Radar och funktionell säkerhet

Avancerade assistenter till föraren

Av Yves Legrand, Freescale Semiconductor

Yves Legrand är vertikal marknadschef för industriell automation och robotik på Freescale. Han bor i Frankrike men har delat sin tid mellan Toulouse och Chicago. Hans erfarenheter sträcker sig från trådlös kommunikation och konsumentprodukter till gröna laddare och trådlös laddning. Han har en mastersexamen i elektronik från Grenoble och en master i industriella system från San Jose State University, Kalifornien.

Technical Papers
Jan Tångring
jan@etn.se
0734-17 13 09

Radarteknik på 77 GH gör det möjligt att skapa små och förbättrade kollisionsvarningssystem. I kombination med kretsar för funktionell säkerhet, processorer och analoga kretsar går det att skapa omfattande säkerhetslösningar för avancerad hjälp till bilföraren eller för autonom körning. Utvecklingen drivs av fordonsmarknaden men kan återanvändas i många andra typer av mobila tillämpningar.

Radarsystem blir allt vanligare i bilarna eftersom de ökar både komforten och säkerheten. Korthållsradar, som ”ser” från några centimeter framför bilen upp till 30 meter kan användas för att hålla koll i ”döda vinkeln”, som backhjälp eller vid parkering inklusive automatisk parkering.

Radar för längre avstånd, upp till 250 meter, kan användas för intelligent farthållning som anpassas till framförvarande fordon. Den kan också användas för mer kritiska funktioner som kollisionsvarningssystem, nödbromsning och även för att trigga system som försträckning av bälten eller att aktivera andra säkerhetssystem när en olycka är oundviklig. För de senare är det nödvändigt att styrsystemet måste ha den högsta graden av funktionssäkerhet eftersom det förr eller senare styr eller bromsar utan förarens medgivande.

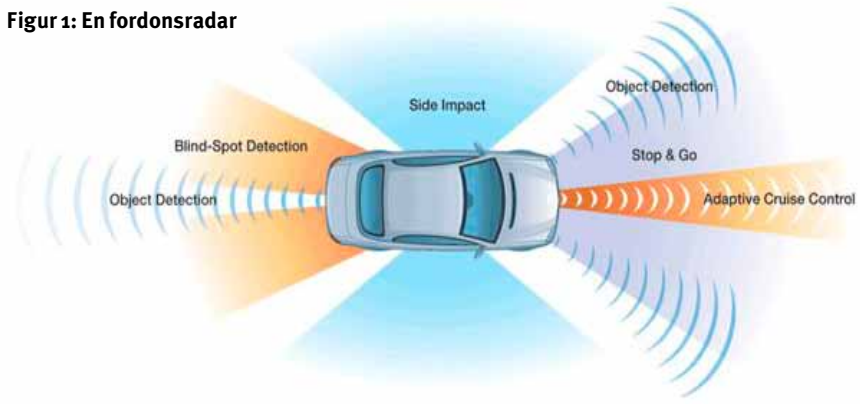
De senaste åren allt bättre radarsystemen gör att de kan nyttjas även i andra tillämpningar som mobila industrimaskiner, kranar eller säkerhetsutrustning till fabriker där en viss yta måste övervakas. Genom att koppla radarn till en kamera går det att skapa en kraftfull kombination där de båda teknikerna kompletterar varandra och på så vis skapar ett robustare och tillförlitligare system. Radarn ser genom regn, dimma och rök plus att den når längre än kameror.

Ett system som kombinerar kameror med radar och dessutom har algoritmer som kombinerar data från flera sensorsystem (sensor fusion) kan dra nytta av bägge teknikerna.

I ett kollisionsvarningssystem skickar en sändare på 77 GHz ut en signal som reflekteras mot föremål och som sedan fånga upp av flera mottagare som är integrerade i fordonet. Sändaren skickar ut en frekvensmodulerad CW-signal vilket innebär att frekvensen åker upp och ned över tiden, typisk är det en triangelformad signal. Eftersom radiovågor rör sig med ljusets hastighet kan avståndet beräknas genom att mäta frekvensskillnaden mellan utsänd om mottagen våglängd om man vet hur frekvensen ändras över tiden. Hastighetsberäkningar använder Dopplereffekten som nyttjar skillnaden mellan den reflekterade frekvensen och den utsända frekvensen.

Radarsystem har funnits länge men det som är n ytt är att biltillverkarna vill ha in dem i mellanklassen inom ett par år, då måste systemen vara både billiga och hålla hög kvalitet. Det är en stor förändring från specialiserade och dyra radarsystem till standardprodukter i bilar. Utmaningen är att reducera kostnaderna

Figur 1: En fordonsradar



Figur 2: Värdediagram

samtidigt som man förbättrar kvaliteten mätt i antal fel. Den här förändringen illustreras av kvalitet relativt kostnad i värdediagrammet.

Det här diagrammet visar på övergången från höga kostnader och god kvalitet till lägre kostnader och faktiskt ännu högre kvalitet. För att nå målet är det många utmaningar som måste lösas.

Traditionella radarsystem använder roterande antenner för att få rumslig (spatiell) upplösning av objekten. Det kan var OK för större system med dyra styrsystem men definitivt inte för en volymprodukt till en bil. En lösning är att använda fasstyrda antenner eller etsade antenner med många sändar- och mottagarkanaler.

Rumsligt åtskilda antenner fångar signaler som inte gått raka vägen med en liten tidsskillnad. Den används för att rekonstruera objektets position precis som den roterande antennen ger positionen. Nackdelen med etsade antenner är att man måste ansluta flera sändar- och mottagarkanaler till antennen. Ett typiskt system kommer att använda fyra sändarelement och 16 mottagarelement men att ha hårdvara bakom varje antennelement är inte ekonomisk möjligt.

Vi räddas av en annan innovation. Istället för att ha diskreta rf-kretsar har Freescale utvecklat en BiCMOS-process för rf-tillämpningar som har tillräcklig prestanda för att integrera alla 77 GHz-funktionerna på en enda krets. Utgående från en högpresterande process med kiselgermaniumkarbid (SiGe:C) på 180 nm har Freesclae utvecklat transistorer med 300 GHz Fmax som klarar radarsignaler på 77 GHz. Tillsammans med analoga och digitala CMOS-kretsar går det att åstadkomma en hög grad av integration av ett flerkanaligt system för 77 GHz på en krets. Kostnaden för flera kanaler kan därmed absorberas av halvledarintegrationen.

En halvledarprocess för 77 GHz är en värdefull tillgång men att hantera kretsarna och montera dem på kretskortet är ytterligare en utmaning. På så här höga frekvenser kan parasitimpedansen i vanliga kapslar förstöra informationen i signalen. Ett sätt att hantera det är att använda okapslade komponenter lödda på ett speciellt mönsterkort i kombination med trådbondning istället för typiska kapslar och våglödning. Här kommer en ny och avancerad kapslingsteknik kallad Redistributed Chip Package, RCP till undsättning.

RCP använder grov litografi för att bygga upp ledarlagren av koppar på ovansidan av en krets eller en stack av kretsar istället för att nyttja kretskortsmaterial. Den här substratlösa kapslingstekniken har mycket lägre parasitkapacitans och -induktans. Det är möjligt att leda högfrekvenssignaler på 77 GHz genom den här kapseln med acceptabel prestanda jämfört med att löda okapslade komponenter. Fördelen är att traditionella kretskortsmaskiner kan användas för att montera den här komponenten vilket ger låga kostnader.

Freescale konstruerar integrerade sändare och mottagare för radartillämpningar med den här tekniken.

Sändaren innehåller en syntetisator för 77 GHz, en VCO på halva frekvensen, en 10 GHz PLL som ger multipler av grundfrekvensen och en effektförstärkare med en modulator på 28-bitar av typen sigma-delta. Kretsen kommer med ESD-skydd för rf och DC liksom digital styrning via ett SPI-gränssnitt.

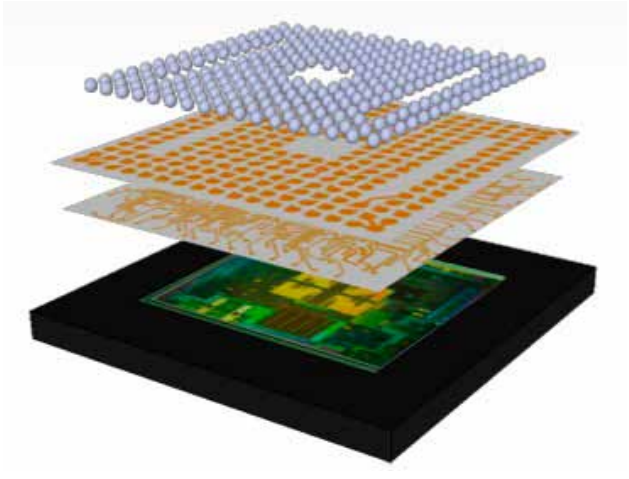
På mottagarsidan integrerar vi i normalfallet fyra mottagarkanaler med en lokaloscillator på 38 GHz och differentiell utgång för mellanfrekvenssignalen (IF). Den typiska brusfaktorn är 13 dB utan en lågbrusförstärkare vilket bidrar till att hålla nere effektförbrukningen och ger hög linjäritet.

En procesor används för att styra sändaren i radarn och för att processa data som kommer från mottagaren. På grund av de säkerhetskritiska kraven i applikationen används en så kallad funktionssäker processor. Utmaningen för systemingenjören är att utforma systemet på ett sådant sätt att det inte uppstår farliga fel eller åtminstone att man kan hantera dem när de uppstår. Farliga fel kan uppstå på grund av:

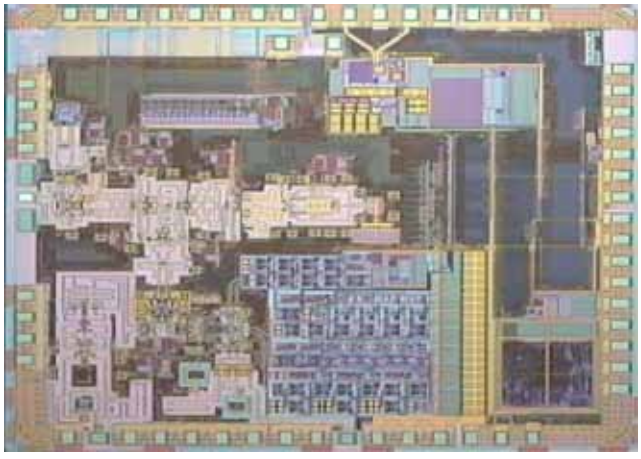
- Slumpmässiga hårdvarufel
- Systematiska hårdvarufel
- Systematiska mjukvarufel

Standarden för funktionskritiska system, IEC 61508, och dess variant för fordonsområdet, ISO 26262, kan tillämpas för att försäkra sig om att elektroniksystem i industrin och för fordonstillämpningar är tillräckligt säkra.

IEC 61508 definierar fyra säkerhetsnivåer (Safety Integrity Levels, SIL) där SIL 4 är den mest stringenta. ISO-dokumentet definierar fyra säkerhetsnivåer (Automotive Safety Integrity Levels, ASIL) där ▶



Figur 3: Uppbyggnad av RCP-kapsling.



Figur 4: Sändarchip för en radar på 77 GHz.

ASIL D är den högsta. Varje nivå definierar ett antal sannolikheter för fel i säkerhetsfunktionen. Det finns ingen direkt korrelation mellan nivåerna i SIL och ASIL men ISO 26262 tar säkerhetsprocessen och de tillhörande kraven till en djupare nivå. Redan vid starten av designprocessen måste man samla in fakta som visar att produkten utvecklas i enlighet med standarderna. Alla potentiella avvikelser som identifieras måste dokumentras för att försäkra sig om att adekvata åtgärder vidtas.

Det finns olika sätt att implementera säkra processorer. Den traditionella lösningen är att använda två separata kretsar och duplicera mjukvaran. Samma mjukvara körs på identiskt sätt på de två processorerna och resultaten jämförs fortlöpande. Om de är identiska är allt frid och fröjd, om inte, vet systemet att ett fel inträffat och kan antingen lösa det eller försätta systemet i ett felsäkert läge.

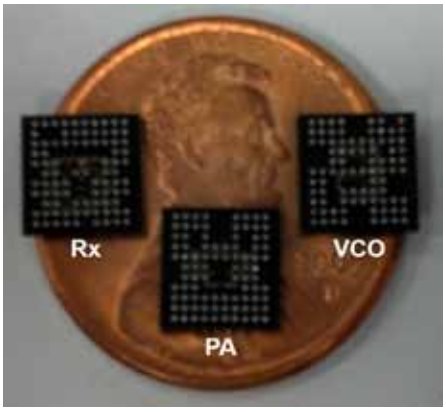
En annan möjlighet är att bara en av styrkretsarna kör säker mjukvara och övervakar den andra styrkretsen som kör applikationen. Med separata styrkretsar måste bägge systemen designas från grunden.

Å andra sidan finns det numera processorlösningar som redan är certifierade. Dessa lösningar fokuserar på att detektera och hantera enstaka fel, latenta fel och beroende fel. Detta uppnås genom inbyggda säkerhetsfunktioner inklusive självtest, övervakning och hårdvarubaserad redundans i styrkretsarna men också i kraftförsörjningen och sensorerna. Systemkretsar har integrerad redundans för de kritiska komponenterna såsom:

- Multipla processorkärnor som körs i lock-step
- I/O-processorkärna
- DMA-kontroller
- Avbrottskontroller
- Dubbel korskopplare
- Minnesskyddsenhet
- Insamlingsenhet för fel
- Kontroller för flash och RAM
- Brygga till periferibuss
- System- och watchdogtimers
- Felkorrigering

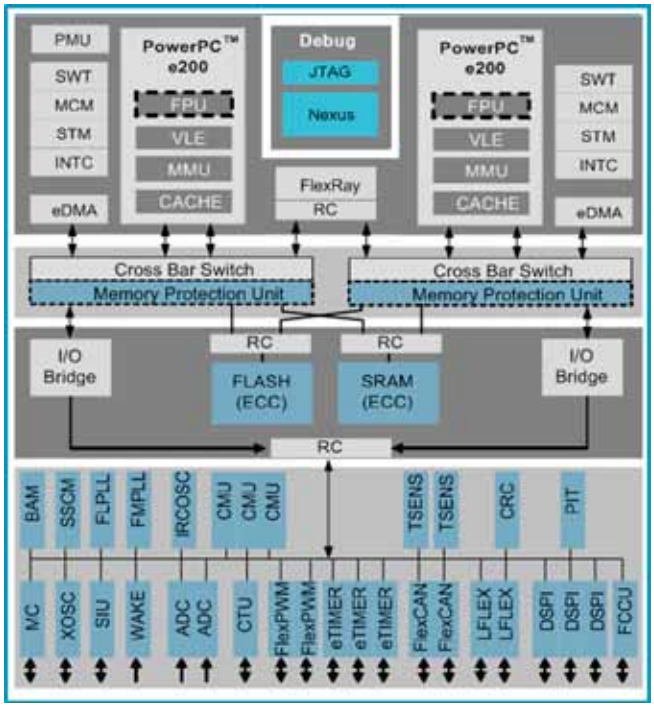
Den stora fördelen med denna form av replikering är att styrkretsen har möjlighet att upptäcka singelfel som tenderar att uppträda oftare som mjuka fel, inte bara i kärnorna utan också i viktiga undermoduler.

Mekanismer för inbyggd självtest (BIST) finns också för kärnorna, korskopplaren och för periferiblocken. Dessutom är kretsen optimerad för att förhindra fel som förorsakas av klockan och spänningsmatningen. MCU:n har hårdvarublock för att upptäcka avvikelser i klockperioden liksom hårdvara för att övervaka spänningarna till kärnorna och flashminnet.



Figur 5: RCP-kapslade radarkomponenter.

Dubbla styrkretsar som körs i lock-step minskar inte behovet av att implementera säkerhetsåtgärder på mjukvarunivå liksom på systemnivå såsom tillräckligt oberoende övervakning av de värden som beräknas av mjukvaran. Förutom högre integrationsgrad skiljer de ut problemen med valideringen. I lösningar som baseras på flera, separata processorer är möjligheten att upptäcka och ta hand om slumpmässiga fel är huvudsakligen beroende av mjukvaran. Men en dubbelkärnig processor som körs i lock-step är det möjligt att verifiera och validera säkerhetsrelaterade egenskaper i beräkningsdelarna på hårdvarunivå oberoende av mjukvaran eftersom exekveringsdelen kommer i en integrerad form och representerar en integrerad säkerhetsmekanism. Det är en avsevärd fördel vid samkonstruktion av hårdvara och/mjukvara. Dessutom medför separeringen av problemen att de är enklare att lokalisera. Om säkerhetsmekanismerna som övervakar de dubbla kärnorna som körs i lock-step triggas beror felet normalt på slumpmässiga fel på hårdvarunivån men om felet triggas av mjukvaruövervakningen är orsaken troligen på systemnivån eller av systematisk karaktär.



Figur 6. Dubbelkärna som körs i lock-step.

Lösningen med en dubbelkärna i lock-step har en fördel i tillgängligheten. I moderna processorer utgör kärnan mindre än 5 procent av hela kretsen medan man räknar med att kretsen som sådan inte står för mer än 1 procent av den totala risken för hårdvarufel (Probabilistic Metric for random hardware failures, PMHF).

Vid en första approximation kommer man fram till att kärnorna bidrar med cirka 0,05 procent men det gäller att vara säker på att hårdvaran fungerar korrekt för att felkorrigeringen som används av mjukvaran för att hantera resterande 99,95 procent av PMHF och därmed har ett ständigt tillgängligt system. Dessutom utgör den dubbla kärnan i lock-step en lämplig infrastruktur för att implementera multipla och tillräckligt oberoende kanaler.

Som stöd för en systemlösning för tillämpning inom funktionell säkerhet har vi utvecklat en krets som både övervakar kraftförsörjningen och levererar kraft. Kretsen, som går under beteckningen System Basis Chip (SBC) levererar kraft till både processorn och andra delar i systemet och optimerar samtidigt effektförbrukningen genom olika energisparlägen. Den innehåller också fysiska gränssnitt och ett seriell gränssnitt för att kunna hantera styrning och diagnostik ihop med processorn. Kombinationen processor och SBC-krets, som designats

som ett så kallat Safety Element out of Context (SEooC), underlättar arbetet med systemets säkerhet. Lösningen gör att man kan minska antalet komponenter vilket ytterligare ökar tillförlitligheten.

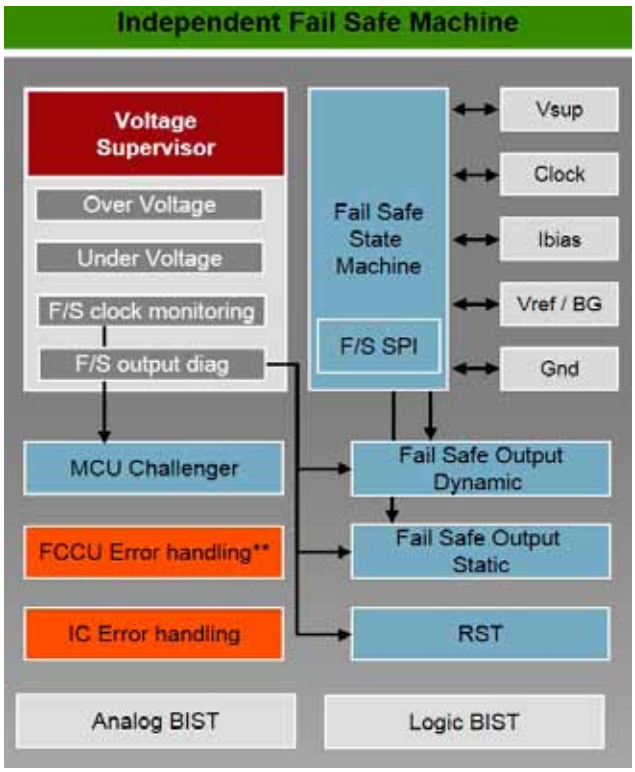
Det finns fyra komponenter som säkerställer kommunikationen mellan processorn och SBC:n:

- avbrottsfri kraft
- felsäkra ingångar som används för att övervaka kritiska signaler
- felsäkra utgångar för att driva felsäkra tillstånd
- en watchdog för avancerad klockövervakning

På systemnivå kan säkerhetstester som processorn föreslår övervakas av SBC:n genom det bistabila protokollet i den så kallade Fault Collection Control Unit (FCCU). Den här kretsen korscheckar vilket ger fristående och redundanta mätningar av systemet vilket ytterligare ökar sannolikheten för att hitta fel. I linje med säkerhetsarkitekturen i SBC-familjen finns en redundant kanal för aktiveringar genom dedicerade felsäkra utgångar. De här utgångarna komplimenterar de (felsäkra utgångarna) som finns i processorn genom att försätta applikationen i ett felsäkert läge när ett fel inträffar.

De här hårdvarufunktionerna gör det enklare för programmeraren att förenkla och implementera mjukvarans arkitektur med en strategi som fokuserar på säkerheten när man bara använder en processor.

Ansvaret för att uppfylla kraven på funktionell säkert ligger på systemnivån och landar därför på systemdesignern. Processorn och SBC:n konstrueras separat och oberoende av sina slutgiltiga tillämpningar som kan vara ett parkeringshjälpmedel, en hjälpreda till bilföraren eller en kran som förflyttar sig.Kretspaketet utvecklas genom att betrakta det som ett fristående säkerhetslösning, så kallad Safety Element out of Context (SEooC). En SEooC en en säkerhetsrelaterad komponent som inte utvecklats för en specifik tillämpning eller produkt. Det finns detaljerade riktlinjer för den här typen av produkter i standarden ISO26262.

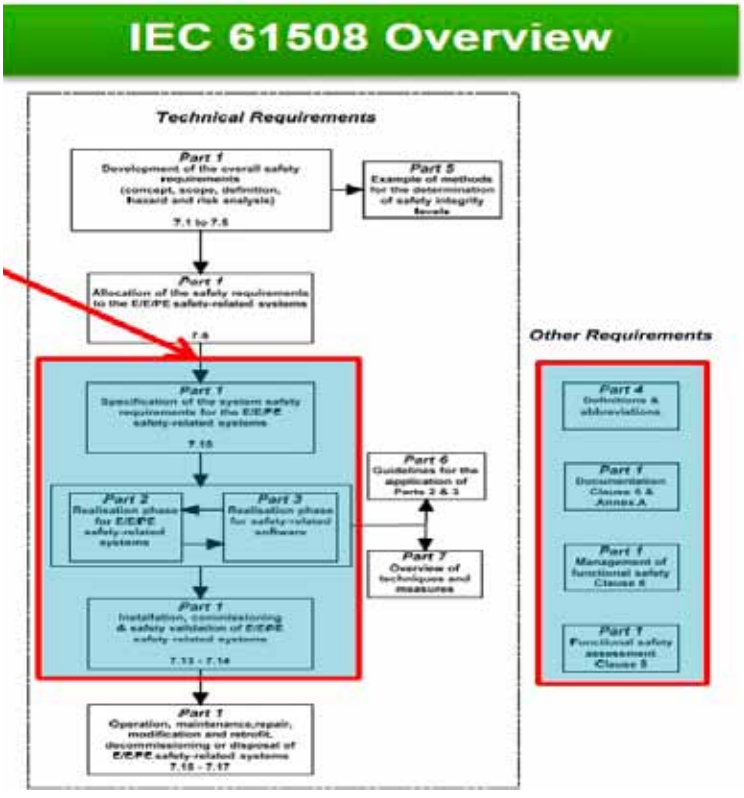


Figur 6. Dubbelkärna som körs i lock-step.

Freescale har samlat sina satsningar på funktionell säkerhet under varumärket SafeAssure. Det täcker support, hårdvara och mjukvara liksom en processer som garanterar att alla relevanta standarder följs under utvecklingsarbetet. Det gäller:

- Säkerhetsanalys av arkitekturen enligt FMEDA, CCA eller FTA.
- Användarhandledning: säkerhetsmanual och applikationsbeskrivning.
- Development Process evidence: PPAP, säkerhetsplan och certifikat

Målet är att korta tiden och minska komplexiteten för utvecklare av säkerhetskritiska system som ska uppfylla ISO 26262 och IEC 61508 liksom att förenkla processen med att dokumentera att systemet följer standarderna. Lösningen gäller särskilt för fordons- och industritillämpningar. ■



Figur 7: SBC Fail Safe Machine

Figur 8: Freescales program kallat Safe Assure