Verification and certification of an electronic component

A circuit (100) is designed to be executed in a predeterminable operating mode of a plurality of operating modes. The circuit comprises a first functional unit (110) and a second functional unit (120). The first functional unit is designed as a static functional unit (110) that in each of the plurality of operating modes of the circuit (100) carries out a consistent function. The second functional unit is designed as an adaptable functional unit (120) that is designed to be configured, prior to the circuit being put into service, according to a first configuration of a plurality of different configurations and during the operating time of the circuit to maintain the first configuration so that the first configuration of the second functional unit defines the predeterminable operating mode of the circuit. This makes it possible to reduce the verification expenditure for the circuit because verification can be limited to the adaptable functional unit.
Description

Technical field

[0001] The invention relates to a circuit for carrying out, in particular, safety-relevant or safety-critical functions. Furthermore, the invention relates to a method for verifying the function of a configurable or programmable circuit.

Background of the invention

[0002] In safety-relevant or safety-critical areas stringent requirements in terms of operational safety are imposed on automation elements such as electrical or electronic units, circuits or other functional units. In this context the term "operational safety" refers, in particular, to the consideration and analysis of dangers that can arise as a result of defective functions of the automation elements during operation of such an automation element, and to minimizing these dangers, with the use of suitable measures, to an acceptable level.

[0003] In the context of this description the terms "safety-relevant areas" or "safety-critical areas" refer, in particular, to technical installations or equipment, which during their operation could pose a danger to the surroundings, i.e. to the environment and or to persons; or to technical installations whose divergent function, i.e. whose defective function, from an intended function would compromise safety. This can, for example, relate to means of transport, in particular aircraft, to industrial automation equipment or other technical installations, in particular technical installations that are operated in spatial proximity to persons.

[0004] The function of such technical installations needs to be verified, and the technical installation per se needs to be certificated for operation. In other words, it must be verified or proven that functional requirements are met by technical installations and that the latter can thus be approved for operation. In the context of verification, investigations are carried out to determine whether in the technical installation there are any divergences of the actual behavior, in other words of the actual function, from the expected or required behavior, in other words from the target function in particular predetermined scenarios, so-called test scenarios. The number and design of the test scenarios can vary from one field of application to another of the technical installation.

[0005] If no such deviation is discovered, the technical installation is certificated for operation.

[0006] This procedure can lead to considerable expenditure for verification and thus also for certification of such technical installations that can involve a host of different configurations or operating modes, in particular when these configurations can be changed during the operating time of the technical installation. For each configuration and for each operating mode respective individual test scenarios are to be drawn up and correspond-
possible, by reducing the complexity and the range of functions of the circuit in the form of the first functional unit and of the second functional unit, to also reduce the verification expenditure necessary for this. By limiting the configuration options or the number of operating modes, and by structuring the circuit in a static and an adaptable functional unit, a reduction in the verification expenditure is achieved, which is tantamount to a reduction in the complexity. In this design modular re-uses of functional units in the adaptable part are possible, which reduces the verification expenditure in that verification is limited to this adaptable part only. The static part was verified earlier and does not need to be verified again.

[0015] Any change to the circuit or to its functional units cannot take place during the operating time of the circuit but only prior to putting the circuit into operation.

[0016] In other words, a circuit as described above and below provides the option that its mode of operation and its range of functions are changed and thus the circuit is configured. However, such a change or configuration of the function is limited to the time prior to putting the circuit into service. Prior to the circuit being put into service it is configured to a function or to an operating mode. In this process the function or the operating mode is selected from a plurality of functions or operating modes.

[0017] During the operating time of the circuit it is not possible to change any functions of the circuit, either by adding new functions or by changing existing functions, in other words the operating mode cannot be changed during the operating time.

[0018] Any change in the operating mode of the circuit requires renewed verification and certification of the circuit. Since the circuit comprises static functional units and adaptable functional units, such a change of the operating mode is limited to the adaptation of one or several adaptable functional units, whereas the static functional units are maintained unchanged.

[0019] Verification of the mode of operation of the circuit can be limited to verification of the adaptable functional units because the static functional units have already undergone verification.

[0020] Thus the expenditure for the verification of a circuit is reduced in that the complexity of the functional units, in other words their range of functions, is reduced, and at least adaptable functional units, after the circuit has been taken out of service and prior to the circuit being put into renewed service, are adaptable in terms of their range of functions, but not, however, during the operating time of the circuit.

[0021] On the one hand a current range of functions (in other words the range of functions provided during the operating time of the circuit) of the adaptable functional unit is reduced, and thus the current complexity of this adaptable functional unit is reduced too, in favor of reduced verification expenditure. On the other hand an entire range of functions (in other words the number of different configurations of the adaptable functional unit, which configurations can optionally be taken individually in each case) of the adaptable functional unit is maintained in that the adaptable functional unit provides the option of adapting its range of functions outside the operating time of the circuit, in other words of differently configuring the adaptable functional unit.

[0022] If the extent of the entire available range of functions is expanded, in other words given new functions, then it may be sufficient in each case to individually verify and certify said new functions.

[0023] The term "operating time" refers to the time period between the beginning of the use of the circuit for a particular task and the end of the use of the circuit for this particular task. Within this time period the circuit can thus be disconnected from an energy supply and can subsequently be activated anew, wherein the circuit then operates in the same operating mode as it did before disconnection from the energy supply. However, as soon as the configuration of the circuit is changed, its operating time in this operating mode or in this configuration is terminated.

[0024] The configuration of the circuit comprises its technical or logic and structural design and the functions carried out therewith, in other words the mode of operation of the circuit. Any change of an individual aspect of the configuration of the circuit requires renewed verification, at least of the changed aspect or of the changed functional unit.

[0025] The adaptable functional unit has several possible configurations and during the concept time or configuration time has one single configuration of the plurality of possible configurations firmly assigned to it. Thus during the operating time the function of the adaptable functional unit cannot be changed; however, reconfiguration is possible after the circuit has been taken out of service, and consequently some other operating mode or some other function is assigned to the circuit. By doing away with changing the configuration during the operating time, the complexity of the adaptable functional unit is reduced, which furthermore also reduces the expenditure associated with verification of this functional unit.

[0026] According to one embodiment the circuit is designed to unchangeably maintain the first configuration of the adaptable functional unit during the operating time of the circuit. According to a further embodiment the circuit is designed to unchangeably maintain the first configuration of the adaptable functional unit during the operating time of the circuit at least until the circuit is taken out of service.

[0027] According to a further embodiment the adaptable functional unit is designed, after the operating time and prior to the circuit being put into service anew, to be configured according to a second configuration, and after the circuit is put into service to unchangeably maintain this second configuration of the circuit at least until the circuit is taken out of service.

[0028] This makes it possible for the circuit to change its operating mode in that the adaptable functional unit is reconfigured, in particular in that only the adaptable
functional unit is reconfigured. Thus, verification and certification are required only in relation to the adaptable functional unit whose range of functions has been changed, whereas there is no need to certify anew the static functional unit, provided its mode of operation is not influenced by the reconfigured adaptable functional unit. According to a further embodiment the circuit is an electrically configurable logic circuit gate.

This can, in particular, be a so-called field-programmable gate array (FPGA) to which a structure of a logic circuit can be programmed or configured. An FPGA is designed in such a manner that it can be programmed with special instructions so that an FPGA can carry out changing functions, in each case depending on the programming or on the configuration. An FPGA comprises a plurality of so-called frames to which in each case a logic circuit structure and connections between two or more circuit structures for forwarding signals between the circuit structures can be programmed.

The first functional unit and the second functional unit can be programmed as circuit structures in a first frame or a second frame of the FPGA.

If an FPGA is reconfigured, i.e. if the contents of the frames are described anew, usually the entire configuration of the FPGA is transmitted from a configuration unit to the FPGA. In this process the frames are, for example, programmed, i.e. configured, one after the other. If in such a reconfiguration of the FPGA the content of the first frame is not changed (in other words if the static functional unit is located in the first frame), there is no need to subject the circuit structure of this first frame to verification. If the content of the second frame is changed and if this circuit structure has not yet been verified, the function of this second frame, in other words the adaptable functional unit, is subjected to verification.

The commands used for configuring the FPGA are converted to electrical signals by the configuration unit and on the FPGA are transposed to circuit structures of functional units and connections between functional units.

There is thus a direct and defined interrelation between the commands used for configuring the FPGA, the electrical signals that are transmitted to an FPGA module, the thus realized logic circuit structures on the FPGA module, and lastly the mode of operation and functioning of the FPGA and of the individual functional units on the FPGA.

However, the functional units can also be individual physical units for a circuit, wherein the circuit comprises a plurality of such functional units.

The circuit can be designed as a plug-in module or expansion module for an arithmetic-logic unit or control unit. The actual functions of the static functional unit and of the adaptable functional unit can vary, depending on the particular field of application. Thus, the functional units can comprise memory modules whose size and access option can vary. The functional units can be input/output modules or a data processing unit, wherein the data processing unit receives a set of input data, processes this data according to the configured function, and provides output data.

The circuit can be used for controlling or monitoring safety-critical processes, for example in an aircraft for navigation, for the autopilot, or for life-sustaining systems. Likewise, the circuit can be used for controlling weapon systems. The plurality of possible configurations of the adaptable functional unit can relate to functions of differing criticality, for example as a control unit for life-sustaining systems (high criticality) and as a control unit for entertainment systems (low criticality) on board aircraft.

According to a further embodiment the circuit can comprise a plurality of adaptable functional units which, taken individually, can be adaptable and replaceable.

According to a further aspect a method for verifying the function of an electrically configurable logic circuit gate is stated, wherein a function of the circuit gate is specified in that the circuit gate is configured by way of electrical signals, and wherein the electrical signals specify the functions of the circuit gate. The method comprises the following steps: in a first step detecting a signal pattern of the electrical signals by means of which the circuit gate is configured takes place; in a following step reconciling the detected signal pattern with a plurality of signal patterns of already verified functions takes place; in a following step a reduced signal pattern is determined by removing the signal patterns of already verified functions from the detected signal pattern; in a following step the function of the reduced signal pattern is verified.

This method allows simple recognition of the changed functional units of a configurable circuit gate with little expenditure because the electrical signals by means of which the circuit gate is configured are analyzed.

The electrical signals used for configuring directly determine the range of functions of the circuit gate; it is thus sufficient if for determining divergent functions of the circuit gate the divergences in the electrical signals that configure the logic circuit gate are determined. According to one embodiment of the method, in the step of reconciling the detected signal pattern with a plurality of signal patterns of already verified functions, value-discrete signals are compared to each other.

This can simplify reconciliation of signal sequences and can reduce the error rate during reconciliation.

According to a further embodiment of the method, in the step of reconciling the detected signal pattern with a plurality of signal patterns of already verified functions, binary signals are compared to each other.

According to a further embodiment of the method, reconciling the detected signal pattern with a plurality of signal patterns of already verified functions takes place by means of a bit pattern comparison.
fying the function of a configurable circuit is stated. The device is designed to read-in a signal pattern of an electrical signal for configuring the circuit, and to carry out the method as described above and below.

[0045] In this process, reading-in the electrical signal can take place by means of an acquisition unit in that electrical signals on a configuration line are acquired. The acquisition unit can, in particular, be designed to read-in voltage levels as well as any changes therein over the time on the configuration line.

[0046] To this effect the device for verifying the function of a configurable circuit can be coupled to a configuration unit or to the configurable circuit in such a manner that the device directly acquires the electrical signal used for configuring the circuit when this electrical signal is transmitted by the configuration unit by way of the configuration line to the configurable circuit.

[0047] According to one embodiment the device for verifying the function of a configurable circuit can be designed to read-in representations of the electrical signals, in other words of the configuration signals, and to process them according to the further steps of the method.

[0048] The term "representations of the electrical signals" refers, for example, to a numeric representation of a curve of an electrical configuration signal of a configurable circuit over time. These representations of electrical signals can, for example, be read from a memory unit by the device for verifying (verification device) the function of a configurable circuit, wherein the memory unit can comprise a plurality of representations of electrical signals.

[0049] In this embodiment the verification device can compare a first representation of electrical configuration signals with a second representation of electrical configuration signals. In this process the part that corresponds to the representations of the electrical configuration signals which represent the static functional unit is detected from both representations. These two parts are checked to determine whether they are identical. If they are identical, these parts are excluded from renewed verification because verification of these static functional units has already taken place. In this embodiment reconciliation can take place in such a manner that patterns relating to entire frames of the circuit are reconciled.

[0050] If individual functional units are programmed to respective individual frames of the configurable circuit, such a comparison of the representations of the signal sequences for functional units can on the whole take place more easily because the beginning of a new frame can unambiguously be recognized in a representation of the signal sequence.

[0051] In this embodiment, for example, the representation of the first signal sequence can comprise two sub-sequences that correspond to two already verified functional units. The first sub-sequence corresponds to a static functional unit, and the second sub-sequence corresponds to an adaptable functional unit. In this arrangement a sub-sequence corresponds to the content of a frame of an FPGA.

[0052] The verification unit compares the representation of each sub-sequence of the first signal sequence with the representation of each sub-sequence of the verified second signal sequence of the two configurations. If identical sub-sequences are detected, they are no longer used for the further consideration of the first signal sequence to be verified. Thus from the representations of the first signal sequence those sub-sequences remain that correspond to the adaptable functional unit. Only these sub-sequences are to be verified in terms of their own function and in terms of the interfaces to other functional units and/or already verified functional units.

Brief description of the drawings

[0053] Below, exemplary embodiments of the invention are discussed in more detail with reference to the enclosed drawings. The following are shown:

Fig. 1 a circuit according to an exemplary embodiment;

Fig. 2 a device for verifying the function of a configurable circuit according to an exemplary embodiment;

Fig. 3 steps of a method according to an exemplary embodiment.

Detailed description of exemplary embodiments

[0054] Fig. 1 shows a circuit 100 with a first functional unit 110 and a second functional unit 120. The two functional units 110, 120 are modules or functional blocks of the circuit 100.

[0055] The first functional unit 110 is designed as a static functional unit, and the second functional unit 120 is designed as an adaptable functional unit. Dividing an overall function of the circuit 100 into a static unit and an adaptable unit takes place in such a manner that in the static unit those functions are contained that do not differ for various fields of application.

[0056] The static unit can comprise different configuration sets, for example a first configuration set for a first group of fields of application and a second configuration set for a second group of fields of application, if in this manner more common features relating to the static unit can be identified.

[0057] The circuit 100 comprises an input interface 130A and an output interface 130B.

[0058] By way of the input interface 130A signals or data are transmitted to the circuit, which signals or data are processed by the functional units of the circuit. This can, for example, relate to data from sensors.

[0059] By way of the output interface 130B the circuit 100 emits signals that are, for example, used as control signals for actuators or that represent a processing result...
The circuit 100 comprises a configuration of the signals on the input interface.

**[0060]** The circuit 100 comprises a configuration interface 140. By way of this interface a programmable circuit is configured, i.e. the circuit receives those signals that define the function of the circuit.

**[0061]** Fig. 2 shows a circuit 100 that by way of the configuration interface is coupled to a configuration unit 300. The configuration unit 300 is designed to convert commands for configuring the circuit 100 to electrical signals, and to transmit these electrical signals by way of the configuration connection 145 to the circuit 100, as indicated by the single arrow along the configuration connection 145.

**[0062]** A verification unit 200 (device for verifying the function of a configurable circuit) is coupled to the configuration connection 145 and is designed to detect the electrical signals transmitted by way of the configuration connection 145.

**[0063]** The detected signals are reconciled, by the verification unit 200, with signal patterns stored in a memory unit 230. The signal patterns stored therein can be already verified signal patterns, and thus already verified commands or electrical signals for functional units of the circuit.

**[0064]** If a signal pattern is detected that is stored in the memory unit 230, this means that this signal pattern or this signal sequence can be excluded from renewed verification because it is a signal sequence that has already been verified.

**[0065]** In order to make it possible to achieve context-dependent recognition of signal patterns, reconciliation can take place in such a manner that signal patterns for entire frames of the circuit are reconciled. In this way it is possible to avoid a situation where sub-sections of a non-verified functional unit, which are also found as sub-sections of a verified functional unit, can be recognized as having been verified.

**[0066]** In other words, a functional unit is reconciled as a whole with the already verified functional units, because the functional unit as a whole needs to be verified.

**[0067]** If individual functional units are programmed to respective individual frames of the configurable circuit, such a comparison of the signal sequences for functional units on the whole can take place more easily because the beginning of a new frame can unambiguously be recognized in a signal sequence.

**[0068]** Fig. 3 diagrammatically shows the reconciliation of two signal sequences 150A, 150B. The signal sequence 150A can, for example, comprise two sub-sequences 155, 158A that correspond to two already verified functional units. Sub-sequence 155 corresponds to a static functional unit, and sub-sequence 158A corresponds to an adaptable functional unit. A sub-sequence corresponds to the content of a frame of an FPGA.

**[0069]** If a circuit is then configured with new functional units according to the signal sequence 150B, the sub-sequences 155 and 158B are transmitted by the configuration unit 300 to the circuit 100, and are detected by the verification unit 200 (see Fig. 2).

**[0070]** Sub-sequences 155, 158A, which correspond to already verified functional units, are stored in the memory unit 230 (Fig. 2).

**[0071]** The verification unit 200 reconciles each sub-sequence of the signal sequence 150B with each verified signal sequence from the memory unit. If in the memory unit 230 identical sub-sequences are determined, they are no longer used for the further consideration of the detected signal sequence. From the signal sequence 150B those sub-sequences then remain that were not found in the memory unit. In the example of Fig. 3 this is the sub-sequence 158B. Only these sub-sequences are to be verified in terms of their own function and in terms of the interfaces to other functional units and/or already verified functional units.

**Claims**

1. A circuit (100) that is designed to be executed in a predeterminable operating mode of a plurality of operating modes, with the circuit comprising:

   a first functional unit (110);
   a second functional unit (120);
   wherein the first functional unit is designed as a static functional unit (110) that is designed, in each of the plurality of operating modes of the circuit (100), to carry out a consistent function;
   wherein the second functional unit is designed as an adaptable functional unit (120) that is designed to be configured, prior to the circuit being put into service, according to a first configuration of a plurality of different configurations;
   wherein the second functional unit (120) is designed, during the operating time of the circuit, to maintain the first configuration so that the first configuration of the second functional unit defines the predeterminable operating mode of the circuit.

2. The circuit (100) of claim 1, wherein the circuit is designed to unchangeably maintain the first configuration of the second functional unit during the operating time of the circuit.

3. The circuit (100) of claim 2, wherein the circuit is designed to unchangeably maintain the first configuration of the second functional unit during the operating time of the circuit at least until the circuit is taken out of service.

4. The circuit (100) of any one of the preceding claims, wherein the second functional unit (120) comprises a plurality of adaptable functional units.

5. The circuit (100) of any one of the preceding claims,
wherein the second functional unit (120) is designed, after the operating time and prior to the circuit being put into service anew, to be configured according to a second configuration, and after the circuit is put into service to unchangeably maintain this second configuration at least until the circuit is taken out of service.

6. The circuit (100) of any one of the preceding claims, wherein the circuit is an electrically configurable logic circuit gate.

7. A method for verifying the function of an electrically configurable logic circuit gate, wherein a function of the circuit gate is specified in that the circuit gate is configured by way of electrical signals, wherein the electrical signals specify the functions of the circuit gate; the method comprising the steps of:

   - detecting a signal pattern of the electrical signals;
   - reconciling the detected signal pattern with a plurality of signal patterns of already verified functions;
   - determining a reduced signal pattern by removing the signal patterns of already verified functions from the detected signal pattern;
   - verifying the function of the reduced signal pattern.

8. The method of claim 7, wherein in the step of reconciling the detected signal pattern with a plurality of signal patterns of already verified functions, value-discrete signals are reconciled to each other.

9. The method of claim 7 or 8, wherein in the step of reconciling the detected signal pattern with a plurality of signal patterns of already verified functions, binary signals are reconciled to each other.

10. The method of claim 9, wherein reconciling the detected signal pattern with a plurality of signal patterns of already verified functions takes place by means of a bit pattern comparison.

11. A device (200) for verifying the function of a configurable circuit, wherein the device is designed to read-in a signal pattern of an electrical signal for configuring the circuit; and wherein the device is designed to carry out the method of any one of claims 7 to 10.
## DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document with indication, where appropriate, of relevant passages</th>
<th>Relevant to claim</th>
<th>CLASSIFICATION OF THE APPLICATION (IPC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>US 5 457 408 A (LEUNG WAi-BOR [US]) 10 October 1995 (1995-10-10)</td>
<td>1-11</td>
<td>INV. G06Q10/00</td>
</tr>
<tr>
<td></td>
<td>* abstract *</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>* column 1, line 12 - column 3, line 15 *</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>* column 5, line 13 - column 8, line 33 *</td>
<td></td>
<td></td>
</tr>
<tr>
<td>X</td>
<td>WO 02/10785 A2 (LOGICVISION INC [US]; NADEAU DOSTIE BENOIT [CA]; BUREK DWAYNE [US]; CO) 7 February 2002 (2002-02-07)</td>
<td>1-11</td>
<td></td>
</tr>
<tr>
<td></td>
<td>* abstract *</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>* page 2 - page 3 *</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>* page 5, line 1 - page 8, line 16 *</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### TECHNICAL FIELDS SEARCHED (IPC)

- G06Q
- G01R

---

The present search report has been drawn up for all claims

Place of search: Munich

Date of completion of the search: 17 July 2015

Examiner: Lopes Margarido, C

### CATEGORY OF CITED DOCUMENTS

- **X**: particularly relevant if taken alone
- **Y**: particularly relevant if combined with another document of the same category
- **A**: technological background
- **D**: document cited in the application
- **L**: document cited for other reasons
- **T**: theory or principle underlying the invention
- **E**: earlier patent document, but published on, or after the filing date
- **P**: intermediary document
- **F**: member of the same patent family, corresponding document
This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on.

The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

17-07-2015

<table>
<thead>
<tr>
<th>Patent document cited in search report</th>
<th>Publication date</th>
<th>Patent family member(s)</th>
<th>Publication date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>TW 302546 B 11-04-1997</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 5457408 A 10-10-1995</td>
<td></td>
</tr>
<tr>
<td>WO 0210785 A2 07-02-2002</td>
<td></td>
<td>AU 7036801 A 13-02-2002</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CA 2416655 A1 07-02-2002</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>JP 2004518222 A 17-06-2004</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 6615392 B1 02-09-2003</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 0210785 A2 07-02-2002</td>
<td></td>
</tr>
</tbody>
</table>

For more details about this annex: see Official Journal of the European Patent Office, No. 12/82