FUNKTIONALE SICHERHEIT BEI POWER-FET-ANWENDUNGEN

Mehr Sicherheit durch "Functional Safety"

Die Realisierung von „Functional Safety"-Lösungen nach IEC 61508 und ISO 26262 beeinflusst den gesamten Ablauf vom Entwurf der ICs bis hin zu den Prozessen und Qualitätsmaßnahmen. Der kommende ISO 26262-Standard hat das Ziel, eine vergleichbare und individuelle Risikobewertung für jede Funktion im Automobil zu erreichen. Der Artikel skizziert die Situation bei Mikrocontrollerplattformen und deren Peripherie und geht dann auf den funktionalen Schutz bei Power-FETs ein.

Der überwiegende Teil der zukünftigen Innovationen im Automobil wird durch neue Elektroniksysteme wie z. B. elektronische Lenkung (X-By-Wire), Bremsassistent (BAS), elektronische Differenzialsperre (EDS) oder auch durch komplette elektrische Antriebe (Hybrid-/E-Car) erreicht. Damit steigt auch die Abhängigkeit von einer sicher funktionierenden Elektronik und findet beim Hybrid- oder Elektroauto seinen neuen Höhepunkt. Ständig verbesserte Qualitätsprogramme haben bisher die Zuverlässigkeit trotz steigender Komplexität und einer Vielzahl von elektronischen Subsystemen pro Automobil auf einem hohen Niveau halten können. Der Einsatz der Elektronik in sicherheitsrelevanten Funktionen wie Lenkung, Fahrverhalten oder automatische Bremsung erfordert jedoch, dass diese Abläufe sicher funktionieren und auch beim Auftreten einfacher Fehler keinen Schaden anrichten. Seit 2004 ist aus Haftungsgründen die Anwendung der IEC 61508 zwingend für alle sicherheitsrelevanten Entwicklungen erforderlich. Speziell für den Automobilbereich befindet sich ISO 26262 für „Functional Safety" in der Normung und soll in den kommenden 2 bis 3 Jahren in Kraft treten. Sie hat das Ziel, eine vergleichbare und individuelle Risikobewertung für jede Funktion im Automobil zu dokumentieren.

Eigensichere Hardware

Die Entwicklung sicherer ASIC-/Custom-ICs wird bereits seit Jahren von den Anforderungen der ABS- und Airbag-Systeme geprägt und ist Stand der Technik. Geht es um mikrocontrollerbasierte Plattformen für die Automobilelektronik, so ist die Situation eine andere. **Bild 1** zeigt das allgemeine Blockdiagramm eines elektronischen Steuerteils im Automobil. Neben der Spannungsversorgung aus der Batterie ist der Mikrocontroller die Zentrale für die Verarbeitung der lokalen Sensorsignale, der Kommunikation zu anderen Subsystemen und der Ansteuerung der Aktuatoren über den Leistungsteil. Für sichere Mikrocontroller-Software, Entwicklungsprozessabläufe und Kommunikationssysteme in der Automobilelektronik sind bereits erhebliche Fortschritte mit AUTOSAR, Automotive Spice/CMMI und Flexray erreicht worden. Auch sind bereits einige Mikrocontroller am Markt bzw. bald verfügbar, die ISO 26262 bis ASIL D (Automotive Safety Integrity Level) erreichen sollen. Wenn es um den Entwurf der Hardware geht, so stehen mehrere Bereiche im Fokus: die Spannungsüberwachung sowie die logische und funktionelle Überwachung der Sensoren und Übertragungswege, gefolgt von der fehlersicheren Ansteuerung des Leistungsteils. Die Überwachung der Sensoren kann sowohl hardwaremäßig wie auch logisch durch die Mikrocontroller-Software erreicht werden. Bei

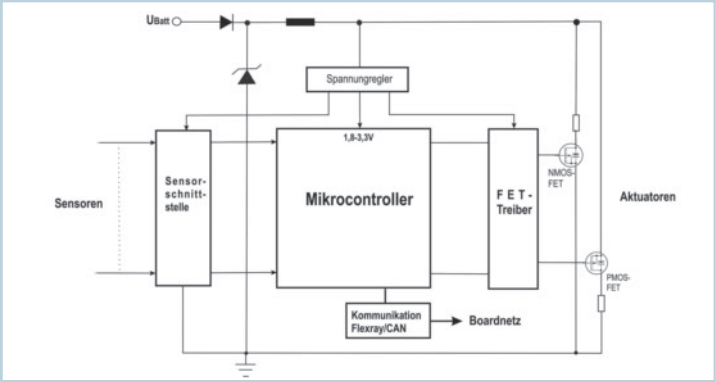

Bild 1: Allgemeines Blockdiagramm der elektronischen Steuereinheit im Automobil.

© automotive

den Übertragungsstrecken helfen geeignete Protokolle Fehler sicher zu erkennen und eventuell zu korrigieren. Der Aufbau von Leistungsendstufen ist eine spezielle Herausforderung, da z. B. eine Redundanz zum Zurücklesen des Aktuatorzustandes sehr kostenintensiv sein kann.

Schnittstelle zwischen MCU und Leistungsteil

Ziel ist es, den Leistungsteil mit den Mikrocontroller-Ausgangssignalen sicher zu betreiben. Der Trend zu immer komplexeren und verlustleistungsärmeren Mikrocontrollern hat kleinere Versorgungsspannungen, geringere Kernspannungen und geringere I/O Spannungen mit geringer Belastbarkeit der Ausgänge zur Folge. I/O-Spannungen von 1,8 V bis 3,3 V bei komplexen Mikrocontrollern sind heute die Regel. Dies widerspricht den steigenden Anforderungen des Leistungsteils, aber auch den langfristigen Planungen für ein 48-V-Bordnetz, um die Ströme - und damit Kabelverluste - zu verringern. Die elektronische Aktivierung z. B. der Lenkung oder der Bremsen, kann im Fehlerfall sehr kritisch sein. ISO 26262 definiert hier die vier Klassen von Risiken (ASIL A bis D). Sie berücksichtigt spezifische Sicherheitsanforderungen und definiert maximal zulässige Ausfallwahrscheinlichkeiten. Auch wird eine Risi-koreduzierung durch eine technische Lösung gefordert. Konkret heißt dies, dass kritische Fehler erkannt werden müssen und Fehlfunktionen aktiv zu verhindern sind. Hier ist die fehlerfreie Ansteuerung der Power-FETs von höchster Bedeutung. Dies gilt natürlich auch für den FET-Treiber, da er das wichtige Bindeglied zwischen der MCU- und der Power-Welt ist. Beim Entwurf des FET-Treibers gilt es, alle Design-Parameter zu erfassen. Typisch sind hier folgende zu nennen:

- Fehlerüberwachung (Verluste von GND oder V_{CC}-Verbindungen zwischen Ausgängen)
- Treiberleistung und Einschaltverhalten (z. B. 3-State der MCU-I/Os)
- Erforderliche Logikpegelverschiebung (z. B. 1,8-5 V auf 5 V bzw. 10 V)
- Verlustleistungsbetrachtungen, Strombelastung und Schaltfrequenze

Bei der Betrachtung der funktionellen Sicherheit des Treibers geht es im Wesentlichen darum, ob Fehler erster Ordnung erkannt werden, und wie die Schaltung reagiert auf:

- Verlust des Masse-Anschlusses durch Defekte auf der Leiterplatte oder in den Komponenten
- Verlust oder Schwankungen der Versorgungsspannung
- Verbindungen/Kurzschlüsse zwischen zwei Ausgängen
- Störimpulse von außen
- Überlastung der Ausgänge und Übertemperatur

FMEA-Nr.: FMFLA1
Project: iC-MFL

Failure-Mode- and Effects-Analysis

iC-Haus

Package: QFN24 | Prepared by: Hz | Last revision date: 10.10.2007 | Page 1 / 12

FM-NR	Potential Effects of Failure	S	Potential Failure Mode	Potential Causes	Current Controls	O	Failure Detection Method	D	RPN
1	no effect	1	PIN 4 GNDR short to GND	Bondwire short to chipedge	SPC assembler	3	SPC assembler; optical inspection, electrical test	2	6
2	all OUTx = resistive lo (< 70 kOhm)	1	PIN 5 VCC open	Bond interruption	SPC assembler; incoming inspection	2	SPC assembler; bond-pull-test, electrical test	1	2
				Poor contact/ poor solderability	SPC assembler; handle chips with care	3	SPC assembler; outgoing inspection, electrical test	1	3
				poor solderpoint	Compilance solderprocess parameters / handle chips with care / monitoring solderprocess	4	Optical inspection, electrical test	1	4
				bond interruption	Compilance solderprocess parameters	3	Electrical test	1	3
			PIN 17 GND open	Bond interruption	SPC assembler; incoming inspection	2	SPC assembler; bond-pull-test, electrical test	1	2
				Poor contact/ poor solderability	SPC assembler; handle chips with care	3	SPC assembler; outgoing inspection, electrical test	1	3
				poor solderpoint	Compilance solderprocess parameters / handle chips with care / monitoring solderprocess	4	Optical inspection, electrical test	1	4
				bond interruption	Compilance solderprocess parameters	3	Electrical test	1	3
			PIN 4 GNDR short to PIN 5 VCC	Touched bondwires	SPC assembler	1	SPC assembler; optical inspection, electrical test	1	1
				Pin misalignment	SPC assembler; handle chips with care	2	SPC assembler; outgoing inspection, electrical test	1	2
				solder bridging on ic pins	Monitoring solderprocess / handle chips with care	3	Optical inspection, electrical test	1	3
			PIN 5 VCC short to GND	Bondwire short to chipedge	SPC assembler	3	SPC assembler; optical inspection, electrical test	2	6
			PIN 17 GND short to VCC	solder bridging on ic pins	Monitoring solderprocess / handle chips with care	3	Optical inspection, electrical test	1	3
			PIN 4 GNDR short to VCC	solder bridging on ic pins	Monitoring solderprocess / handle chips with care	3	Optical inspection, electrical test	1	3
3	all OUTx= active lo (> 2 mA)	1	PIN 15 EN open	Bond interruption	SPC assembler; incoming inspection	2	SPC assembler; bond-pull-test, electrical test	1	2
				Poor contact/ poor solderability	SPC assembler; handle chips with care	3	SPC assembler; outgoing inspection, electrical test	1	3
				poor solderpoint	Compilance solderprocess parameters / handle chips with care / monitoring solderprocess	4	Optical inspection, electrical test	1	4

S = Severity O = Occurrence D = Detection Risk Priority Number RPN = Severity * Occurence * Detection

FMFLA1.doc
Printed: 10.10.07

Bild 2: Auszug aus einer FMEA-Analyse. © automotive

Diese Evaluierung führt automatisch zur FMEA (Failure Mode Effect Analysis). Hier gilt es systematisch die Möglichkeiten und Maßnahmen zu dokumentieren, um eine funktionelle Sicherheit nach IEC 61508 und ISO 26262 zu erreichen.

FMEA-Betrachtungen auf der Treiberebene

Bei der FMEA-Betrachtung geht es darum, zu beschreiben, welche Funktionen das Bauteil erfüllt und welche Fehlfunktionen auftreten können. Es folgt die Analyse von Ursache und Wirkung bei einer Fehlfunktion, sowie eine Bewertung der Bedeutung für das Gesamtprodukt und den Benutzer. Dann muss die Frage beantwortet werden, wie wahrscheinlich diese Fehlfunktion ist. Ebenso, wie sie erkannt und verhindert werden kann, um Folgeschäden zu vermeiden. Diese detaillierten Analysen werden dokumentiert und fließen bei der Entwurfsplanung der integrierten Schaltung mit ein. Natürlich auch in die Produktion, den IC-Test und in die Qualitätssicherung des Produktes. Bild 2 zeigt als Beispiel die erste Seite aus der umfangreichen FMEA-Analyse eines FET-Treibers. Die Vermeidung eines potenziellen Fehlers steht im Vordergrund, aber auch die sichere Erkennung während der Herstellung und im späteren Betrieb (**Bild 2**). Mit der FMEA-Betrachtung erfolgt die Festlegung, welche möglichen Fehler kritisch sind, und wie sie erkannt werden können, bzw. wie ihre Auswirkungen zu verhindern sind. Diese Erkenntnisse beeinflussen direkt das IC-Design.

"Functional Safety" Beispiel eines FET-Treibers

Als ein Beispiel aus einer Familie von sicheren FET-Treibern werden hier bei einem IC-Typ die konkreten Maßnahmen im Detail beschrieben. **Bild 3** zeigt die prinzipielle Ansteuerung eines NMOS-Logic-FET (z. B. IRLZ44N) mit dem iC-MFL als Treiber. Im Fehlerfall muss der IC auf jeden Fall verhindern, dass der NMOS-Logic-FET mit einem Logiksignal aktiviert wird. Der steuernde Ausgang muss also auch bei einem Fehler erster Ordnung auf sicherem LOW-Pegel bleiben. Zu den Grundfunktionen, Pegelverschiebung (von 1,8 V - 3,3 V auf 5 V) und Treibern der Power-FET-Eingänge, sichert das iC-MFL durch sein Design folgende Fehler ab:

- Verlust von Masse oder V_{CC} am IC
- Offene Eingänge (z.B. Leitungsbruch oder 3-State der MCU-I/O-Ports)
- Kurzschluss zwischen zwei Ausgängen

Die kritischste Situation ist der Verlust der Masse oder der Versorgungspannung V_{CC}, da dann bei üblichen FET-Treibern kein sicherer Low-Pegel an den Ausgängen garantiert ist. Es wurde daher neben der traditionellen V_{CC}-Überwachung auch eine Überwachung der Masse im Baustein eingeführt. Bei einer Unterbrechung des Masseanschlusses wären ohne diese Maßnahmen keine definierten Potenzial-Verhältnisse für die interne Logik vorhanden und der externe FET würde über parasitäre Pfade aus dem IC aufgesteuert werden. Daher verfügt der Baustein über zwei Masseanschlüsse (GND und GNDR). Wird ein Anschluss

unterbrochen, so erkennt die Überwachung den Fehler und schaltet die Ausgangsstufen ab. Wird V_{CC} unterbrochen, so werden die Ausgänge ebenfalls definiert durch einen internen Pull-Down-Widerstand von ca. 30 kΩ gegen Masse und damit in den sicheren Betriebszustand gezogen.
Zur Erhöhung der Störsicherheit wurden alle Eingänge mit Schmitt-Trigger-Stufen und Pull-Down-Strömen versehen. Pull-Down-Ströme sichern in der Startphase des Mikrocontrollers, in der alle I/O-Ports im TriState-Zustand sind, einen definierten Eingangszustand des FET-Treibers.
Die Ausgänge des FET-Treibers sind aktive Push/Pull-Stromquellen, wobei die Pull-Seite gegen Masse stärker ist als die Push-Seite. Werden also zwei Ausgänge extern kurzgeschlossen, bei denen der eine einen High-Pegel und der anderen einen Low-Pegel treibt, so „gewinnt" quasi der Low-Treiber und stellt einen Low-Pegel sicher. Die Ausgänge sind zum Schutz vor Störimpulsen überspannungsfest (18 V, 100 ms) ausgelegt.
Für die anderen Einsatzfälle, z. B. PMOS-FET-Ansteuerung, oder für andere Eingangs- und Ausgangsspannungsbereiche wurden ebenfalls FMEA-Analysen durchgeführt, um die gleiche Ein-Fehlersicherheit zu erzielen. Sowohl für NMOS- als auch für PMOS- FETs sind sichere Treiberbausteine mit einem einstellbaren Ausgangsspannungsbereich von 5 V, 10 V und "Full Scale" verfügbar. Das obige Beispiel beschreibt nur die Maßnahmen, die Fehler während des Betriebes absichern und die direkt vom IC-Entwurf beeinflusst werden.

Ausblick

Wie gezeigt beeinflusst die Realisierung von „Functional Safety"-Lösungen nach IEC 61508 und ISO 26262 den gesamten Ablauf vom Entwurf der integrierten Schaltungen bis hin zu den verwendeten Prozessen und Qualitätsmaßnahmen. Sie führt zwangsläufig zu einer abteilungsübergreifenden Teamarbeit und macht die notwendigen Entwicklungsanstrengungen deutlich. Entsprechende Analysen sind in allen anderen Teilbereichen der Elektronik erforderlich. Ähnliches gilt selbstverständlich auf kompletter Systemebene, wie z. B. für die Lenkung oder für Bremssysteme. Es ist zu erwarten, dass sich "Functional Safety" sowohl im Automobilbereich als auch im industriellen Umfeld mehr und mehr als Standard etabliert. (oe)

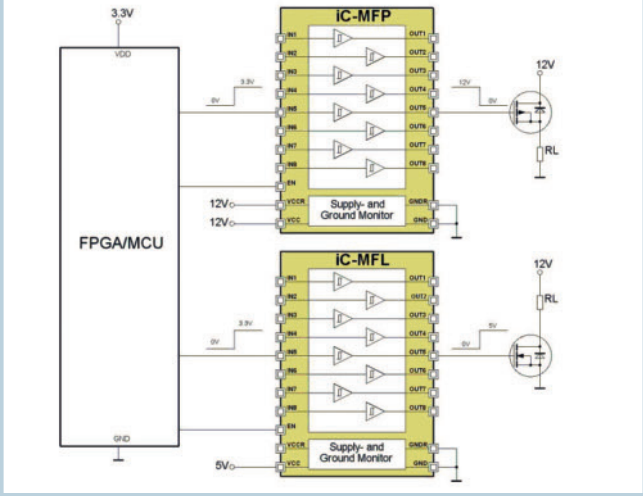

Bild 3: Sichere Power-FET-Ansteuerung. © automotive

Dipl.-Ing. Thomas Franken ist bei der iC-Haus GmbH IC-Entwickler mit dem Schwerpunkt auf FMEA-Design.

@ iCHaus
www.ichaus.de