

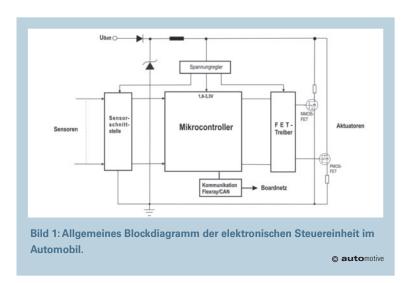
Mehr Sicherheit durch "Functional Safety"

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.

er 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



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

You CAN get it...

Hardware und Software für CAN-Bus-Anwendungen...



www.peak-system.com



Otto-Roehm-Str. 69 4293 Darmstadt / Germany Tel.: +49 6151 8173-29 Fax: +49 6151 8173-29 info@peak-system.com

FMEA-Nr.: FMFLA1 Project: iC-MFL		Failure-Mode- and Effects-Analysis					(CHau		
Pack	kage: QFN24	Prepare	d by: Hz	Last re	vision date: 10.10.2007			Pag	ge
FM- NR	Potential Effects of Failure	S	Potential Failure Mod	le Potential Cause	S Current Controls	0	Failure Detection Method	D	
1	no effect	1	PIN 4 GNDR short to GND	Bondwire short to chipedge	SPC assembler	3	SPC assembler; optical inspection, electrical test	2	
2	all OUTx = resistive lo (< 70 kOhm)		PIN 5 VCC open	Bond interruption	SPC assembler; incoming inspection	2	SPC assembler, bond-pull- test, electrical test	1	T
	(TO KOMI)			Poor contact/ poor solderability	SPC assembler; handle chips with care	3	SPC assembler; outgoing inspection, electrical test	1	T
				poor solderpoint	Compilance solderprocess	4	Optical inspection,	-	\vdash
					parameters / handle chips with care / monitoring solderprocess	4	electrical test	1	L
				bond interruption	Compilance solderprocess parameters	3	Electrical test	1	
			PIN 17 GND open	Bond interruption	SPC assembler; incoming inspection	2	SPC assembler; bond-pull- test, electrical test	1	
				Poor contact/ poor solderability	SPC assembler; handle chips with care	3	SPC assembler, outgoing inspection, electrical test	1	
				poor solderpoint	Compilance solderprocess parameters / handle chips with	4	Optical inspection, electrical test	1	
		1		For Discounting	care / monitoring solderprocess	4		1	_
				bond interruption	Compilance solderprocess parameters	3	Electrical test	1	
			PIN 4 GNDR short to PIN 5 VCC	Touched bondwires	SPC assembler	1	SPC assembler; optical inspection, electrical test	1	
			The second secon	Pin misalignment	SPC assembler; handle chips with care	2	SPC assembler, outgoing inspection, electrical test	1	
				solder bridging on ic pins	Monitoring solderprocess /	3	Optical inspection,	1	T
			PIN 5 VCC short to	Bondwire short to chipedge	handle chips with care SPC assembler	3	SPC assembler, optical	2	
			PIN 17 GND short to	solder bridging on ic pins	Monitoring solderprocess /	3	inspection, electrical test Optical inspection,	1	-
			VCC PIN 4 GNDR short to	solder bridging on ic pins	handle chips with care Monitoring solderprocess /	3	Optical inspection,	1	-
3	all OUTx= active lo	-	VCC PIN 15 EN open	Bond interruption	handle chips with care SPC assembler; incoming		electrical test SPC assembler; bond-pull-		-
5	(> 2 mA)	1		Poor contact/	inspection SPC assembler; handle chips	2	test, electrical test SPC assembler; outgoing	1	-
				poor solderability	with care	3	inspection, electrical test	1	-
				poor solderpoint	Compilance solderprocess parameters / handle chips with care / monitoring solderprocess	4	Optical inspection, electrical test	1	
								(©
	Diese Evaluierung	führt	automatisch zu	r FMEA (Failure	"Functional Sa	fet	y" Beispiel		© 16
	Diese Evaluierung Mode Effect Analys lichkeiten und Mal funktionelle Sicherl erreichen.	führt sis). Hi ßnahm heit na	automatisch zu er gilt es systen en zu dokumer ch IEC 61508 ur	natisch die Mög- ntieren, um eine	FET-Treibers Als ein Beispiel aus e werden hier bei eine im Detail beschriebe	iner em l	Familie von sich C-Typ die konkro Bild 3 zeigt die p	eir nerer eten orinzi	n I pi
	Diese Evaluierung Mode Effect Analys lichkeiten und Mal funktionelle Sicherl erreichen.	führt sis). Hi ßnahm heit na	automatisch zu er gilt es systen en zu dokumer ch IEC 61508 ur	natisch die Mög- ntieren, um eine nd ISO 26262 zu	FET-Treibers Als ein Beispiel aus e werden hier bei eine im Detail beschriebe erung eines NMOS-I	einer em le en. E	Familie von sich C-Typ die konkro Bild 3 zeigt die p c-FET (z.B. IRLZ	eir nerer eten orinzi	n I pi
	Diese Evaluierung Mode Effect Analys lichkeiten und Mal funktionelle Sicherl erreichen. FMEA-Betrace	führt sis). Hi ßnahm heit na	automatisch zu er gilt es systen en zu dokumer ch IEC 61508 ur gen auf dei	natisch die Mög- ntieren, um eine nd ISO 26262 zu	FET-Treibers Als ein Beispiel aus e werden hier bei eine im Detail beschriebe erung eines NMOS-L MFL als Treiber. Im Fe	iner em le en. E ogie	Familie von sich C-Typ die konkro Bild 3 zeigt die p c-FET (z.B. IRLZ rfall muss der IC	eir nerer eten orinzi 744N	n I pi je
	Diese Evaluierung Mode Effect Analys lichkeiten und Mal funktionelle Sicherl erreichen. FMEA-Betrac ebene Bei der EMEA Betra	führt sis). Hi ßnahm heit na	automatisch zu er gilt es systen en zu dokumer ch IEC 61508 ur gen auf der	natisch die Mög- ntieren, um eine nd ISO 26262 zu r Treiber-	FET-Treibers Als ein Beispiel aus e werden hier bei eine im Detail beschriebe erung eines NMOS-I MFL als Treiber. Im Fe hindern, dass der NM	einer em le en. E ogie ehle	Familie von sich C-Typ die konkro Bild 3 zeigt die p c-FET (z. B. IRLZ rfall muss der IC S-Logic-FET mit o	eir nerer eten orinzi 744N auf einer	n I pi J)
	Diese Evaluierung Mode Effect Analys lichkeiten und Mal funktionelle Sicherl erreichen. FMEA-Betrac ebene Bei der FMEA-Betra	führt sis). Hi ßnahm heit na ehtun achtun	automatisch zu er gilt es systen en zu dokumer ch IEC 61508 ur gen auf der g geht es darum	natisch die Mög- ntieren, um eine nd ISO 26262 zu r Treiber- , zu beschreiben,	FET-Treibers Als ein Beispiel aus e werden hier bei eine im Detail beschriebe erung eines NMOS-IMFL als Treiber. Im Fehindern, dass der NM aktiviert wird. Der st	einer em le en. E ogie ehle vios euer	Familie von sich C-Typ die konkro Bild 3 zeigt die p c-FET (z. B. IRLZ rfall muss der IC G-Logic-FET mit o rnde Ausgang m	eir eten eten grinzi 244N auf einer	n I pi J) je m
	Diese Evaluierung Mode Effect Analys lichkeiten und Mal funktionelle Sicherl erreichen. FMEA-Betrac ebene Bei der FMEA-Betrs welche Funktioner	führt sis). Hi ßnahm heit na ehtun achtun	automatisch zu er gilt es systen en zu dokumer ch IEC 61508 ur gen auf der g geht es darum, Bauteil erfüllt u	natisch die Mög- ntieren, um eine nd ISO 26262 zu r Treiber- , zu beschreiben, nd welche Fehl-	FET-Treibers Als ein Beispiel aus e werden hier bei eine im Detail beschriebe erung eines NMOS-I MFL als Treiber. Im Fehindern, dass der NM aktiviert wird. Der steinem Fehler erster O	einer em le en. E ogie hle ehle VOS euel	Familie von sich C-Typ die konkro Bild 3 zeigt die p c-FET (z. B. IRLZ rfall muss der IC B-Logic-FET mit o rnde Ausgang m rung auf sicherer	eir nerer eten orinzi 744N auf einer nuss m LC	n I pi je m a
	Diese Evaluierung Mode Effect Analys lichkeiten und Mal funktionelle Sicherl erreichen. FMEA-Betrac ebene Bei der FMEA-Betrs welche Funktioner funktionen auftrete	führt sis). Hi ßnahm heit na ehtun achtun n das	automatisch zu er gilt es systen en zu dokumer ch IEC 61508 ur gen auf der g geht es darum, Bauteil erfüllt u en. Es folgt die A	natisch die Mög- ntieren, um eine nd ISO 26262 zu r Treiber- , zu beschreiben, nd welche Fehl- Analyse von Ursa-	FET-Treibers Als ein Beispiel aus ein Werden hier bei eine im Detail beschriebe erung eines NMOS-LMFL als Treiber. Im Fehindern, dass der NM aktiviert wird. Der steinem Fehler erster üben. Zu den Grund	einer em le en. E ogie ehle ordo Ordo Ifunl	Familie von sich C-Typ die konkro Bild 3 zeigt die p c-FET (z. B. IRLZ rfall muss der IC B-Logic-FET mit o rnde Ausgang m rung auf sicherer ktionen, Pegelv	eir eten eten grinzi Z44N auf einer nuss m LC	n I pi J) je m a DV
	Diese Evaluierung Mode Effect Analys lichkeiten und Mal funktionelle Sicherl erreichen. FMEA-Betrac ebene Bei der FMEA-Betrs welche Funktioner funktionen auftrete che und Wirkung be	führt sis). Hi ßnahm heit na ehtun achtun n das n könn ei einer	automatisch zu er gilt es systen en zu dokumer ch IEC 61508 ur gen auf der g geht es darum, Bauteil erfüllt u en. Es folgt die A	natisch die Mög- ntieren, um eine nd ISO 26262 zu r Treiber- , zu beschreiben, nd welche Fehl- Analyse von Ursa- owie eine Bewer-	FET-Treibers Als ein Beispiel aus ein Werden hier bei eine im Detail beschriebe erung eines NMOS-LMFL als Treiber. Im Fehindern, dass der NM aktiviert wird. Der steinem Fehler erster üben. Zu den Grund 1,8 V - 3,3 V auf 5 V)	em len. E en. E Logie MOS euer Drdn Ifund	Familie von sich C-Typ die konkro Sild 3 zeigt die p c-FET (z. B. IRLZ rfall muss der IC S-Logic-FET mit of rnde Ausgang m rung auf sicherer ktionen, Pegelv Treibern der Pov	eir nerer eten vrinzi Z44N auf einer nuss m LC ersc wer-f	n I pi je m a DV
	Diese Evaluierung Mode Effect Analys lichkeiten und Mal funktionelle Sicherl erreichen. FMEA-Betrac ebene Bei der FMEA-Betrs welche Funktioner funktionen auftrete che und Wirkung be tung der Bedeutung	führt sis). Hi ßnahm heit na ehtun achtun n das n könn ei einer g für da	automatisch zu er gilt es systen en zu dokumer ch IEC 61508 ur gen auf der geht es darum, Bauteil erfüllt uen. Es folgt die Ar Fehlfunktion, so s Gesamtproduk	natisch die Mög- ntieren, um eine nd ISO 26262 zu r Treiber- , zu beschreiben, nd welche Fehl- Analyse von Ursa- owie eine Bewer-	FET-Treibers Als ein Beispiel aus ein Werden hier bei eine im Detail beschriebe erung eines NMOS-LMFL als Treiber. Im Fehindern, dass der NM aktiviert wird. Der steinem Fehler erster üben. Zu den Grund 1,8 V - 3,3 V auf 5 V) sichert das iC-MFL d	em leen. E en. E Logie HOS euer Drdn Urdn und	Familie von sich C-Typ die konkro Sild 3 zeigt die p c-FET (z. B. IRLZ rfall muss der IC S-Logic-FET mit of rnde Ausgang m rung auf sicherer ktionen, Pegelv Treibern der Povansein Design fol	eir nerer eten vrinzi Z44N auf einer nuss m LC ersc wer-f	n I pi je m a DV
	Diese Evaluierung Mode Effect Analys lichkeiten und Mal funktionelle Sicherl erreichen. FMEA-Betrac ebene Bei der FMEA-Betra welche Funktioner funktionen auftrete che und Wirkung be tung der Bedeutung zer. Dann muss die	führt sis). Hi ßnahm heit na achtun achtun könn ei einer g für da	automatisch zu er gilt es systen en zu dokumer ch IEC 61508 ur gen auf der geht es darum, Bauteil erfüllt uen. Es folgt die Ar Fehlfunktion, so s Gesamtproduk beantwortet we	natisch die Mög- ntieren, um eine nd ISO 26262 zu r Treiber- , zu beschreiben, nd welche Fehl- Analyse von Ursa- owie eine Bewer- ct und den Benut-	FET-Treibers Als ein Beispiel aus ein Werden hier bei eine im Detail beschriebe erung eines NMOS-LMFL als Treiber. Im Fehindern, dass der NM aktiviert wird. Der steinem Fehler erster üben. Zu den Grund 1,8 V - 3,3 V auf 5 V) sichert das iC-MFL d	em leen. E en. E Logie HOS euer Drdn Urdn und	Familie von sich C-Typ die konkro Sild 3 zeigt die p c-FET (z. B. IRLZ rfall muss der IC S-Logic-FET mit of rnde Ausgang m rung auf sicherer ktionen, Pegelv Treibern der Povansein Design fol	eir nerer eten vrinzi Z44N auf einer nuss m LC ersc wer-f	n N pi je m a DV:hii
	Diese Evaluierung Mode Effect Analys lichkeiten und Mal funktionelle Sicherl erreichen. FMEA-Betrace ebene Bei der FMEA-Betra welche Funktioner funktionen auftrete che und Wirkung be tung der Bedeutung zer. Dann muss die scheinlich diese Fe und verhindert wer	führt sis). Hi sis). Hi sis). Hi sis nahm heit na achtun achtun ei einer g für da er Frage ehlfunk rden ka	automatisch zu er gilt es systen en zu dokumer ch IEC 61508 ur gen auf der geht es darum. Bauteil erfüllt ur en. Es folgt die Ar Fehlfunktion, so s Gesamtproduk beantwortet wetion ist. Ebenso, nn, um Folgesch	natisch die Mög- ntieren, um eine nd ISO 26262 zu r Treiber- , zu beschreiben, nd welche Fehl- Analyse von Ursa- owie eine Bewer- et und den Benut- erden, wie wahr- , wie sie erkannt näden zu vermei-	FET-Treibers Als ein Beispiel aus ein Werden hier bei eine im Detail beschriebe erung eines NMOS-LMFL als Treiber. Im Fehindern, dass der NM aktiviert wird. Der st einem Fehler erster (ben. Zu den Grund 1,8 V - 3,3 V auf 5 V) sichert das iC-MFL der Verlust von Massen Offene Eingänge MCU-I/O-Ports)	em lennem	Familie von sich C-Typ die konkrusten Geren die konkrusten Geren die konkrusten Geren die Population der V _{CC} am IC B. Leitungsbruch Geren der V _{CC} am IC B. Leitungsbruch	eir nerer eten orinzi Z44N auf j einer nuss m LC ersc wer-F lgen on ode	n I pi je m a DV hi
	Diese Evaluierung Mode Effect Analys lichkeiten und Mal funktionelle Sicherl erreichen. FMEA-Betrac ebene Bei der FMEA-Betrac welche Funktioner funktionen auftrete che und Wirkung be tung der Bedeutung zer. Dann muss die scheinlich diese Fe und verhindert wer den. Diese detailli und fließen bei der	führt sis). Hi sis). Hi sis). Hi sis). Hi sis heit na chtun achtun ei einer g für da e Frage chlfunkteten Entwu	automatisch zu er gilt es systen en zu dokumer ch IEC 61508 ur gen auf der geht es darum. Bauteil erfüllt ur en. Es folgt die Ar Fehlfunktion, so s Gesamtproduk beantwortet wetion ist. Ebenso, nn, um Folgesch Analysen werderfsplanung der in alle in die Arien en zu dokumen.	natisch die Mög- ntieren, um eine nd ISO 26262 zu r Treiber- , zu beschreiben, nd welche Fehl- Analyse von Ursa- owie eine Bewer- kt und den Benut- erden, wie wahr- , wie sie erkannt näden zu vermei- en dokumentiert ntegrierten Schal-	FET-Treibers Als ein Beispiel aus ein Werden hier bei eine im Detail beschriebe erung eines NMOS-LMFL als Treiber. Im Fehindern, dass der NM aktiviert wird. Der steinem Fehler erster üben. Zu den Grund 1,8 V - 3,3 V auf 5 V) sichert das iC-MFL der Verlust von Massen Offene Eingänge MCU-I/O-Ports) Kurzschluss zwis	em len. E cogic euer Drdn lfunl fund urch se oc (z.E	Familie von sich C-Typ die konkro G-Typ die konkro G-Typ die konkro G-Typ die personen G-Logic-FET mit of G-Logic-FET mit of rade Ausgang mung auf sicherer ktionen, Pegelv Treibern der Pool sein Design folder V _{CC} am IC G-Typ die G-Typ	eir nerer eten prinzi Z44N auf einer nuss m LC ersc wer-f gend	n I pi
	Diese Evaluierung Mode Effect Analys lichkeiten und Mal funktionelle Sicherl erreichen. FMEA-Betrac ebene Bei der FMEA-Betrac welche Funktioner funktionen auftrete che und Wirkung be tung der Bedeutung zer. Dann muss die scheinlich diese Fe und verhindert wer den. Diese detailli und fließen bei der tung mit ein. Natür	führt sis). Hi sis). Hi sis). Hi sis). Hi sis heit na schtun achtun ei einer g für da e Frage shlfunkten kaierten Entwulich au	automatisch zu er gilt es systen en zu dokumer ch IEC 61508 ur gen auf der gen auf der geht es darum. Bauteil erfüllt ur en. Es folgt die Arehlfunktion, so s Gesamtproduk beantwortet wetion ist. Ebenso, nn, um Folgesch Analysen werderfsplanung der ir ch in die Produk	natisch die Mög- ntieren, um eine nd ISO 26262 zu r Treiber- , zu beschreiben, nd welche Fehl- analyse von Ursa- owie eine Bewer- kt und den Benut- erden, wie wahr- wie sie erkannt näden zu vermei- en dokumentiert ntegrierten Schal- ttion, den IC-Test	FET-Treibers Als ein Beispiel aus ein Werden hier bei eine im Detail beschriebe erung eines NMOS-IMFL als Treiber. Im Fehindern, dass der NM aktiviert wird. Der steinem Fehler erster üben. Zu den Grund 1,8 V - 3,3 V auf 5 V) sichert das iC-MFL der Verlust von Massen Offene Eingänge MCU-I/O-Ports) Kurzschluss zwisten.	iner len. E Logid Logi	Familie von sich C-Typ die konkro G-Typ die konkro Gild 3 zeigt die po-c-FET (z. B. IRLZ rfall muss der IC G-Logic-FET mit orrnde Ausgang mung auf sicherer ktionen, Pegelv Treibern der Pool sein Design folder V _{CC} am IC G. Leitungsbruch zwei Ausgängest der Verlust der St. Leitungsbruch st. der Verlust der	eir nerereten orinzi Z44N auf einer einer wer-F dgena n ode en	n N pi N p
	Diese Evaluierung Mode Effect Analys lichkeiten und Mal funktionelle Sicherl erreichen. FMEA-Betrac ebene Bei der FMEA-Betrac welche Funktioner funktionen auftrete che und Wirkung be tung der Bedeutung zer. Dann muss die scheinlich diese Fe und verhindert wer den. Diese detailli und fließen bei der tung mit ein. Natür und in die Qualitäts	führt sis). Hi ßnahm heit na schtun achtun das e Frage ehlfunkten kaierten Entwu sicherusischerus	automatisch zu er gilt es systen en zu dokumer ch IEC 61508 ur gen auf der gen auf der geht es darum. Bauteil erfüllt ur en. Es folgt die Ar Fehlfunktion, so s Gesamtproduk beantwortet wetion ist. Ebenso, nn, um Folgesch Analysen werderfsplanung der inch in die Produkting des Produkter	natisch die Mögnitieren, um eine nd ISO 26262 zu r Treiber- , zu beschreiben, nd welche Fehlmalyse von Ursabwie eine Bewerkt und den Benuterden, wie wahrt, wie sie erkannt näden zu vermeiten dokumentiert integrierten Schaltion, den IC-Test es. Bild 2 zeigt als	FET-Treibers Als ein Beispiel aus ein werden hier bei eine im Detail beschriebe erung eines NMOS-IMFL als Treiber. Im Fehindern, dass der NM aktiviert wird. Der steinem Fehler erster (ben. Zu den Grund 1,8 V - 3,3 V auf 5 V) sichert das iC-MFL der Verlust von Massen Offene Eingänge MCU-I/O-Ports) Kurzschluss zwisten.	iner len . E Logic Logic MOS euer Drdn lfund urch se oc (z.E cher ion i	Familie von sich C-Typ die konkro G-Typ die konkro Gild 3 zeigt die po-c-FET (z. B. IRLZ rfall muss der IC G-Logic-FET mit ornde Ausgang mung auf sicherer ktionen, Pegelv Treibern der Pool sein Design folder V _{CC} am IC G. Leitungsbruch zwei Ausgängest der Verlust der C, da dann bei	eir nerer eten prinzi Z44N auf einer nuss m LC ersc wer-F lgen o ode en	n I pi je m a DV shi FE de er
	Diese Evaluierung Mode Effect Analys lichkeiten und Mal funktionelle Sicherl erreichen. FMEA-Betrac ebene Bei der FMEA-Betrac welche Funktioner funktionen auftrete che und Wirkung be tung der Bedeutung zer. Dann muss die scheinlich diese Fe und verhindert wer den. Diese detailli und fließen bei der tung mit ein. Natür und in die Qualitäts Beispiel die erste S	führt sis). Hi ßnahm heit na schtun achtun das e Frage ehlfunkten kaierten Entwu sicheruseite au	automatisch zu er gilt es systen en zu dokumer ch IEC 61508 ur gen auf der gen auf der geht es darum. Bauteil erfüllt ur en. Es folgt die Ar Fehlfunktion, so s Gesamtproduk beantwortet wetion ist. Ebenso, nn, um Folgesch Analysen werderfsplanung der in ch in die Produkting des Produkters der umfangreie	natisch die Mögnitieren, um eine nd ISO 26262 zu r Treiber- , zu beschreiben, nd welche Fehlmalyse von Ursabwie eine Bewerkt und den Benuterden, wie wahrt, wie sie erkannt näden zu vermeiten dokumentiert integrierten Schaltion, den IC-Test es. Bild 2 zeigt als	FET-Treibers Als ein Beispiel aus ein Werden hier bei eine im Detail beschriebe erung eines NMOS-IMFL als Treiber. Im Fehindern, dass der NM aktiviert wird. Der steinem Fehler erster üben. Zu den Grund 1,8 V - 3,3 V auf 5 V) sichert das iC-MFL der Verlust von Massen Offene Eingänge MCU-I/O-Ports) Kurzschluss zwisten.	iner len . E Logic Logic MOS euer Drdn lfund urch se oc (z.E cher ion i	Familie von sich C-Typ die konkro G-Typ die konkro Gild 3 zeigt die po-c-FET (z. B. IRLZ rfall muss der IC G-Logic-FET mit ornde Ausgang mung auf sicherer ktionen, Pegelv Treibern der Pool sein Design folder V _{CC} am IC G. Leitungsbruch zwei Ausgängest der Verlust der C, da dann bei	eir nerer eten prinzi Z44N auf einer nuss m LC ersc wer-F lgen o ode en	n I pi je m a DV shi FE de er
	Diese Evaluierung Mode Effect Analys lichkeiten und Mal funktionelle Sicherl erreichen. FMEA-Betrac ebene Bei der FMEA-Betrac welche Funktioner funktionen auftrete che und Wirkung be tung der Bedeutung zer. Dann muss die scheinlich diese Fe und verhindert wer den. Diese detailli und fließen bei der tung mit ein. Natür und in die Qualitäts Beispiel die erste S lyse eines FET-Treib	führt sis). Hi ßnahm heit na schtun achtun das e Frage ehlfunkten kaierten Entwu sichert aubers. D	automatisch zu er gilt es systen en zu dokumer ch IEC 61508 ur gen auf der gen auf der geht es darum. Bauteil erfüllt ur en. Es folgt die Ar Fehlfunktion, so s Gesamtproduk beantwortet wetion ist. Ebenso, nn, um Folgesch Analysen werderfsplanung der in ch in die Produkting des Produktes der umfangreie vermeidung ei	natisch die Mögntieren, um eine nd ISO 26262 zu r Treiber- , zu beschreiben, nd welche Fehlanalyse von Ursabwie eine Bewerkt und den Benuterden, wie wahrt, wie sie erkannt näden zu vermeiten dokumentiert integrierten Schaltion, den IC-Test es. Bild 2 zeigt als chen FMEA-Ana-	FET-Treibers Als ein Beispiel aus ein werden hier bei eine im Detail beschriebe erung eines NMOS-L MFL als Treiber. Im Fehindern, dass der NM aktiviert wird. Der st einem Fehler erster (ben. Zu den Grund 1,8 V - 3,3 V auf 5 V) sichert das iC-MFL d Verlust von Mass Offene Eingänge MCU-I/O-Ports) Kurzschluss zwis Die kritischste Situat Versorgungspannung bern kein sicherer Lo	iner len. E Logic len. E Logic len. E Logic len. E Logic len	Familie von sich C-Typ die konkrostid 3 zeigt die po-FET (z. B. IRLz rfall muss der IC S-Logic-FET mit ornde Ausgang mung auf sicherer ktionen, Pegelv Treibern der Pool sein Design folder V _{CC} am IC 3. Leitungsbruch zwei Ausgängest der Verlust der C _C , da dann bei egel an den Aus	eir nerereten orinzi Z44N auf jeinen sum LC ersc wer-F lgend n ode en	n No pin No pin
	Diese Evaluierung Mode Effect Analys lichkeiten und Mal funktionelle Sicherl erreichen. FMEA-Betrac ebene Bei der FMEA-Betrac welche Funktioner funktionen auftrete che und Wirkung be tung der Bedeutung zer. Dann muss die scheinlich diese Fe und verhindert wer den. Diese detailli und fließen bei der tung mit ein. Natür und in die Qualitäts Beispiel die erste S lyse eines FET-Treib Fehlers steht im Vo	führt sis). Hi ßnahm heit na schtun achtun das lenerg für da e Frage ehlfunk den ka ierten Entwu lich au sichert au bers. Dordergrift der grift der grif	automatisch zu er gilt es systen en zu dokumer ch IEC 61508 ur gen auf der gen auf der geht es darum. Bauteil erfüllt ur en. Es folgt die Ar Fehlfunktion, so s Gesamtproduk beantwortet wetion ist. Ebenso, nn, um Folgesch Analysen werderfsplanung der inch in die Produkting des Produkteis der umfangreie vermeidung ei und, aber auch d	natisch die Mög- ntieren, um eine nd ISO 26262 zu r Treiber- , zu beschreiben, nd welche Fehl- Analyse von Ursa- owie eine Bewer- et und den Benut- erden, wie wahr- , wie sie erkannt näden zu vermei- en dokumentiert ntegrierten Schal- tion, den IC-Test es. Bild 2 zeigt als chen FMEA-Ana- ines potenziellen	FET-Treibers Als ein Beispiel aus ein Werden hier bei eine im Detail beschriebe erung eines NMOS-I MFL als Treiber. Im Fehindern, dass der NM aktiviert wird. Der st einem Fehler erster üben. Zu den Grund 1,8 V - 3,3 V auf 5 V) sichert das iC-MFL d Verlust von Mass Offene Eingänge MCU-I/O-Ports) Kurzschluss zwis Die kritischste Situat Versorgungspannung bern kein sicherer Loist. Es wurde daher in	iner len. E Cogiciente MOS euer Drand uurch (z.E cher ion i	Familie von sich C-Typ die konkro G-Typ	eir nerereten orinzi Z44N auf jeiner nuss m LC eersco wer-Figeno n ode en	n I N N N N N N N N N N N N N N N N N N
	Diese Evaluierung Mode Effect Analys lichkeiten und Mal funktionelle Sicherl erreichen. FMEA-Betrac ebene Bei der FMEA-Betrac welche Funktioner funktionen auftrete che und Wirkung be tung der Bedeutung zer. Dann muss die scheinlich diese Fe und verhindert wer den. Diese detailli und fließen bei der tung mit ein. Natür und in die Qualitäts Beispiel die erste S lyse eines FET-Treib Fehlers steht im Vo	führt sis). Hi ßnahm heit na schtun achtun das len könnei einer gfür da erten Entwu lich au sicheru bers. Dordergrift Herst	automatisch zu er gilt es system en zu dokumer ch IEC 61508 ur gen auf der gen auf der geht es darum. Bauteil erfüllt ur en. Es folgt die Ar Fehlfunktion, so s Gesamtproduk beantwortet wetton ist. Ebenso, nn, um Folgesch Analysen werderfsplanung der in ch in die Produkting des Produkters der umfangreigie Vermeidung ei und, aber auch die ellung und im Gellung und Gellung und im Gellung und Gell	natisch die Mögnitieren, um eine nd ISO 26262 zu r Treiber- , zu beschreiben, nd welche Fehlanalyse von Ursabwie eine Bewerkt und den Benuterden, wie wahrt, wie sie erkannt näden zu vermeien dokumentiert ntegrierten Schaltion, den IC-Test es. Bild 2 zeigt als chen FMEA-Anaines potenziellen die sichere Erken-	Als ein Beispiel aus ein Werden hier bei eine im Detail beschriebe erung eines NMOS-L MFL als Treiber. Im Fehindern, dass der NM aktiviert wird. Der steinem Fehler erster üben. Zu den Grund 1,8 V - 3,3 V auf 5 V) sichert das iC-MFL der Verlust von Massen Offene Eingängen MCU-I/O-Ports) Kurzschluss zwisten Kein sicherer Losist. Es wurde daher in chung auch eine Über	em len. E Cogiciente MOS euer MOS euer Drant leund urch se och con ion i VC w-P neberwa	Familie von sich C-Typ die konkro G-Typ	eir nerer eten prinzi Z44N auf j einer nuss m LC ersci wer-f gend n ode en üblik egäng illen n	nn I N N N N N N N N N N N N N N N N N N
	Diese Evaluierung Mode Effect Analys lichkeiten und Mal funktionelle Sicherl erreichen. FMEA-Betrac ebene Bei der FMEA-Betrac welche Funktioner funktionen auftrete che und Wirkung be tung der Bedeutung zer. Dann muss die scheinlich diese Fe und verhindert wer den. Diese detailli und fließen bei der tung mit ein. Natür und in die Qualitäts Beispiel die erste S lyse eines FET-Treib Fehlers steht im Vo nung während der	führt sis). Hi ßnahm heit na ehtun achtun achtun ei einer gfür da e Frage ehlfunk den kalerten Entwu eite au bers. Dordergright Herst	automatisch zu er gilt es system en zu dokumer ch IEC 61508 ur gen auf der gen auf der geht es darum. Bauteil erfüllt ur en. Es folgt die Ar Fehlfunktion, so s Gesamtproduk beantwortet wetton ist. Ebenso, nn, um Folgesch Analysen werderfsplanung der in ch in die Produkting des Produkters der umfangreigie Vermeidung ei und, aber auch die ellung und im statzechtung erfolgen.	r Treiber- , zu beschreiben, nd welche Fehl- analyse von Ursa- bwie eine Bewer- kt und den Benut- erden, wie wahr- , wie sie erkannt näden zu vermei- en dokumentiert ntegrierten Schal- ttion, den IC-Test es. Bild 2 zeigt als chen FMEA-Ana- ines potenziellen lie sichere Erken- späteren Betrieb	Als ein Beispiel aus ein Werden hier bei eine im Detail beschriebe erung eines NMOS-L MFL als Treiber. Im Fehindern, dass der NM aktiviert wird. Der steinem Fehler erster üben. Zu den Grund 1,8 V - 3,3 V auf 5 V) sichert das iC-MFL der Verlust von Massen Offene Eingänge MCU-I/O-Ports) Kurzschluss zwisten Kein sicherer Lotist. Es wurde daher in chung auch eine Übegeführt. Bei einer Ur	em len. Een. Een. Een. Een. Een. Een. Een. E	Familie von sich C-Typ die konkro G-Typ die konkro Gild 3 zeigt die poperen in Sild 3 zeigt die poperen in zwei Ausgängen in	eir nerer eten prinzi Z44N auf j einer nuss m LC ersc wer-f lgend ublid egan üblid egan wer-f ublid sgän eeiner Mass	nn I N N N N N N N N N N N N N N N N N N
	Mode Effect Analystichkeiten und Mal funktionelle Sicherlerreichen. FMEA-Betracebene Bei der FMEA-Betracebene Bei der FMEA-Betracebene Bei der FMEA-Betracebene Gebene Bei der FMEA-Betracebene Gebene Bei der FMEA-Betracebene Gebene G	führt sis). Hi ßnahm heit na schtung achtung den kan könne einerg für da erten Entwuglich au sicheru deite au bers. Dordergricht aus der Schlasse Eablasse E	automatisch zu er gilt es system en zu dokumer ch IEC 61508 ur gen auf der gen auf der geht es darum. Bauteil erfüllt ur en. Es folgt die Ar Fehlfunktion, so s Gesamtproduk beantwortet wetton ist. Ebenso, nn, um Folgesch Analysen werderfsplanung der in ch in die Produkting des Produkters der umfangreigie Vermeidung eind, aber auch die ellung und im setrachtung erfolg kritisch sied und deligen ein der der der geroop gestellt was der	r Treiber- , zu beschreiben, nd welche Fehl- analyse von Ursa- bwie eine Bewer- at und den Benut- erden, wie wahr- wie sie erkannt näden zu vermei- en dokumentiert integrierten Schal- tion, den IC-Test es. Bild 2 zeigt als chen FMEA-Ana- ines potenziellen lie sichere Erken- späteren Betrieb t die Festlegung,	Als ein Beispiel aus ein Werden hier bei eine im Detail beschriebe erung eines NMOS-L MFL als Treiber. Im Fehindern, dass der NM aktiviert wird. Der steinem Fehler erster üben. Zu den Grund 1,8 V - 3,3 V auf 5 V) sichert das iC-MFL der Verlust von Massen Offene Eingängen MCU-I/O-Ports) Kurzschluss zwisten Kein sicherer Losist. Es wurde daher in chung auch eine Über	em len. Een. Een. Een. Een. Een. Een. Een. E	Familie von sich C-Typ die konkro G-Typ die Konde Ausgang mang auf sicherer ktionen, Pegelv Treibern der Poor sein Design folder V _{CC} am IC G-Typ die Konkro G	eir nerer eten prinzi Z44N auf j einer nuss m LC ersc wer-F lgend ublid gäng verime im Mass efinice	n (

FMEA-Betrachtungen auf der Treiber-

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 $V_{\rm CC}$ 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 k Ω gegen Masse und damit in den sicheren Betriebszustand gezogen.

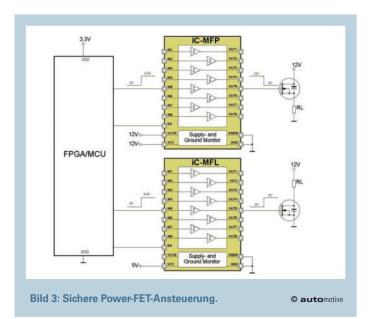
Zur Erhöhung der Störsicherheit wurden alle Eingänge mit Schmitt-Trigger-Stufen und Pull-Down-Strömen versehen. Pull-Down-Ströme sichern in der Startphase des Mikrocontrollers, in der alle I/O-Ports im TriState-Zustand sind, einen definierten Eingangszustand des FET-Treibers.

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)



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



Simulation - Prüftechnik - Versuchsauswertung 7. Technologietag "Prüfstandskonzepte in der Automobilindustrie"

Am 26. Mai 2009 im CongressPark Wolfsburg



Der NI-Technologietag bietet Ihnen:

- ein hochkarätiges Vortragsprogramm
- zwei begleitende Workshops
- eine umfangreiche Fachausstellung

Diskutieren Sie mit NI-Experten sowie zahlreichen Ausstellern und Fachkollegen und holen Sie sich neue Impulse für Ihre Aufgabenstellungen! Die Teilnahme an der ganztägigen Veranstaltung ist kostenfrei.

Agenda und kostenfreie Anmeldung: ni.com/germany/automotivetag

National Instruments Germany GmbH Konrad-Celtis-Str. 79 • 81369 München Tel.: 089 7413130 • Fax: 089 7146035 ni.com/germany • info.germany@ni.com

