Funktionale Sicherheit

Wie Hall-Sensoren mit Diagnosefunktion für mehr Sicherheit sorgen

04.07.17 | Autor / Redakteur: Tatjana Kübler und Dr Thomas Wolf * / Hendrik Härter

Funktionale Sicherheit: Dank integrierter Diagnosefunktion sind spezielle Hall-Sensoren ASIL-A geeignet. (Bild: vege/Fotolia.com)

Ausfälle oder Fehlfunktionen von sicherheitsrelevanten Systemen müssen unbedingt vermieden werden. Dank integrierter Diagnosefunktion sind spezielle Hall-Sensoren ASIL-A geeignet.

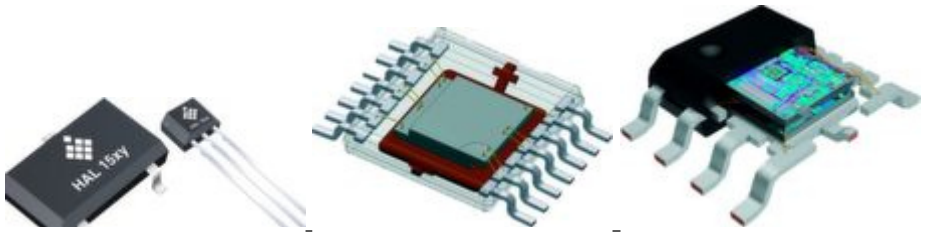
Die stetig wachsenden Sicherheitsanforderungen der EU an die Automobilindustrie erfordern Standards, um die Sicherheit der Fahrzeuginsassen zu steigern. Im Rahmen des Konzepts der funktionalen Sicherheit soll das Risiko von Ausfällen oder Fehlfunktionen von sicherheitsrelevanten Systemen im Kraftfahrzeug vermindert werden. Die zugrundeliegende Norm der funktionalen Sicherheit stellt die *ISO26262* dar. Mit ihr gehen Sicherheitsmaßstäbe für sicherheitsrelevante Systeme und deren Einzelkomponenten in den Applikationen einher.

Systeme im Sinne der Norm bestehen sehr oft aus einem oder mehreren Sensoren, einem Steuergerät und einem Aktor. Um die Anforderungen von normgerechten Systemen zu erfüllen, hat der Hersteller TDK-Micronas (vertrieben von Endrich Bauelemente) mit dem HAL15xy (Bild unten) einen Hall-Schalter entwickelt, welcher

mit allen notwendigen Diagnosefeatures wie der Option eines Selbsttests zur Funktionsprüfung des Sensors oder einer Drahtbrucherkennung ausgestattet ist.

Auch bei den analogen, programmierbaren Hallsensor-Serien von TDK wird die Funktionssicherheit von Hallsensor-Anwendungen durch redundante Typen weiter erhöht. Die Sicherheitsanforderungen der erwähnten **ISO26262** werden in vier verschiedene Automotive Safety Integrity Levels = ASIL unterteilt: A, B, C und D. Dabei stellt Level D die höchste Stufe der Sicherheitsanforderungen an das System und seine Komponenten dar.

BILDERGALERIE



Fotostrecke starten: Klicken Sie auf ein Bild (3 Bilder)

Entwicklungs- und Herstellungsprozessen dokumentieren

Für die elektronischen Bauteile in einer nach ASIL klassifizierten Anwendung bedeutet ASIL in erster Linie die detaillierte Dokumentation von Entwicklungs- und Herstellungsprozessen nach den vorgegebenen Normen. Ein Beispiel für eine ASIL-D-Applikation ist die Lenkung eines Fahrzeugs, deren Ausfall in der Praxis ein Worst-Case-Szenario darstellen würde. Ein wichtiger Aspekt ist, dass der HAL15xy von TDK-Micronas als Einzelkomponente selbst nicht ASIL-klassifiziert sein kann. Das ist nur dem ganzen System vorbehalten.

Die Komponenten können ausschließlich „ASIL-ready“ sein und tragen dazu bei, dass ein System ein bestimmtes ASIL-Level erreicht. Für die quantitative Bewertung, um die Sicherheitsanforderungen zu erfüllen, wurden im Rahmen der ISO26262 verschiedene Metriken festgelegt, die das System auf die Ausfallmöglichkeit hin untersuchen und bewerten, wie häufig ein zufälliger Ausfall eines Bauteils das ganze System in einen unsicheren Zustand bringen könnte. Folgende Metriken sind in der Norm definiert:

- Die **Failure in Time Rate = FIT-Rate** beschreibt die Ausfallrate eines Bauteils oder einer Komponente. Sie gibt die Anzahl der Ausfälle in 109 Stunden an.
- Die **Single Point Fault Metric = SPFM** spezifiziert die Robustheit des Systems

hinsichtlich einzelner Fehler, deren Auftreten zum Ausfall des gesamten Systems führen. Verfügt das System bzw. der Sensor über mehr interne Kontrolleinrichtungen, umso besser. Beispielsweise müssen 90 Prozent der wichtigsten Funktionsparameter durch das System überprüft werden, damit das System nach Norm ASIL-B klassifiziert ist. Die Prozentwerte für die anderen Klassen sind der Norm zu entnehmen.

- Die **Latent Fault Metric = LFM** spezifiziert die Robustheit des Systems hinsichtlich der Fehler, die schleichend oder verzögert zum Ausfall des Systems beitragen. Ein Beispiel kann die Alterung des Sensors sein. Auch hier gilt: Je höher die in der Norm für jede Klasse festgelegte Prozentzahl ist, desto umfangreicher sind die im System eingebauten Diagnosemaßnahmen, die zur Erkennung solcher Fehler beitragen.

ERGÄNZENDES ZUM THEMA

Wenn die Redundanzfunktion integriert ist
Wenn die Redundanzfunktion integriert ist

Sensoren mit integrierter Redundanzfunktion in einem Gehäuse haben den Vorteil, dass sich Kosten senken lassen und die Zuverlässigkeit des Gesamtsystems erhöht wird. Grund sind kleinere Leiterplatten (PCB) und weniger Lötaufwand. Die Sensoren des Typs HAR37xy werden im gleichen SOIC8-Gehäuse produziert wie die übergeordnete Single-Die-Familie HAL37xy.

Anwender, die bereits die Single-Die-Variante verwenden, sparen sich Zeit für das Re-Design, da sie den gleichen Magnetkreis und Modulformfaktor verwenden können. Dank der identischen x/y-Positionierung der Hall-Elemente lassen sich kleinere Magnete für ihr Design verwenden.

Der entscheidende Gedanke hinter den Definitionen ist nicht, Ausfälle des Systems zu verhindern. Vielmehr soll bei einem auftretenden Fehler sichergestellt werden, dass dieser vom System erkannt wird und das System in einen „sicheren Zustand“ (Fail

Safe) gebracht wird, der das Fahrzeug und die Insassen nicht in Gefahr bringt.

Wichtig ist, dass sich die Sensoren der *HAL15xy-Familie* aufgrund der implementierten Diagnosemaßnahmen und gegebenenfalls einer entsprechenden Dekomposition sogar für Systeme mit einer höheren ASIL-Klassifizierung als ASIL-A eignen würden. Unter Dekomposition wird die Aufteilung bzw. Umverteilung der Sicherheitsanforderungen auf die einzelnen unabhängigen Systemelemente verstanden. Das Prinzip der Dekomposition wird am Beispiel eines elektrischen Fensterhebers erläutert.

Dekomposition am Beispiel eines elektrischen Fensterhebers

Der elektrische Fensterheber stellt an sich keine sicherheitskritische Applikation dar. Wenn sich ein Fenster nicht mehr öffnen oder schließen lässt, ist das für den Fahrer ärgerlich, aber nicht unmittelbar sicherheitsrelevant. Was die Anwendung sicherheitskritisch werden lässt, ist der Einklemmschutz. Der Einklemmschutz muss vor allem dann gewährleistet sein, wenn Kinder in Gefahr kommen können. Deshalb wird die Applikation in eine ASIL-A-Klassifizierung eingestuft.

Um die einwandfreie Funktion des Fensterhebers zu gewährleisten, sind Informationen wie Drehzahl und Drehrichtung des Antriebsmotors notwendig. Es ist prinzipiell möglich, diese Parameter über den Hallsensor *HAL7xy* zu gewinnen. Der Hall-Schalter besteht aus zwei nebeneinander platzierten Hallelementen in einem Gehäuse, deren Signale durch eine interne Logik ausgewertet werden. Zudem besitzt der Sensor zwei Ausgänge, die jeweils ein Taktsignal zur Detektion der Rotationsgeschwindigkeit des Motors und ein weiteres in Form eines Drehrichtungssignals an die Steuereinheit des Fensterhebers übermitteln.

Damit übernimmt der Sensor einen Teil der Informationsverarbeitung. Aufgrund der höheren Komplexität des *HAL7xy* handelt es sich um einen vergleichsweise kostenintensiven Hall-Schalter. In einem alternativen Ansatz wird der preislich günstigere Single-Plate-Hall-Schalter des Typs *HAL15xy* eingesetzt. Er gibt nur die

Information über die Drehzahl als Taktsignal vom Sensor an die Steuereinheit weiter.

Die Bewegungsrichtung der Fensterscheibe wird von der Steuereinheit über den Zugriff auf die Motorsteuerung ohne Sensor ermittelt. Der sicherheitsrelevante Aspekt der Motordrehrichtung wird durch Dekomposition vom Sensor auf die Fensterheber-Steuerung verlagert. Das Prinzip der Dekomposition ermöglicht es, sicherheitsrelevante Aspekte von einer Systemkomponente auf eine andere umzulagern, die hinsichtlich der funktionalen Sicherheit günstiger oder zweckmäßiger ist.

Power-ON-Selbsttest-Funktion

Die Sensorfamilie *HAL15xy* gibt es als 3-Draht- und 2-Draht-Hall-Schalter. Bei den 2-Draht-Sensoren stehen zwei Abschlüsse zur Verfügung, die neben der Stromversorgung auch zur Anzeige des Funktionszustandes oder der Diagnosefunktion dienen. Der Schaltzustand des 2-Draht-Sensors spiegelt sich in der Stromaufnahme des Sensors wider, während beim 3-Draht-Sensor für das Ausgangssignal und damit für die Diagnose ein separater Ausgangspin zur Verfügung steht.

Die 3-Draht-Hallsensoren von TDK-Micronas bieten mit der Power-ON-Selbsttest-Funktion ein interessantes Feature: Dieser Selbsttest ermöglicht es, die wichtigsten internen Parameter innerhalb weniger Millisekunden nach dem Anlegen der Betriebsspannung abzufragen. Für einen Selbsttest sind zwei freie Ports des Mikrocontrollers nötig. Ein Port-Pin schaltet die Versorgungsspannung V_{SUP} des Sensors ein und aus. Der andere Port-Pin ist mit dem Ausgang des Sensors verbunden.

Wird der Sensor vom Controller bei auf LOW gehaltenem Ausgangspin OUT aus dem ausgeschalteten Zustand mit Spannung versorgt, startet der Sensor einen Selbsttest. Danach wird der Ausgangs-Pin des Hallsensors vom Controller freigegeben und dieser beobachtet die Reaktion des Sensors. Nach einer kurzen Verzögerung prüft der Sensor

den Signalpfad.

Dabei wird ein Magnetfeld simuliert, was einer Hallspannung am Sensorelement entspricht. Am Ende des Signalpfades wird das tatsächliche Messsignal mit dem Sollwert verglichen und am Ausgangspin ein Low-Signal ausgegeben, falls der Funktionstest erfolgreich war. Anschließend wird die Richtung des simulierten Magnetfeldes umgekehrt.

Wenn ein Fehlerfall eintritt

Stimmen Vorzeichen und Betrag mit dem Sollwert überein, wird der Ausgang für wenige Millisekunden auf High gelegt. Der Selbsttest ist abgeschlossen und der Sensor startet im normalen Betriebsmodus und zwar selbst dann, wenn ein Fehler erkannt wurde. Der angeschlossene Mikrocontroller verfolgt Timing und Pegel des Ausgang-Pins während des Selbsttests und bewertet, ob der Selbsttest erfolgreich war oder ob ein Fehler vorliegt. Bei einem Fehler geht der Ausgang auf jeden Fall in einen hochohmigen Tri-State-Zustand über.

Das Steuergerät erkennt den Zustand und sorgt dafür, dass dieser für das Fahrzeug keine Gefahr darstellt. Zudem lässt sich prüfen, ob alle Drahverbindungen zum Sensor vorhanden sind. Bei Drahtbruch würde der Selbsttest nicht starten. Beim 2-Draht-Sensor startet der interne Selbsttest immer automatisch, es sei denn, die Option wurde vom Hersteller während der Produktion deaktiviert. Der Fail-Safe-Zustand wird im Fehlerfall durch einen Errorstrom signalisiert. Während im fehlerfreien Betrieb die Ströme zwischen 12 bis 17 mA (High) und 2,5 bis 7 mA (Low) liegen, zeigt ein Strom >2 mA einen Fehler an.

Die *HAL15xy-Familie* bietet neben dem Power-ON-Selbsttest sowohl bei der 3-Draht- als auch bei der 2-Drahtversion bei Betrieb eine Diagnoseprozedur. Dabei werden Über- oder Unterspannung, Drahtbruch, fehlerhafte Stromlevels oder Hallspannungen sowie vom Sollwert abweichende Referenzspannungen detektiert. Im Fehlerfall schaltet

der Ausgangspin analog zum Selbsttest in einen hochohmigen (High-Z) Fail-Safe-Zustand, beim 2-Draht-Sensor ist der Fail-Safe-Zustand ein Fehlerstrom <2 mA.

Das Konzept des redundanten Aufbaus der Sensoren

Ein weiteres Feature ist das Konzept des redundanten Aufbaus des Hallsensors. Die Sensoren eignen sich auch für das zuvor erwähnte Prinzip der Dekomposition. Sicherheitsanforderungen an eine zuverlässige Messwerterfassung können durch zwei einzelne, unabhängige Sensoren der gleichen Bauart realisiert werden. Da zwei Sensoren nicht an der gleichen Stelle sind, liefern sie unterschiedliche Messergebnisse.

Die Steuereinheit vergleicht beide Ergebnisse auch auf Plausibilität. Eine redundante Ausführung erfüllt die Bedingung der Unabhängigkeit der Messungen. Die redundanten Sensoren enthalten zwei Chips, die übereinander angeordnet sind. Beide Sensor-Chips arbeiten unabhängig, da sie zwar mechanisch durch eine Zwischenschicht verbunden, aber elektrisch gegeneinander isoliert sind.

Entscheidender Unterschied der beiden linearen Sensoren *HAR24xy* und *HAR37xy* ist die gegenseitige Positionierung der beiden Dies. Der Versatz der beiden verwendeten Dies beim *HAR24xy* ermöglicht im Vergleich zum *HAR37xy* eine niedrigere Bauhöhe, da die Bonddrähte beim *HAR24xy* nach links und rechts weggeführt werden. Beim *HAR37xy* liegen die beiden Dies und damit die zwei Messzellen des Chips exakt übereinander, wodurch das Magnetfeld an der selben lateralen Position ermittelt wird.

* Tatjana Kübler und Dr. Thomas Wolf arbeiten bei der Endrich Bauelemente Vertriebs GmbH.