

Segurança Funcional em Aplicações com FETs de Potência

Eng. Thomas Franken, iC-Haus GmbH
Tradução: William Salomão, iC-BR Microelectronics
www.iC-BR.com

10 de Fevereiro de 2012

Sistemas eletrônicos automotivos críticos em segurança exigem que sua operação seja sistematicamente analisada e documentada. Nesse âmbito, o padrão ISO 26262 para “Segurança Funcional” tem como objetivo realizar uma avaliação de risco mensurável e individual para cada função do veículo. Este artigo esboça a situação das plataformas baseadas em microcontroladores e seus periféricos, para então se aprofundar na segurança funcional de aplicações com FETs de potência. Um exemplo atual ilustra como uma análise de segurança FMEA deve ser conduzida, desde o projeto do CI, para se obter a “Segurança Funcional” de um driver FET. Os princípios desse exemplo podem ser aplicados a outros sistemas críticos em segurança, como, por exemplo, em máquinas industriais.

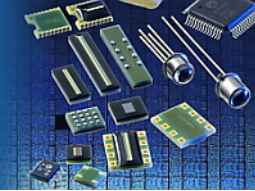
Mais segurança através da “Segurança Funcional”

As principais inovações automobilísticas do futuro se tornarão realidade através de novos sistemas eletrônicos, como a direção eletrônica (X-By-Wire), a assistência de frenagem (BAS) e o bloqueio eletrônico do diferencial (EDS), ou através de sistemas de tração híbridos/elétricos. Com isso, aumenta a necessidade de se desenvolver uma eletrônica de funcionamento seguro, sobretudo nos carros híbridos e elétricos. Programas de qualidade constantemente aprimorados garantiram a manutenção de um alto nível de confiabilidade na indústria automotiva, apesar do aumento da complexidade e da quantidade de subsistemas eletrônicos nos veículos. Contudo, o uso da eletrônica em funções críticas em segurança, como direção, comportamento dinâmico ou frenagem automática, exige que esses processos funcionem de forma segura, evitando a incidência de danos

mesmo na ocorrência de falhas simples. Desde 2004 na Alemanha, é obrigatória a implementação da norma IEC 61508 para funções críticas em segurança. Especificamente para a indústria automotiva, há o padrão ISO 26262 para “Segurança Funcional”, que deve ser adotado com força nos próximos anos. Seu objetivo é realizar e documentar uma avaliação de risco mensurável e individual para cada função do veículo.

Hardware seguro

O desenvolvimento de CIs customizados (ASICs) para aplicações críticas em segurança atingiu status de tecnologia de ponta, em parte, graças aos requisitos dos sistemas de airbag e ABS. A situação é outra, contudo, quando se trata de plataformas para eletrônica automotiva baseadas em microcontroladores. A figura 1 apresenta um diagrama de blocos genérico para um módulo de controle eletrônico veicular. O microcontrolador é responsável pelo processamento dos sinais de sensores, da comunicação com outros subsistemas e do acionamento de atuadores, através dos circuitos de potência. Ferramentas como AUTOSAR[1], Spice Automotivo/CMMI[2] e Flexray[3, 4] representaram grandes progressos para a segurança em softwares de microcontroladores, processos de desenvolvimento e sistemas de comunicação. Além disso, há no mercado microcontroladores que implementam o padrão ISO 26262 até sua especificação ASIL D (*Automotive Safety Integrity Level*). Contudo, no projeto de hardware, deve-se levar em conta considerações extras, como o monitoramento da tensão de alimentação, a observação lógica e funcional de sensores e linhas de transmissão, além do acionamento livre de falhas dos circuitos de potência. O monitoramento de sensores pode ser feito tanto via hardware quanto



software, através do microcontrolador, e o uso de protocolos adequados permite a identificação e eventualmente a correção de erros na transmissão de dados. Já no que se refere aos circuitos de potência, os requerimentos são especiais, já que, por exemplo, a implementação de redundância na leitura dos estados dos atuadores pode ser extremamente custosa.

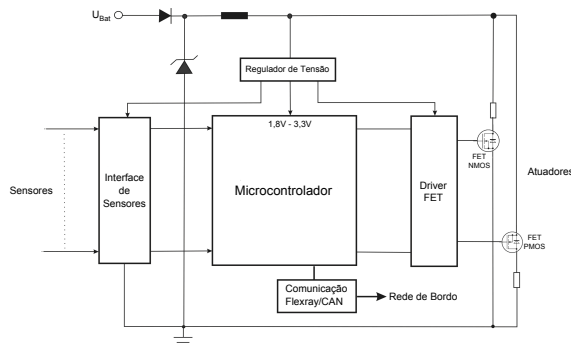


Figura 1: Diagrama de blocos genérico para um módulo de controle eletrônico veicular

Interface entre o MCU e os circuitos de potência

O objetivo desse interfaceamento é acionar de forma segura os circuitos de potência a partir das saídas do microcontrolador (MCU). A tendência de se projetarem microcontroladores cada vez mais complexos e eficientes resultou em componentes com tensões de alimentação, operação e I/O menores. Valores entre 1,8 V e 3,3 V são hoje regra para microcontroladores complexos, o que vai diretamente de encontro aos requerimentos cada vez mais intensivos dos circuitos de potência, bem como ao plano de longo prazo de se usar uma rede de 48 V a bordo, a fim de se reduzirem as correntes e, conseqüentemente, as perdas na transmissão. Por sua vez, o acionamento eletrônico da direção ou dos freios, por exemplo, pode ser extremamente crítico na ocorrência de falhas. Com isso em vista, o ISO 26262 define quatro classes de risco (ASIL A até D)[2]. O padrão observa requerimentos de segurança específicos e define probabilidades máximas de ocorrência de falhas, buscando uma solução técnica para reduzir os riscos envolvidos. De forma concreta, isso significa

que falhas críticas devem ser detectadas e defeitos, evitados de forma ativa. Neste caso, o acionamento livre de falhas dos FETs de potência é essencial. O mesmo vale para o driver FET, que é responsável pelo interfaceamento entre o MCU e os circuitos de potência. Assim, no projeto do driver FET, diversos parâmetros devem ser levados em conta, dentre os quais:

- Monitoramento de falhas (perda de conexão com terra ou V_{CC} , curto-circuito entre saídas)
- Desempenho do driver e comportamento de inicialização (ex.: I/O do MCU em tri-state)
- Conversão de nível necessária (ex.: 1,8-5 V para 5 V ou 10 V)
- Potência dissipada, consumo de corrente e frequência de chaveamento

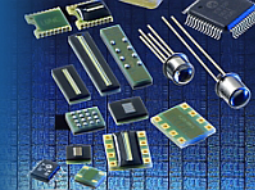
Quanto à segurança funcional do driver, deve-se definir se falhas de primeira ordem podem ser detectadas, e como o CI reage a elas:

- Perda de conexão com o terra causada por defeito na placa de circuito impresso ou em outros componentes
- Perda ou flutuação da tensão de alimentação
- Curto-circuito entre duas saídas
- Interferência
- Sobrecarga das saídas e temperatura excessiva

Essa avaliação incorre automaticamente num estudo FMEA (*Failure Mode Effect Analysis*)[5], cujo objetivo é documentar sistematicamente as possibilidades de falhas e as medidas necessárias para a obtenção da segurança funcional descrita pela IEC 61508 e pelo ISO 26262.

FMEA - Considerações no nível do driver

As considerações da análise FMEA visam descrever quais funções o componente implementa e quais defeitos podem surgir. Disso, passa-se a uma análise de causa e efeito de cada defeito, assim como uma avaliação do seu significado para



o produto como um todo e para o usuário. Então, deve-se levantar a probabilidade de ocorrência dessa falha e como ela pode ser detectada e prevenida, para evitar danos em sua consequência. Essas análises detalhadas devem ser documentadas e incorporadas ao projeto do circuito integrado, bem como à sua produção, testes e processos de qualidade. A figura 2 apresenta a primeira página de uma extensa análise FMEA de um driver FET. A prevenção de uma falha em potencial vem em primeiro plano, assim como sua detecção de forma segura durante a fabricação e sua posterior operação (fig. 2).

FMEA-No.: FMEA1 Project: iC-MFL		Failure-Mode- and Effects-Analysis				iC-Haus			
Package: QFN24		Prepared by: Hz	Last revision date: 10.10.2007		Page 17/12				
FMEA- No.	Potential Effects of Failure	S	Potential Failure Mode	Potential Causes	Current Controls	O	Failure Detection Method	D	RPN
1	no effect	1	PSN FETDR short to GND	Bondwire short to chipedge	SIC assembly	3	SIC assembly: optical inspection, electrical test	2	6
2	#IC1: -output to (0-750mA)	1	PSN VCC open	Bond interruption	SIC assembly: mounting	2	SIC assembly: non-destructive test	1	2
			PSN VCC open	Flow coverage / poor solderability / poor soldering	SIC assembly: handle chips with care	3	SIC assembly: mounting inspection, electrical test	1	3
			PSN VCC open	Flow coverage / poor solderability / poor soldering	parameters: handle chips with care / mounting: solderability	4	Optical inspection, electrical test	1	4
			PSN VCC open	Bond interruption	Compliance with process	3	Electrical test	1	3
			PSN FETDR open	Bond interruption	SIC assembly: mounting	2	SIC assembly: non-destructive test, electrical test	1	2
			PSN FETDR open	Flow coverage / poor solderability / poor soldering	SIC assembly: handle chips with care	3	SIC assembly: mounting inspection, electrical test	1	3
			PSN FETDR open	Flow coverage / poor solderability / poor soldering	parameters: handle chips with care / mounting: solderability	4	Optical inspection, electrical test	1	4
			PSN FETDR open	Bond interruption	Compliance with process	3	Electrical test	1	3
			PSN FETDR short to PSN VCC	Vertical bondwire	SIC assembly	1	SIC assembly: optical inspection, electrical test	1	1
			PSN FETDR short to PSN VCC	Pin misplacement	SIC assembly: handle chips with care	2	SIC assembly: mounting inspection, electrical test	1	2
			PSN VCC: short to GND	Welding bridging on to pins	Manufacturing soldering / handle chips with care	3	Optical inspection	1	3
			PSN VCC: short to GND	Bondwire short to chipedge	SIC assembly	3	SIC assembly: optical inspection, electrical test	2	6
3	#IC1: -output to (0-2 mA)	1	PSN FETDR short to PSN VCC	Welding bridging on to pins	Manufacturing soldering / handle chips with care	3	Optical inspection	1	3
			PSN FETDR short to PSN VCC	Bond interruption	SIC assembly: mounting	2	SIC assembly: non-destructive test, electrical test	1	2
			PSN FETDR short to PSN VCC	Flow coverage / poor solderability / poor soldering	SIC assembly: handle chips with care	3	SIC assembly: mounting inspection, electrical test	1	3
			PSN FETDR short to PSN VCC	Flow coverage / poor solderability / poor soldering	parameters: handle chips with care / mounting: solderability	4	Optical inspection, electrical test	1	4

Figura 2: Trecho extraído de uma Análise FMEA

Como resultado da análise FMEA, definem-se quais das falhas identificadas são críticas, e como elas podem ser detectadas, e suas consequências, prevenidas. O resultado desse estudo influi diretamente no projeto do CI.

“Segurança Funcional” - Exemplo de um driver FET

A título de ilustração, descrevem-se aqui, em detalhes, as medidas adotadas no projeto de um CI de uma família de drivers FET seguros. A figura 3 mostra o acionamento de um FET NMOS (ex.: IRLZ44N) usando o iC-MFL como driver. Em caso de falha, o CI deve evitar de toda forma que o FET NMOS seja acionado. Assim, a saída do driver deve, em caso de falha de primeira ordem, apresentar nível lógico baixo. Além de funções básicas, como conversão de nível (de 1,8 V - 3,3 V para 5 V) e acionamento de FETs de potência, o iC-MFL garante funcionamento seguro, mesmo na ocorrência das seguintes falhas:

- Perda de terra ou V_{CC} no CI
- Entradas em aberto (ex.: trilhas rompidas ou portas do MCU em tri-state)
- Curto-circuito entre duas saídas

A situação mais crítica é a perda de terra ou da tensão de alimentação V_{CC}, já que, nesse caso, os drivers FET comuns não garantem um nível lógico baixo nas saídas. Para isso, além do tradicional monitoramento de V_{CC}, foi incluído no iC-MFL o monitoramento de terra. Sem essas medidas, no caso de uma interrupção na conexão com o terra, a lógica interna não teria nenhum potencial de referência, e o FET externo poderia ser acionado através de cargas parasitárias. Por isso, o CI possui duas conexões de terra (GND e GNDR). Caso uma delas seja interrompida, o monitoramento identificará a falha e desligará as saídas. Caso haja uma interrupção em V_{CC}, as saídas serão conectadas ao terra através de um resistor *pull-down* de cerca de 30kΩ, garantindo funcionamento seguro.

Para aumentar a imunidade a ruídos, todas as entradas do iC-MFL possuem *Schmitt-triggers* e resistores *pull-down*. Os resistores *pull-down* garantem um estado definido para o driver FET, sobretudo durante a inicialização do microcontrolador, quando suas portas estão em tri-state.

As saídas do driver FET são do tipo *push-pull* ativas, com o lado *pull* mais forte para o terra em relação ao *push*. Assim, caso duas saídas sejam curto-circuitadas externamente, uma, com nível alto e a outra, com nível baixo, o driver *lowside* "ganha" a disputa, mantendo o sinal resultante em nível baixo. Adicionalmente, as saídas são protegidas contra impulsos de sobretensão (18 V, 100 ms).

Para outros casos, como, por exemplo, controle de FETs PMOS, ou para outros valores de tensão de entrada/saída, também existem componentes para os quais foram realizadas as mesmas análises FMEA, atingindo o mesmo nível de segurança. Tanto para FETs NMOS, quanto PMOS existem drivers com saídas ajustáveis de tensão em 5 V, 10 V e “full scale”. O exemplo acima descreve apenas as medidas tomadas para evitar falhas durante o funcionamento, que tenham relação direta com o projeto do CI.

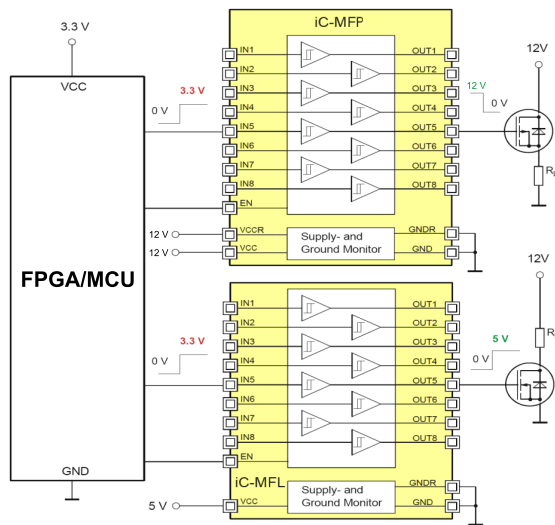
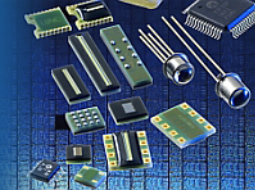


Figura 3: Acionamento seguro de FETs de potência

Conclusão

Como demonstrado aqui, a implementação de uma solução de “Segurança Funcional” segundo a IEC 61508 e o ISO 26262 influencia todo o desenvolvimento do driver, do projeto do circuito integrado até a escolha dos processos e medidas de qualidade envolvidos. Ela implica num amplo trabalho em equipe e torna claros os esforços de desenvolvimento. É importante frisar que análises correspondentes são necessárias em todas as outras partes da eletrônica, como no nível do sistema completo, por exemplo, nos casos da direção eletrônica e dos sistemas de freio. De uma forma geral, a “Segurança Funcional” deve se tornar um padrão cada vez mais adotado, tanto no setor automotivo quanto na indústria em geral.

Para mais informações sobre os drivers FET da iC-Haus, visite:

<http://iC-BR.com/products/output.htm>

Autor:

Thomas Franken é engenheiro de desenvolvimento na iC-Haus GmbH responsável por design FMEA nos projetos.
www.ichaus.com

Tradução:

William Salomão é sócio da empresa iC-BR Microelectronics, parceira técnica e comercial da iC-Haus no Brasil.
www.iC-BR.com

Referências

- [1] Peter Schiekofer, AUTOSAR Schritt für Schritt einsetzen, Automobil-Elektronik, Januar 2007, pp. 24-26.
- [2] Roland Pabst, Entwicklung sicherheitsrelevanter Steuergeräte im Automobil, Automobil-Elektronik, August 2007, pp. 46-47.
- [3] Dr. Karsten Böke, Flexray fährt, Elektronik Automotive 5.2007, pp. 74-77.
- [4] Eugen Mayer, Serielle Bussysteme im Automobil, Elektronik Automotive, 2.2007, pp. 42-45.
- [5] <http://www.fmeainfocentre.com/>