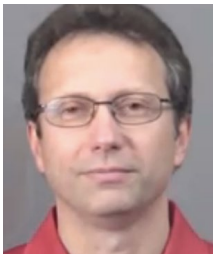
Freescale:
Kinetis M kan isolera kod som är juridiskt relevant

Av : Joe Circello och Martin Mienkina

Joe Circello är känd som chefsarkitekt för både MC68060, Coldfire och ett antal 32-bitars processorer för fordonselektronik. Han har 22 år på Freescale bakom sig och är idag Technical Fellow. Sin utbildning fick han på Milwaukee School of Engineering och Arizona State University.



Martin Mienkina är System Solutions Engineer på Freescale och har på sistone specialiserat sig på bland annat processorer för smarta mätare. Han har sedan millennieskiftet jobbat på Freescale i Roznov i Tjeckien, en timmes bilresa från universitetet i Zilina i Slovenien där han tog sin doktorsexamen i elektroteknik.

Det är inte bara säkerhetskritisk kod som av kvalitetsskäl bör skiljas från annan kod. Detsamma gäller kod som avgör storleken på abonnentens elräkning eller som är juridisk relevant på andra sätt. Freescale berättar om sin processor Kinetis M som kan isolera programvarans olika delar på flera olika sätt.

Vi omges av elektroniska mätinstrument – hemma, på jobbet och på verkstadsgolvet. Vattenmätare, gasmätare, värmemätare, energimätare, vågar, taxametrar, och ännu fler, var vi än ser. Nuförtiden hanterar de flesta av dem debitering – och andra funktioner som lyder under lagar och regler – i en styrkrets. Med andra ord avgörs storleken på konsumenters räkningar direkt av hur exakta och pålitliga dessa mätinstrumentet och deras styrprogram är.

Det finns organisationer som OIML (International Organization of Legal Metrology) och WELMEC (European Cooperation in Legal Metrology) som ger ut riktlinjer för hur program som styr mätinstrument ska konstrueras. En specifik detalj som krävs är kodseparation [1][2]. I denna artikel ska vi berätta om grunderna för kodseparation och vi ska visa hur Freescales styrkretsfamilj Kinetis M är alldeles särskilt lämpad för mätfunktioner där just kodseparering kan användas både för att ge tekniska fördelar och för att sänka utvecklingskostnad och time-to-market.

Mätinstrument styrs av programkod med respektive utan juridisk substans (se figur 1), sett ur utvecklarens perspektiv.

Den programkod som styr AD-omvandlare som levererar mätvärden som har betydelse för debiteringen, är ett exempel på kod med juridisk substans. Likaså programkod som hanterar bearbetning, presentation, utskrift och kryptering av dessa data, och programkod som lagrar debiteringsdata, loggfiler och lastprofiler i ickeflyktigt minne. Och eftersom viss information måste lagras vid bestämda tidpunkter, styrs även realtidsklockan av programkod med juridisk substans.

Den programkod som saknar juridisk substans är den som sköter övriga funktioner – som att sända digitalt signerade datapaket till operatören eller kommunicera med utrustning kopplad till hemdatanätet.Exempelvis kan man tänka sig att en uppkopplad tvättmaskin programmeras att tvätta under timmar när belastningen inte är på topp, för lägre taxa. Eller kanske smarta värmeelement

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

ELEKTRONIK TIDNINGEN

Figur 0
En smart elmätare byggd kring Kinetis M kan lägga lagreglerad kod i en egen isolerad cell. Då blir det bland annat betydligt enklare att uppdatera den mjukvara som ej är lagreglerad.

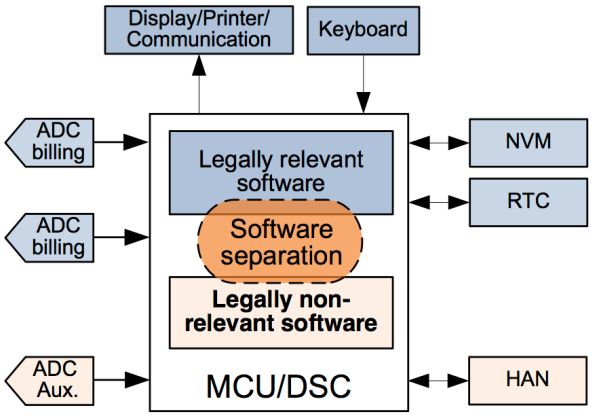
aktiveras och inaktiveras under bestämda tider för att jämna ut belastningen.

Mängden programkod som saknar juridiskt substans ökar. Det har nämligen blivit allt viktigare för mätinstrument att kunna dela data på olika sätt och i olika protokoll med smarta apparater. Och om en viss funktion eller ett visst protokoll saknas, måste tillverkaren av mätinstrumentet snabbt och billigt kunna ta fram stöd för dem.

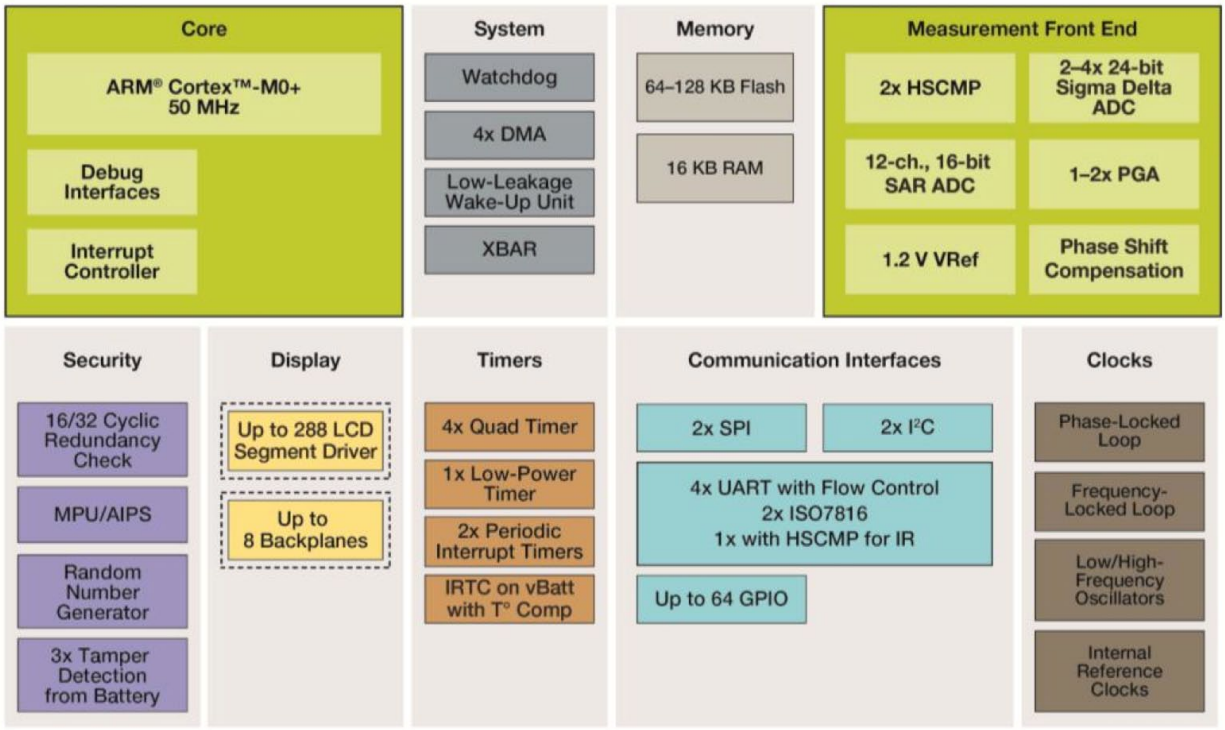
Det är som sagt enbart programkod med juridisk substans som är föremål för reglering. Och när programkoden ifråga väl har godkänts är det inte tillåtet att modifiera den utan att därefter inhämta nytt godkännande. Om kodsepareringsteknik saknas, betraktas dessvärre hela blocket av firmware som programkod med juridisk substans – och varje modifiering kräver att man går igenom en omfattande och kostsam godkännandeprocess.

Om kodseparering däremot används – enligt OIML:s och WELMEC:s riktlinjer – kan tillverkaren modifiera juridisk irrelevant mjukvara utan att därefter behöva skaffa ett nytt godkännande. Detta ger mer flexibilitet och betydande kostnadsbesparninar.

Freescales systemarkitekter har arbetat med hårdvarustöd för isolering av operativsystem och mjukvara i drygt två decennier. På sistone har även styrkretsar börjat utrustas med med minnesskyddsenheter (MPU, memory protection unit) som omfattar både minnet på kretsen och externt minne. Freescales styrkretsserie Kinetis M tar ytterligare ett steg: utöver att skydda minnet reglerar den åtkomsten till de flesta av kretsens periferienheter. Kinetis M är tveklöst den mest avancerade styrkrets man kan få tag på vad gäller kodseparering. Systemplattformen på Kinetis M är uttryckligen konstruerad för att ge hårdvarustöd för kodseparering. Utöver hårdvarublock som hanterar access till on chip-minne, periferienheter och IO-portar, integrerar dessa kretsar även analoga periferienheter med hög prestanda, och så har de en



Figur 1
Ett mätinstruments mjukvarudelar.



Figur 2. Kinetis M blockdiagram

bred uppsättning digitala funktionsblock och kommunikationsfunktioner.

Freescales styrkretsfamilj Kinetis M har de onchip-periferienheter, den beräkningsprestanda och den strömstyrning som du behöver för att utveckla billiga, högt integrerade mätinstrument (se figur 2).

Grunden är en 32-bitars Cortex Mo+-kärna på upp till 50 MHz. Alla kretsar i familjen har en front-end för mätning som inkluderar en mycket exakt 24-bitars sigmadelta-ADC, förstärkare med programmerbar gain (PGA), en intern spänningsreferens (Vref) på 1,2 v med hög precision, fasskiftskompenseringsblock, 16-bitars SAR-ADC och peripheral crossbar (XBAR). XBAR-modulen fungerar som en programmerbar växelmatris och tillåter multipla samtidiga kopplingar mellan interna och externa signaler. I alla kretsar finns dessutom en noggrann oberoende realtidsklocka (IRTC) med både passiv och aktiv detektering av otillåten manipulering.

Utöver analoga och digitala funktionsblock, är Kinetis M-familjen utvecklad med fokus på att stödja den efterfrågade kodsepareringen – hårdvarublock stöder en tydlig separering mellan juridiskt relevant kod och annan mjukvarufunktionalitet. Följande block är några av dem som kan reglera och/eller övervaka åtkomst:

- Arm Cortex Mo+-kärnan
- DMA-styrningsmodulen
- MCM-modulen (Miscellaneous Control Module)
- MPU:n (minneskyddssenheten)
- Periferibryggan
- GPIO-modulen (General Purpose Input Output)

Systemplattformen Kinetis M kan använda både Mo+-kärnan och DMA-styrmodulen som master till bussen (se figur 3). Via MCM-modulen kan mastern ställas in att bestämma de traditionella accesstyperna Privileged och User. Dessutom kan MCM-modulen bestämma accessattribut utifrån en mjukvarustyrd processidentifierare som anger att tillståndet är Secure eller Nonsecure. Program och DMA-kanaler som körs Privileged Secure har inga begränsningar vad gäller vilka resurser de kan använda.

User Secure och Nonsecure har lägre prioritet än Privileged Secure. Dessutom kan program och DMA-kanaler som körs User Secure eller Nonsecure varken komma åt kärnans System Control Block, Nested Vectored Interrupt Controller eller System Timer.

Utöver dessa grundläggade åtkomstrestriktioner för User Secure och Nonsecure kan plattformen också begränsa åtkomsten till de on chip-periferienheter som är avgörande för chipkonfiguration, reset-kontroll och effekthantering. Sammanfattningsvis kan hårdvaran kan genomdriva en åtkomstprioritetsmodell med tre tillstånd där Priviledged (Secure) > User Secure > User Nonsecure.

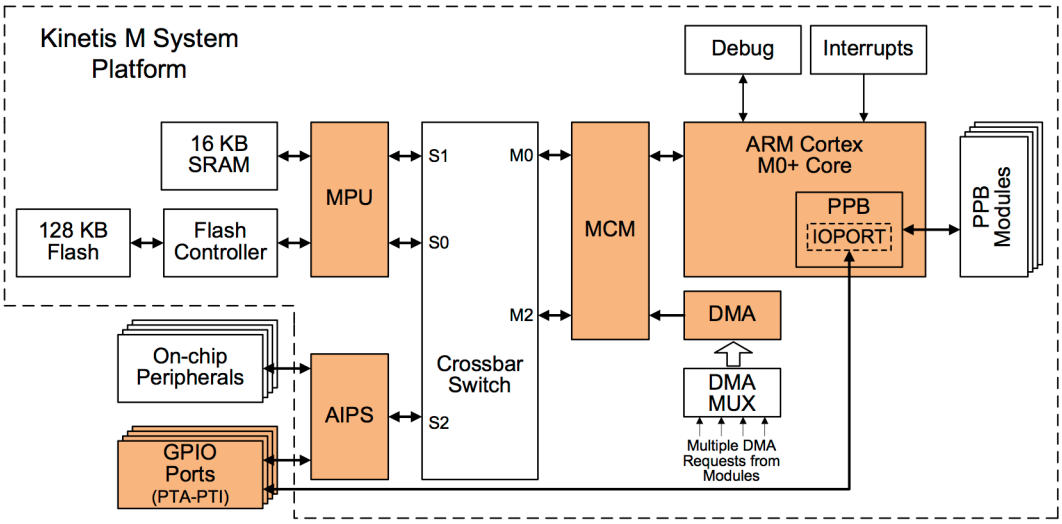
DMA-modulen i Kinetis M har fyra oberoende DMA-kanaler, var och en med en programmerbar Transfer Channel Descriptor som körs Privileged Secure, User Secure eller User Nonsecure. Otillåtna åtkomstförsök leder till att buss-cykeln avbryts med en felkod.

Här följer en beskrivning av de hårdvarublock som styr åtkomsten till on-chip-minne och on-chip-periferienheter för Mo+-kärnan och DMA Controller bus-masters som körs med attributen Privileged Secure, User Secure eller User Nonsecure.

För det första åtkomstskyddar MPU:n i hårdvara on-chip-flash och SRAM. MPU:n har åtta programmerbara 128-bitars regiondeskriptorer som var och en definierar start- och slutadress och stöder läs, skriv- och exekveringsskydd för buss-masters och access-modes som stöds. Detta block detekterar åtkomstfel om det sker en minnesreferens utanför alla minnesregioner, eller om minnesrefererensen är spärrad i de minnesregioner som berörs. Otillåtna accesser genererar en felterminering. MPU:n kan bara programmeras i Privileged access-mode.

För det andra: AIPS (Peripheral Bridge) konverterar crosssbar-switchens gränssnitt till ett protokoll som är kompatibelt med slavperiferienheterna on-chip. Den sköter alla de buss-master-transaktioner (”buss-cykler”) som är destinerade för de anslutna slave-enheterna och stöder programmerbara unika accessrättigheter för varje ansluten slave-enhet. Varje perfieriport definerar read- och write-attribut för buss-masters och de access-modes som stöds av modulen. Otillåtna accesser genererar ett termineringsfel. Liksom MPU:n kan AIPS endast programmeras i Priviledged acces-mode.

Särskild vikt fästes vid att GPIO-mo-



Figur 3. De hårdvarublock vars åtkomstattribut styrs.

dulen skulle ha accesskontroll. Kinetis M-familjen har 68 GPIO-ben grupperade i nio portar. Varje åttabensport (PTA-PTI) stöder läs- och skrivskydssattribut för alla de buss-masters och access-modes som stöds av porten. GPIO:erna kan accessas via periferibryggan eller IOPORT, som är ett särskilt single-cycle-gränssnitt mot Mo+-kärnan. Otillåtna accesser som sker via IOPORT behandlas som RAZ/WI (Read As Zero/Write Ignored) medan de som sker via periferibryggan genererar fel.

Efter varje reset-tillstånd inklusive POR (Power-on Reset) börjar Mo+-kärnan exekvera kod i läge Privileged Secure. Det är nödvändigt att initiera alla nämnda hårdvarublock och programmera deras respektive accessattribut. Alla konfigurationsattribut kan låsas mjukvarumässigt fram till nästa POR.

Efter att alla accessattribut programmerats, kan mätinstrumentets firmware initiera den mjukvara och de DMA-överföringar som har, respektive saknar, juridisk substans. De viktigare programmen och DMA-överföringarna – de som har juridisk substans – exekveras i Privileged Secure-läge, medan juridiskt ickesubstantiella program och DMA-överföringar exekveras i User Secure- eller i User Nonsecure-accessmode, för hindra deras åtkomst till resurser som är kritiska för enhetens konfigurering och hindra dem från att påverka exekveringen av de program som har juridisk substans.

Eftersom många halvledartillverkare har styrkretsar som ensamma klarar att driva mätinstrument – både beräkningar och analoga och digitala delar – så är det snart en förutsättning för en konform produkt att den stöder OIML:s och WELMEC:s riktlinjer för kodseparation.

Dessa riktlinjer framhålls idag som rättesnören (best practises) när det gäller konstruktion av styrkretsbaserade mätare och de efterföljs dels av tillverkare och dels av de certifieringsorgan som ansvarar för att deklarera produkter som konforma.

Freescales Kinetis M-familj har direkt på chipet precis de analoga och digitala periferienheter som krävs för att utveckla billiga och högt integrerade mätare.

En rik uppsättning periferienheter backas upp av en Cortex-Mo+-kärna med klockfrekvens upp till 50 MHz med tillhörande strömsparfunktioner. Utöver integrerade periferifunktioner har Kinetis-M-styrkretsen en hårdvaruarkitektur som stöder kodseparation.

Allt detta, tillsammans med låga kostnader och de strömsparmöjligheter som 90 nm processteknik ger, gör Kinetis M till ett idealiskt val för vattenmätare, fasmätare, värmemätare, energimätare, vågar, taxametrar och en växande mängd elektroniska allt mångfunktionellare mätinstrument för hem, arbetplatser och verkstadsmiljöer.

Referenser

• OIML, OIML D31, "General Requirements for Software Controlled Measuring Instruments", edition 2008 (E) http://workgroups.oiml.org/tcsc/tc-07/tc-07-sc-04/reference-documentation/D031-e08.pdf

• WELMEC, WELMEC 7.2, "Software Guide (Measuring Instruments Directive 2004/22/EC)" http://www.welmec.org/fileadmin/user_files/publications/WELMEC_07.02_Issue5_SW_2012-03-19.pdf

• ARM Cortex-Mo+ Devices - Generic User Guide, 2012 ARM http://infocenter.arm.com/help/topic/com.arm.doc.duio662b/DUIo662B_cortex_mop_rop1_dgug.pdf