Apparna trängs i hypervisorn – men håller avstånd

EXPERTARTIKEL

Framtidens fordonsdatorer är utspridda i zoner och har hårdvarustöd för separerande virtualisering som klarar realtid.

Bilindustrins megatrend – mjukvarudefinierade fordon – kommer att tvinga fram förändringar av de datorarkitekturer som används i fordon. En och samma hårdvara måste kunna köra flera program samtidigt. Det är avgörande att man kan garantera att de är tryggt separerade från varandra och kan möta sina realtidskrav.

Virtualisering är nyckeln. Det görs antingen i ren mjukvara eller med stöd i hårdvara. Denna text fokuserar på det senare. Vi kommer som exempel att beskriva ett system bestående av en mikrokontroller (MCU) med virtualiseringsstöd i hårdvara, och en hypervisor som adderar ytterligare möjligheter.

Förarassistans, komfort, konfigurationssystem och diverse nya tjänster är högsta mode. De kräver kraftfull hårdvara – och mer hårdvara – vilket står i konflikt med målet att fordon ska bli lättare och bränslesnålare.

Ett sätt att möta utmaningen är att packa in så många funktioner som möjligt på en och samma processor. Det förenklar nätverket, sänker kostnaderna och minskar vikten.

Marknaden erbjuder flera olika lösningar för att göra konsolidering av det här slaget.

Autosar

Medlemmar i konsortiet Autosar utvecklade redan för nästan tio år sedan en arkitektur som skyddar minne och kan uppfylla tidskrav för enskilda funktioner. Program med säkerhets- och realtidskrav på olika nivåer kan köras samtidigt i samma operativsystem (OS).

Nackdelen är att den här arkitekturen är begränsad till ett enda operativsystem. Denna inflexibilitet betyder att det endast är möjligt att leverera programvara i form av ett enda monolitiskt programpaket.

Det betyder att enskilda appar inte kan uppdateras modulärt. Det är inte heller möjligt att göra efteranpassningar.

Om programmen kommer från olika källor, till exempel en OEM, en tredjepart eller ett eget äldre system, finns dessutom en möjlig säkerhetsrisk. Därför kan inga ändringar göras i något av de integrerade systemen utan att ECU:n och hela programsystemet omkvalificeras från grunden.

Hårdvaruvirtualisering

Något som kan ge kunden större flexibilitet är isolering via virtualisering. Det finns rena mjukvarulösningar för detta och det finns lösningar som tar stöd i hårdvarufunktioner – sedan några år finns ECU:er från flera olika tillverkare som kan separera program störningsfritt och med garanterad realtidsprestanda.

Funktioner som är integrerade med operativsystemet allokeras till olika minnesområden, vilket ger spatial separation. Segmentering säkerställer att funktionerna inte stör varandra. Därmed kan programpaket med olika funktionssäkerhetskrav integreras på samma processor.

Till skillnad från Autosar levereras inte mjukvaran i ett monolitiskt paket. Varje funktion kan modifieras för sig, utan omcertifiering. Det går att lägga till och ta bort funktioner utan större ansträngning.

När flera tillämpningar körs i samma MCU måste de garanteras åtkomst och de måste separeras. För ändamålet finns två mekanismer:

- Brandväggar som fungerar som portvakter. De validerar att åtkomst är tillåten för en applikation som försöker initiera en transaktion.
- En Quality-of-service-mekanism som ser till att varje tilämpning får den bandbredd som behövs, garanterat fri från störningar

Virtualisering på en MCU från ST

STMicroelectronics MCU-familj Stellar har hårdvarustöd för en typ 1-hypervisor, även kallad bare-metal-hypervisor. En hypervisor av typ 1 är ”lean” – den ger en knappt påvisbar prestandaförlust. De funktioner som krävs för separation är permanent integre-

Av Isaac Trefz och Jan Pistulka, STMicroelectronics

Isaac Trefz är produktchef över COQOS Hypervisor SDK på OpenSynergy och har över 20 års erfarenhet inom programutveckling och diagnostiska verktyg för bilindustrin. Han läste till elektroingenjör på Massachusetts Institute of Technology.

Jan Pistulka är system- och applikationschef på ST Microelectronics, baserad i Tyskland. Han startade på ST som fältingenjör och har arbetat inom vitt spridda fält, bland annat kommunikation, OTA, virtualisering, batterihanteringssystem och kraftledningskommunikation.
Hans examen kommer från Tjeckiens tekniska universitet i Prag.

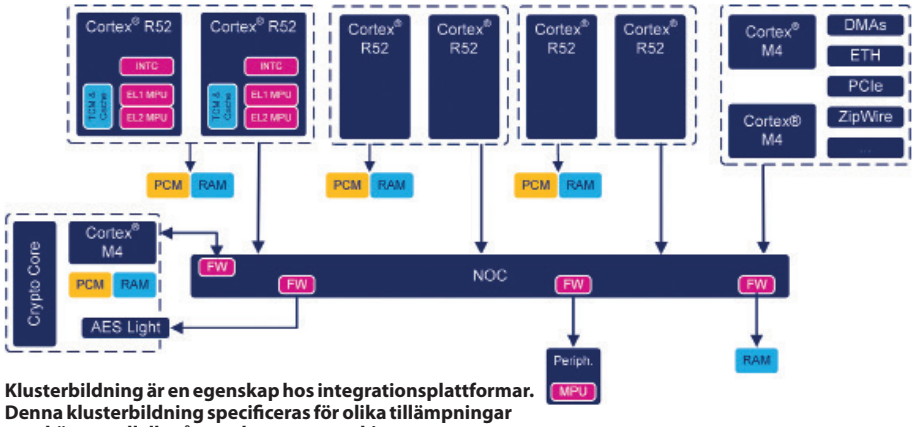
FAKTA

Stellar

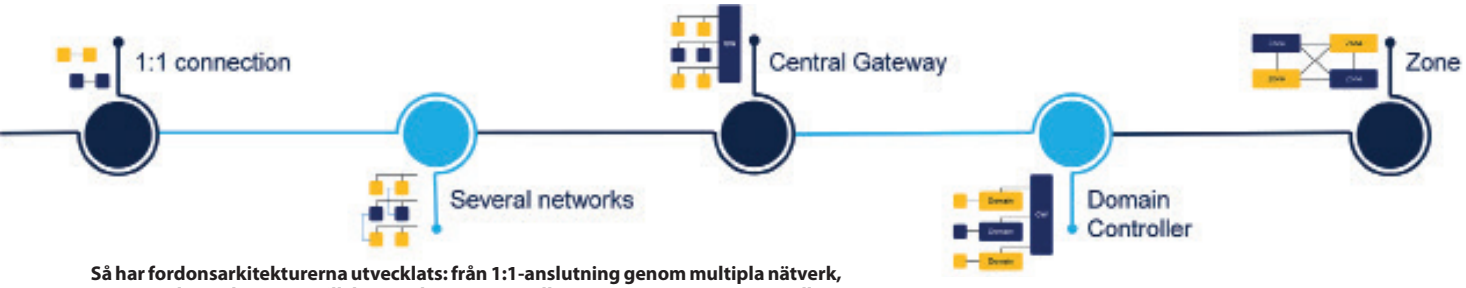
Beräkningskraften i Stellar kommer från en Cortex R-52 med ett antal M4-kärnor som den avlastar uppdrag till. M4-kärnorna sköter även strömstyrning.

Stellar-familjen är byggd på energieffektiv 28 nm FD SOI (Fully Depleted Silicon on Insulator) som har en revolutionerande implementering av PCM (phase-change-memory) för fordon. Detta öppnar helt nya möjligheter för Over-the-air-uppdateringar och gör att hälften av minnesvolymen inte behöver användas med standard Flash-teknik.

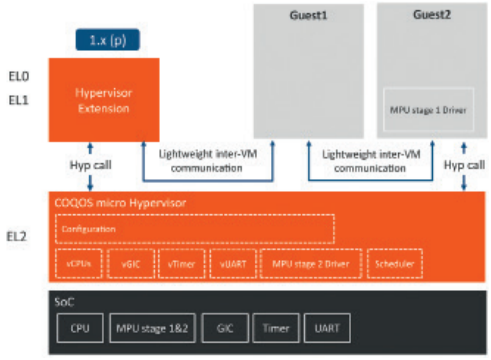
Stellar finns redan på marknaden i flera varianter och når ASIL-D-nivån enligt ISO-26262.



Klusterbildning är en egenskap hos integrationsplattformar. Denna klusterbildning specificeras för olika tillämpningar som körs parallellt på en och samma maskinvara.



Så har fordonsarkitekturerna utvecklats: från 1:1-anslutning genom multipla nätverk, via centraliserad gateway till dagens domän-controllers. Nästa steg är zon-controllers.



En typisk arkitektur för hypervisorn COQOS i en realtidsprocessor. De orangefärgade rutorna representerar den virtuella plattformen OpenSynergy för bilar.

rade. Den mjukvara som finns är huvudsakligen till för konfigurering.

En typ 1-hypervisor är ett tunt mjukvarulager som körs direkt på hårdvaran. Virtuella maskiner (VM) används för att isolera tjänster som körs oberoende av varandra i respektive VM, var och en av dem tilldelad specifika hårdvaruresurser.

Även tjänster från olika leverantörer kan utvecklas, driftsättas och uppdateras oberoende av varandra. Det kan göras till och med efter produktionsstart, utan att övriga tjänster behöver verifieras på nytt med avseende på deras realtidsegenskaper.

Stellar kör typ 1-hypervisorn COQOS från OpenSynergy. Med hjälp av hårdvarustödet i Stellar konfigurerar COQOS minnesgränser och åtkomsträttigheter till målsystem och delade resurser.

COQOS har fulla rättigheter och är den som initialt konfigurerar hela systemet. Den tilldelar alla gäster en VMID (Virtual Machine ID) som används av brandväggarna för att validera accesser.

Om det behövs virtualisering eller separation stöder hårdvaran även virtualisering av interrupt.

På så sätt kan funktioner inom olika domäner (till exempel kaross, cockpit, ADAS) köras tillsammans och samtidigt på en enda Stellarbaserad ECU. Prestandan är hög nog för att det ska finnas utrymme för att integrera ännu fler funktioner.

Zonstandardisering på Virtio

Framtidens arkitekturer för fordon kommer att försöka gruppera funktioner rumsligt. De kommer att använda så kallade zondatorer för att minska kabeldragningen.

Systemen i QOQOS kan kommunicera med varandra utan hårdvara via virtuella enheter. För detta utnyttjas standarden Virtio som OpenSynergy är aktivt involverad i via konsortiet Oasis Open sedan 2018.

Fysiska Can-bussar ersätts av virtuella Virtio-Can-bussar, som utnyttjar delat minne. Kontakter kan även tas mellan virtuella maskiner via Virtio-vsock eller Virtio-net beroende på tillämpning.

Dessa virtualiseringar kan sammantaget resultera i en viktminskning på upp till 70 kg, utöver de minskade kostnaderna för integration.

Användningsfall

Bilens systemarkitektur kan delas upp i zoner. Zondatorer i fordonets främre, mellersta och bakre del kommunicerar via en central gateway. Den vidarebefordrar data snabbt och på ett sätt som är säkrat mot angrepp.

En Zonal Front Computer i fordonets front är ett exempel på var en Stellar-MCU skulle kunna passa in, med Virtio-baserad hårdvara och en COQOS-hypervisor. Den skulle exempelvis kunna hantera karossfunktioner, IO-aggregering, kraftdistribution och några av ADAS-sensorerna.

Det finns ett strikt separationskrav på alla nivåer på all firmware. Säkerhet, timing och cybersäkerhet får inte äventyras, inte heller funktionalitet. En ASIL-D-applikation får inte äventyras av någon annan mjukvara och ett byte till en ny firmware-image får inte påverka övriga funktioner i mikrokontrollern.

Med bytet till Stellar fick STMicroelectronics en ARM-baserad plattform med stöd för en typ 1-hypervisor. Placeringen av icke-flyktiga minnen (NVM) i kluster gör att denna MCU-familj lämpar sig för integrationsplattformar och zonarkitekturer.

Slutsats

EE-arkitekturer måste minska sin materialanvändning för att tillverkarna ska kunna bygga lättare fordon – trots det ökande antalet funktioner i alltmer automatiserade bilar. Komponentbristen och de skyhöga bränsle- och elpriserna gjorde målet ännu viktigare. Den dag är förbi då det gick att höja prestanda genom att höja klockfrekvensen eller lägga till fler processorkärnor.

Samspelet mellan integrerad hårdvaruvirtualisering och nya hypervisorer som mångfaldigar deras funktionalitet är en effektiv lösning.

Eftersom lösningen skiljer hårdvara från tillämpningar går det att planera en arkitektur utan att börja grubbla över hårdvara och portering. När programvaran är färdig kan tillverkarna bestämma vilka och hur många SoC:er som efterfrågad beräkningskraft kräver. Här finns många möjligheter till innovation när det gäller utformningen av en Zonal E/E-arkitekturer. ■