischen Eignung des Safety Clients, so werden die Daten vom Safety Client in zweckmäßiger Ausführung nicht funktional sicher verarbeitet. Eine Verarbeitung unter diesen Umstand kann somit nur unter dem Verlust eines Sicherheitsintegritäts-Levels erfolgen. Mit anderen Worten, werden die empfangenen Daten durch dieses zweite Sub-System mittels dessen sicherer Hardware- und/

oder Software-Komponente hinsichtlich Datenunverfälschtheit ausgewertet und in zweckmäßiger Ausführung nur dann funktional sicher weiterverarbeitet, sofern auf der Auswertung basierend auf die Unverfälschtheit der Daten erkannt wird. In zweckmäßiger Ausführung jedoch werden bei der Kombination von Sub-Systemen mit unterschiedlicher systematischer Eignung, Kennzeichnungsattribute immer an den geringeren Sicherheitslevel angepasst, also z.B. auf den Wert des geringeren Sicherheitsintegritäts-Levels gesetzt. Folglich wird nach der Übertragung von Daten zwischen zwei Sub-Systemen das den Daten hinzugefügte Kennungsattribut durch das empfangene Sub-System bevorzugt immer auf ein Kennungsattribut gesetzt, welches den geringsten Sicherheitslevel kennzeichnet, und zwar aus der Gruppe der Sicherheitslevel, welchen die bei dieser Übertragung beteiligten Sub-Systeme genügen und für welchen die übertragenen Daten bei dieser Übertragung als geeignet gekennzeichnet sind.

[0044] Werden die funktional sicheren Daten weder geändert noch sicherheitsgerichtet weiterverarbeitet, so können im Sinne eines schwarzen Kanals ferner grundsätzlich beliebig viele Standard Komponenten für den Weitertransport der Daten bzw. deren Speicherung beteiligt sein.

[0045] Der vorstehend beschriebene Systemaufbau bzw. das damit umgesetzte Verfahren kann in äußerst zweckmäßiger Weise Anwendung in der gesamten Prozesskette vom Programmiersystem bis hin zum sicheren Steuerungssystem finden.

[0046] Basierend auf der **Fig.** 3 wird nachfolgend nochmals ein weiteres bevorzugtes Ausführungsbeispiel beschrieben.

[0047] Es wird hierbei angenommen, dass ein Maschinenhersteller zur Risikominderung einer Maschine eine Schutzeinrichtung einsetzt, welche z.B. einen Not-Halt und eine berührungslos wirkende Schutzeinrichtung (BWS) besitzt. Dies ist in der Regel ein Not-Aus-Schalter, der dazu dient, die Maschine im Gefahrenfall oder zur Abwendung einer Gefahr schnell in einen sicheren Zustand zu versetzen sowie als BWS z.B. ein Lichtvorhang, ein Induktiver Näherungsschalter oder ein kapazitativer Abstandssensor.

[0048] Nur wenn beide Schutzeinrichtungen den sicheren Zustand melden darf ein Antrieb aktiviert werden. Diese Schutzeinrichtung wird von einer sicheren Steuerung überwacht, die mit einem Programmiersystem programmiert wird. Dazu erstellt ein Programmierer ein sicheres Steuerungsprogramm mittels einer dazu geeigneten Software. Diese Software besteht sowohl ans Standard als auch sicheren Komponenten. Durch die Überwachung der Standard Komponenten durch die sicheren Komponenten ergibt sich ein funktional sicheres System. Der Programmierer kann somit das System für den Einsatz in der Sicherheitstechnik verwenden. Exemplarisch und vereinfacht setzt sich das System wie folgt zusammen.

[0049] Das sichere Steuerungsprogramm wird mittels eines Programmeditors entwickelt. Dieser Programmeditor ist bei **Fig.** 3 durch das Sub-System **4** angezeigt. Der Programmeditor besteht aus Standard Softwarekomponenten, bei **Fig.** 3 mit „Std. Komp. A“ des Sub-Systems **4** angezeigt. Diese ermöglichen die Eingabe und Anzeige des Steuerungsprogramms. Weiterhin besteht der Programmeditor im Kontext der Sicherheitstechnik aus sicheren Softwarekomponenten, bei **Fig.** 3 mit „Safety Context A“ des Sub-Systems **4** angezeigt. Die sicheren Softwarekomponenten Überwachen die korrekte Funktionsweise des Programmeditors und stellen die Integrität der Daten des Steuerungsprogramm sicher. Die sicheren Softwarekomponenten qualifizieren die Daten des sicheren Anwendungsprogramms, d.h. im vorliegenden Beispiel des Steuerungsprogrammes mit den vorstehend beschriebenen sicherheitstechnischen Kennzeichnungsattributen sowie in zweckmäßiger Weise den Prüfsummen und (erweiterten) Attributen. Der Programmeditor und also das Sub-System der **Fig.** 3 stellen somit einen Safety Server dar.

[0050] Die Daten des Steuerungsprogrammes werden an mindestens einen Compiler übergeben, um aus den Programmquellen ausführbaren Maschinencode für die Sicherheitssteuerung zu erzeugen. Dieser mindestens einen Compiler ist bei **Fig.** 3 durch das Sub-System **5** angezeigt. Die Übergabe kann auch über eine Zwischenspeicherung auf Festplatte oder anderen nicht flüchtigen Speichermedien erfolgen. Dabei verifiziert der mindestens eine Compiler die Datenintegrität sowie die Systematische Eignung der Daten, welche durch die sicherheitstechnischen Attribute, d.h. durch die vorstehend beschriebenen sicherheitstechnischen Kennzeichnungsattribute und in zweckmäßiger Weise die Prüfsummen und (erweiterten) Attributen, definiert sind. Ist die Integrität verletzt bzw. entsprechen die Daten nicht der geforderten systematischen Eignung, so wird die Weiterverarbeitung nicht funktional sicher weitergeführt. In diesem Verfahrensschritt agiert der mindestens eine Compiler folglich als Safety Client (vgl. Sub-System **5** der **Fig.** 3).

[0051] Verarbeitet der mindestens eine Compiler die Programmquellen zu ausführbaren Maschinencode so wird zweckmäßig eine Prüfsumme zur Datenintegrität auf dem Maschinencode berechnet. Weiterhin wird der Maschinencode mit den sicherheitstechnischen Kennzeichnungsattributen versehen. Diese können identisch mit denen der Programmquellen sein, bzw. können ergänzt oder reduziert werden. Das heißt, in der praktischen Umsetzung der Erfindung können die Kennzeichnungsattribute nach einer

Verarbeitung von Daten kein höheres Sicherheitsniveau ausweisen als die Kennzeichnungsattribute der Quelldaten. In diesem Verfahrensschritt dient der mindestens eine Compiler somit als Safety Server (vgl. Sub-System **5** der **Fig.** 3).

[0052] Über eine Kommunikationsbeziehung zwischen sicherer Programmiersoftware und der sicheren Steuerung werden der Maschinencode und die dazugehörigen sicherheitsrelevanten Daten auf die sichere Steuerung übertragen. Im Sinne dieser Erfindung kann für diese Art der Kommunikation auch ein vorstehend als schwarzer Kanal eingesetzt werden, der dann weder die Rolle als Safety Client oder Safety Server einnimmt, da die Daten durch den Transport nicht verändert werden.

[0053] Die sichere Steuerung ist bei **Fig.** 3 durch das Sub-System **6** angezeigt.

[0054] Die sichere Steuerung nimmt den Maschinencode entgegen und verifiziert Datenintegrität sowie die systematische Eignung des Maschinencodes. Ist die Prüfung erfolgreich, so bringt die Sicherheitssteuerung den Maschinencode zur Ausführung. In dieser Erfindung ist die Sicherheitssteuerung somit wiederum ein Safety Client.

[0055] Da somit ein erfindungsgemäß aus verschiedenen Sub-Systemen aufgebautes System unterschiedliche Sicherheitslevel erkennt und eine Weiterverarbeitung von Daten stets auf dem geringeren von zwei unterschiedlichen Sicherheitsleveln durchführt, können die Anforderung an ein funktional sicheres Systems stets erfüllt werden. Bevorzugt wird hierbei jedoch, sofern die Verarbeitung von Daten durch die sichere Hardware- und/oder Software-Komponente eines Sub-Systems basierend auf einem Sicherheitslevel erfolgt ist, welcher geringer ist, als der Sicherheitslevel, dem dieses Sub-System genügt, dieses von diesem Sub-System dem in der Datenverarbeitungskette eines Systems nachfolgenden Sub-System und/oder einem Benutzer angezeigt.

Bezugszeichenliste

1	Sub-System,
11	sichere Hardware- und/oder Software-Komponente,
12	nicht sichere (Standard-) Komponente;
2	Sub-System,
21a, 21b, 21c	sichere Hardware- und/oder Software-Komponenten,
22a, 22b, 22c	nicht sichere (Standard-) Komponenten;
3	Sub-System,
31a, 31b	sichere Hardware- und/oder Software-Komponenten,
32a, 22b, 22c	nicht sichere (Standard-) Komponenten;
4	Sub-System;
5	Sub-System;
6	Sub-System;
100	Daten;
101	Kennzeichnungsattribut;

ZITATE ENTHALTEN IN DER BESCHREIBUNG

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

Zitierte Patentliteratur

- DE 102004020994 B4 [0010]

Zitierte Nicht-Patentliteratur

- Norm IEC 61508 [0002]
- Europäischen Norm EN 61508 [0002]
- IEC 61508 [0003]
- IEC 61508 [0004]
- IEC 61508-3:2010 [0004]
- IEC 61508 [0007]

Patentansprüche

1. Verfahren zum Verarbeiten und Übertragen von Daten innerhalb eines funktional sicheren elektrischen, elektronischen und/oder programmierbar elektronischen Systems, welches aus wenigstens zwei Sub-Systemen aufgebaut wird, welche jeweils wenigstens eine sichere Hardware- und/oder Software-Komponente umfassen und jeweils einem bestimmten Sicherheitslevel für eine funktional sichere Datenverarbeitung genügen, mit folgenden Schritten:
Verarbeiten von Daten mittels der sicheren Hardware- und/oder Software-Komponente eines ersten der Sub-Systeme zu funktional sicheren Daten eines ersten Sicherheitslevels und Hinzufügen zu diesen Daten durch dieses erste Sub-System wenigstens ein Kennzeichnungsattribut, welches die Eignung dieser Daten für den Einsatz dieses ersten Sicherheitslevels kennzeichnet; und
Übertragen dieser Daten einschließlich des hinzugefügten Kennzeichnungsattributs von diesem ersten Sub-System an ein zweites dieser Sub-Systeme, und
Empfangen dieser Daten einschließlich des hinzugefügten Kennzeichnungsattributs durch dieses zweite Sub-System; und
Prüfen des empfangenen Kennzeichnungsattributs durch das zweite Sub-System mittels dessen sicherer Hardware- und/oder Software-Komponente dahingehend, ob der Sicherheitslevel, den dieses Kennzeichnungsattribut kennzeichnet gegenüber dem Sicherheitslevel, welchem das zweite Sub-System genügt, gleich oder ungleich ist, und, wenn die Prüfung ungleiche Sicherheitslevel ergibt funktional sicheres Weiterverarbeiten der Daten basierend auf dem geringeren Sicherheitslevel.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet,** dass die empfangenen Daten durch dieses zweite Sub-System mittels dessen sicherer Hardware- und/oder Software-Komponente hinsichtlich Datenunverfälschtheit ausgewertet werden und nur funktional sicher weiterverarbeitet werden, sofern auf der Auswertung basierend auf die Unverfälschtheit der Daten erkannt wird.

3. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet,** dass die Verarbeitung von Daten durch die sichere Hardware- und/oder Software-Komponente eines Sub-Systems basierend auf einem Sicherheitslevel, welcher geringer ist, als der Sicherheitslevel, dem dieses Sub-System genügt, dem in einer Datenverarbeitungskette nachfolgenden Sub-System und/oder einem Benutzer angezeigt wird.

4. Verfahren nach einem der vorstehenden Ansprüche, **dadurch gekennzeichnet,** dass die wenigstens zwei Sub-Systeme auch aus jeweils wenigstens einer nicht-sicheren Hardware- und/oder Software-Komponente aufgebaut werden.

5. Verfahren nach vorstehendem Anspruch, **dadurch gekennzeichnet,** dass die Verarbeitung von Daten durch die nicht-sichere Hardware- und/oder Software-Komponente eines Sub-Systems von der sicheren Hardware- und/oder Software-Komponente dieses Sub-Systems dahingehend überwacht wird, dass die Daten während der Verarbeitung nicht korrumpiert werden.

6. Verfahren nach vorstehendem Anspruch, **dadurch gekennzeichnet,** dass vor der Verarbeitung von Daten durch die nicht-sichere Hardware- und/oder Software-Komponente, Daten, welche nicht geändert werden sollen, von den übrigen Daten separiert und separat gesichert werden und/oder separat mit einer Prüfsumme belegt werden.

7. Verfahren nach einem der vorstehenden Ansprüche, **dadurch gekennzeichnet,** dass durch das Kennzeichnungsattribut, durch welches die Eignung von Daten für den Einsatz dieses bestimmten Sicherheitslevels gekennzeichnet wird, hinsichtlich jeglicher Weiterverarbeitung dieser Daten ein maximal erreichbarer Sicherheitsintegritäts-Level und/oder der Einsatz eines vordefinierten Sprachumfangs, bspw. gemäß LVL (Limited Variability Languages), oder FVL (Full Variability Language) definiert wird.

8. Verfahren nach einem der vorstehenden Ansprüche, **dadurch gekennzeichnet,** dass nach der Übertragung von Daten zwischen zwei Sub-Systemen das den Daten hinzugefügte Kennungsattribut durch das empfangene Sub-System immer auf ein Kennungsattribut gesetzt wird, welches den geringsten Sicherheitslevel kennzeichnet, und zwar aus der Gruppe der Sicherheitslevel, welchen die bei dieser Übertragung beteiligten Sub-Systeme genügen und für welchen die übertragenen Daten bei dieser Übertragung als geeignet gekennzeichnet sind.

9. Vorrichtung zur Durchführung des Verfahrens nach einem der vorstehenden Ansprüche, umfassend eine sichere Hardware- und/oder Software-Komponente die einem bestimmten Sicherheitslevels für eine funktional sichere Datenverarbeitung genügt, **dadurch gekennzeichnet,**
dass die sichere Hardware- und/oder Software-Komponente dazu eingerichtet ist,
– Daten zu funktional sicheren Daten eines bestimmten Sicherheitslevels zu verarbeiten und diesen Daten anschließend wenigstens ein Kennzeichnungsattribut hinzu zu fügen, welches die Eignung dieser Daten für den Einsatz dieses bestimmten Sicherheitslevels kennzeichnet,
und/oder dass die sichere Hardware- und/oder Software-Komponente dazu eingerichtet ist,
nach Erhalt von Daten, welche zu funktional sicheren Daten eines bestimmten Sicherheitslevels verarbeit sind und denen ein Kennzeichnungsattribut hinzugefügt ist, welches die Eignung dieser Daten für den

Einsatz dieses bestimmten Sicherheitslevels kennzeichnet, das diesen Daten hinzugefügte Kennzeichnungsattribut dahingehend zu prüfen, ob der Sicherheitslevel, den dieses Kennzeichnungsattribut kennzeichnet gegenüber dem Sicherheitslevel, welchem die Hardware- und/oder Software-Komponente genügt, gleich oder ungleich ist, und, wenn die Prüfung ungleiche Sicherheitslevel ergibt, eine Weiterverarbeitung der Daten auf dem geringeren Sicherheitslevel basierend durchzuführen.

Es folgen 3 Seiten Zeichnungen

Anhängende Zeichnungen

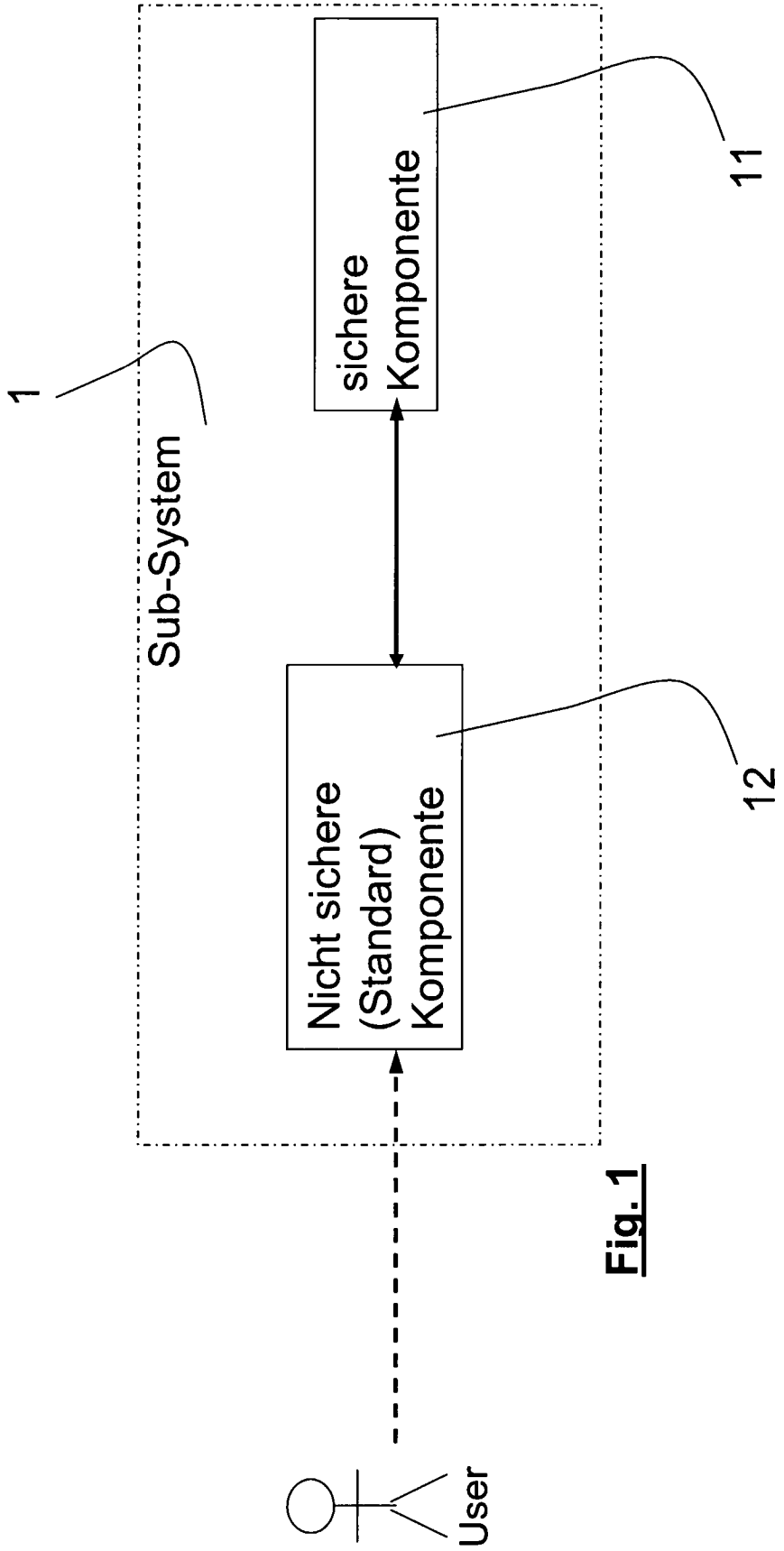

Fig. 1

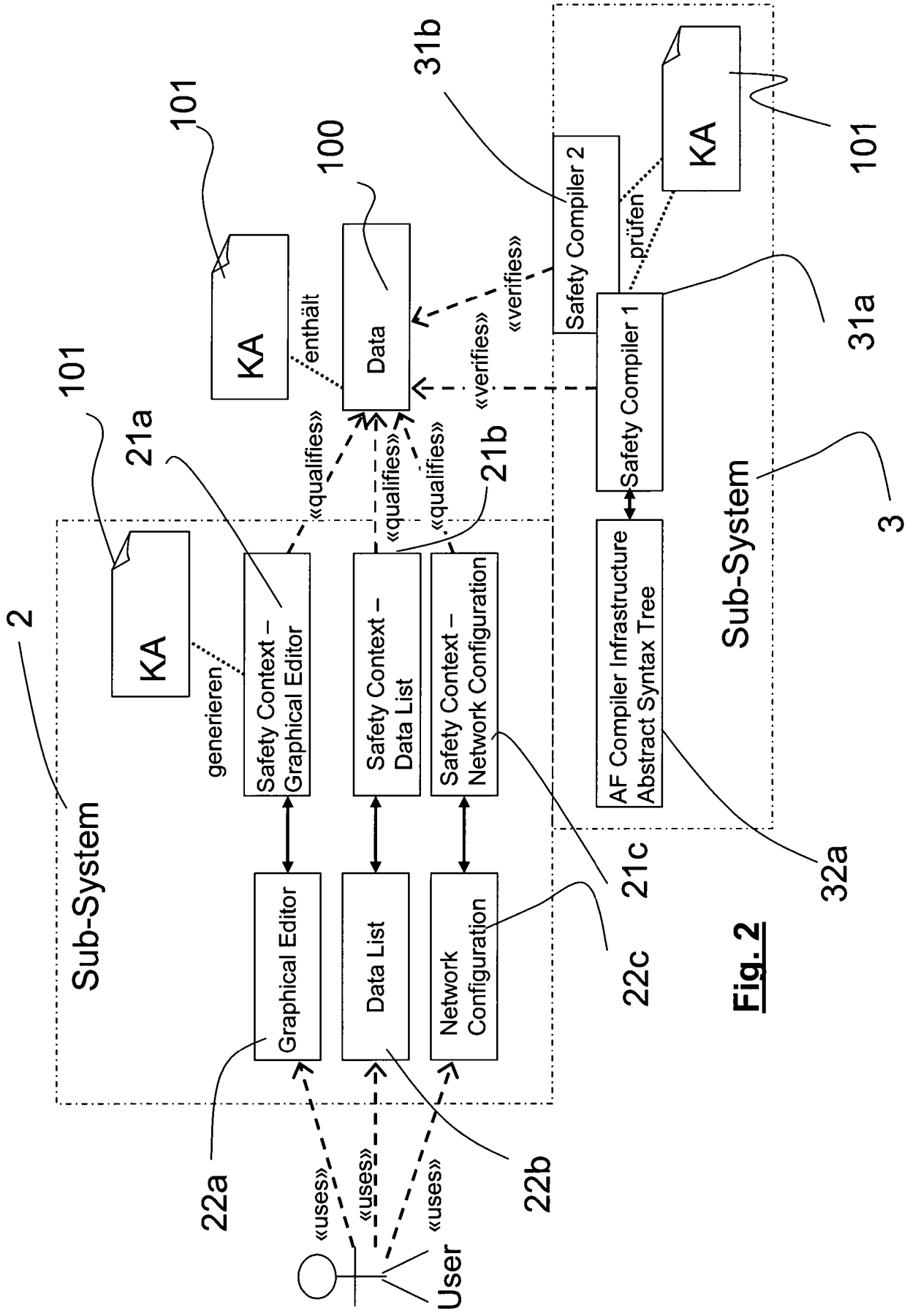
2
Sub-System
101
KA
generieren
21a
Safety Context – Graphical Editor
Graphical Editor
22a
Safety Context – Data List
Data List
Safety Context – Network Configuration
Network Configuration
21b
21c
22b
22c
«qualifies»
«qualifies»
«qualifies»
100
Data
enthält
101
KA
31b
Safety Compiler 2
«verifies»
«verifies»
prüfen
Safety Compiler 1
31a
AF Compiler Infrastructure Abstract Syntax Tree
32a
Sub-System
3
«uses»
«uses»
«uses»
User

Fig. 2

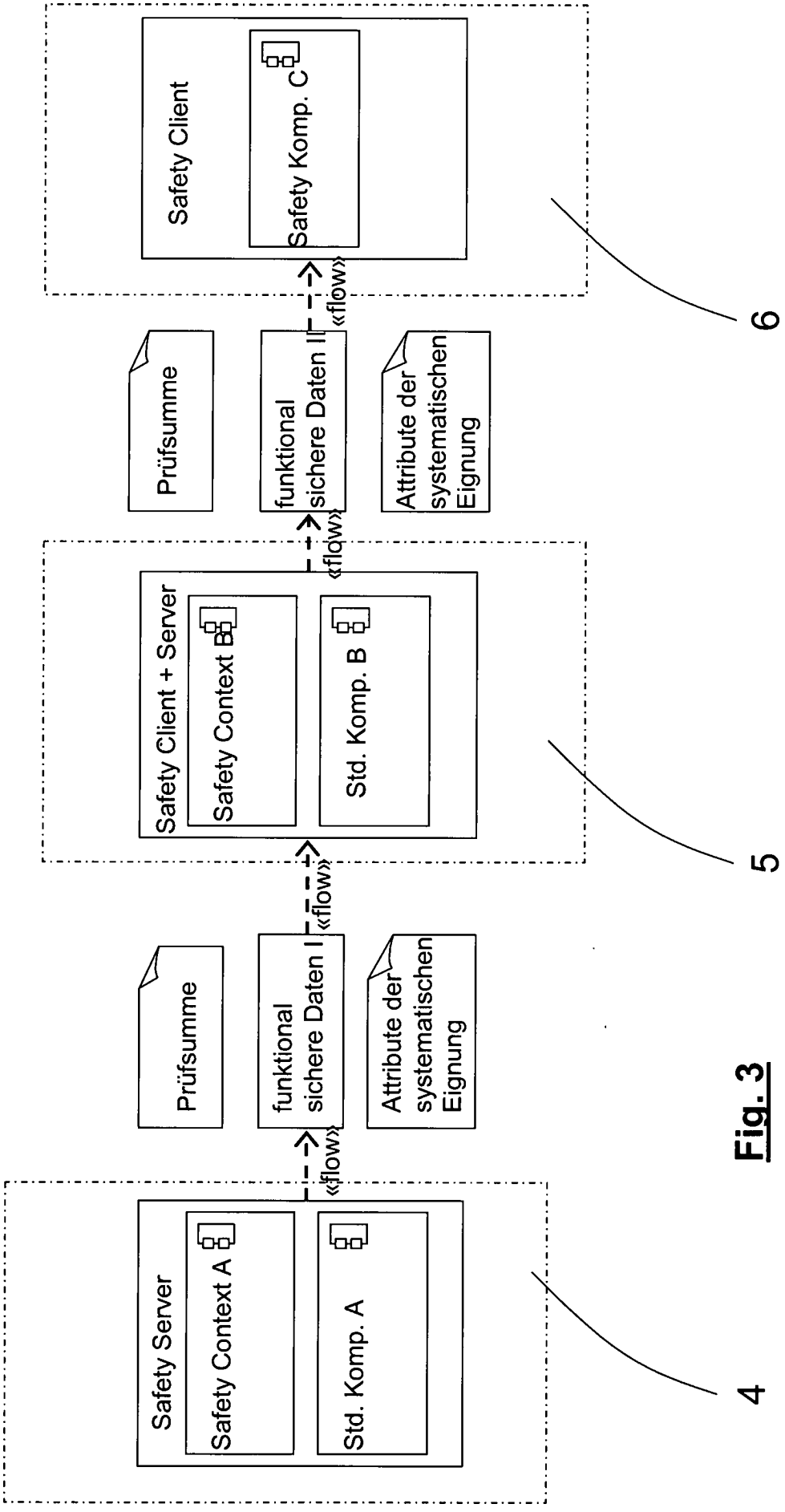
Safety Server
Safety Context A
Std. Komp. A
4
Prüfsumme
funktional sichere Daten I
Attribute der systematischen Eignung
«flow»
Safety Client + Server
Safety Context B
Std. Komp. B
5
Prüfsumme
funktional sichere Daten II
Attribute der systematischen Eignung
«flow»
Safety Client
Safety Komp. C
6

Fig. 3