Mjukvarukrav i nästa

Fem-i-topp bland åtgärder som ger säkrare och robustare ADAS-system

Av Peter Hoogenboom, Green Hills Software

Peter Hoogenboom är teknikchef i EMEA hos Green Hills Software i Nederländerna med över 30 års erfarenhet inom utveckling av inbyggda system. Från utveckling av kompilatorer och debuggers (1984), över till realtidsoperativsystem (1998) och hårdvaruprobar (2000), till BSP-utveckling för INTEGRITY RTOS och säkra arbetsstationer. Sedan 2008 har Peter hanterat funktionell säkerhet och säkerhetsrelaterade certifieringsprojekt.

Nästa generation ADAS (automatiska förarstödssystem, och kanske på sikt helt förarlösa bilar) ställer programutvecklare och systemkonstruktörer av fordon inför till synes oförenliga krav på säkerhetscertifiering, datasäkerhet, signalbehandling och visualisering. I denna artikel presenteras fem viktiga överväganden för OEM:er, leverantörer och underleverantörer som vill kunna skapa lyckad programvara, infrastruktur och produkter för ADAS.

5. Stöd programuppdatering!

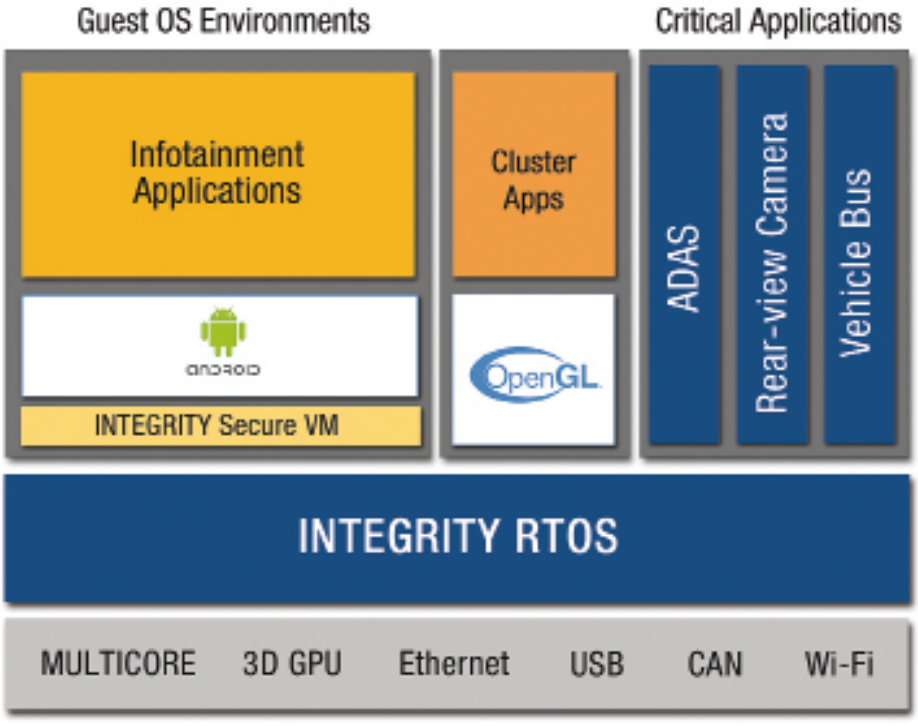
Äldre förarassistanssystem, till exempel enkla elektroniska instrumentkluster, kännetecknas av att de var relativt små program i enkla operativsystem som OSEK och AUTOSAR, och utvecklades av programmerare med erfarenhet av säkerhetskritiska utvecklingsprocesser.

Nästa generation ADAS kännetecknas av mer extrema krav, som exempelvis 3D-grafik med stora mängder kod, och måste dessutom eventuellt integrera programvara från tredje part utvecklad av konstruktörer utan formell bakgrund inom säkerhetskritisk programvaruutveckling. Konstruktörer måste planera för att kunna möta tuffa utmaningar i dessa allt mer komplexa system och bygga ett pålitligt och skalbart system för patcher och uppdateringar.

Marknaden för mobila enheter har visat att det är viktigt och praktiskt med uppdatering av programvara, alltifrån från den lägsta nivån av firmware upp till hela mobila operativsystem och applikationer. Mobiltelefontillverkare har gjort ett beundransvärt arbete med att utveckla och distribuera denna funktionalitet.

SÄKER UPPDATERING i fält kräver en kryptografisk infrastruktur inbyggd i SoC:n och systemprogramvaran. I synnerhet måste programvaran kontrolleras för sin integritet och äkthet via digitala signaturer, vars verifieringsnyckel måste skyddas mot manipulering som kan ske både via programvara eller fysiska angrepp. Verifieringsnyckeln måste ligga i åverkanssäker nyckellagring on-chip eller vara skyddad av en hårdvarubaserad nyckel.

Systemprogramvaran som används för att utföra valideringen måste själv vara skyddad mot manipulering med en kombination av säker boot, dynamisk integritetskontroll och fjärrattestering.



Figur 1. ADAS-delsystem och icke-kritiska partitioner konsoliderade på en flerkärnig processor.

4. Uppfyll ISO 26262 ASIL D !

Medan många äldre elektroniska styrsystem utvecklades av små, erfarna team med en etablerad kompetens i att leverera säkra och tillförlitliga programvaror, kräver omvandlingen till sofistikerad ADAS en formaliserad process som kan garantera att den funktionella säkerheten inte bara blir en eftertanke.

Säkerhetsstandarden ISO 26262, som först publicerades 2011, syftar till att ge vägledning och har i allmänt mottagits väl i hela fordonsbranschen. Verkställighet saknas dock eftersom regeringarna ännu inte har utfärdat ett enda ISO 26262-krav.

LEDANDE AKTÖRER inom fordonsindustrin, inklusive vissa OEM-företag och underleverantörer, ser ISO 26262-efterlevnad som ett internt krav och ett mål för att möta de utmanande funktionella säkerhetskraven i ADAS och andra system.

Att åtminstone skaffa sig kompetens inom ISO 26262 och visa på en förmåga att möta den högsta nivån (ASIL D) och att väl-

generation ADAS

ja leverantörer som kan göra detsamma (till exempel via oberoende bedömning av TÜV) – ger en konkurrensfördel.

EN UTVECKLARE KAN SKRIVA ett perfekt program men det kan fortfarande bli fel om kompilatorn misslyckas med att korrekt översätta källkod till maskinkod. ISO 26262, som behandlar användning av verktyg för programvaruutveckling av säkerhetskritisk programvara, kräver kvalificering av verktyg genom en kombination av utvecklingshistoria (förtroende genom användning), utvärdering av verktygsleverantörens utvecklingsprocess och validering av verktygets funktionalitet. Verktyg som klassificerats på högsta kvalifikationsnivå, T3, genererar som utdata kod som är körbar på säkerhetsrelaterade system. Även om ett antal kompilatorleverantörer hävdar att de har en certifierbar kompilator eller kvalificeringspaket som kan certifieras av en tillverkare, har hittills endast C-kompilatorer från Green Hills och ARM certifierats av oberoende part för användning i ISO 26262 ASIL D-system (oberoende certifierade av TÜV).

3. Integrera konsumentteknik på ett säkert sätt!

Nästa generation ADAS utnyttjar avancerad grafik, signalbehandling och andra sofistikerade program och algoritmer. ADAS utnyttjar multimediainnovationer från hemelektronik som mobiler och spel och konstruktörer måste vara uppdaterade på relaterade standarder som OpenGL, OpenVG, OpenVX och OpenCL.

En stor utmaning ligger dock i att förena komplexa hemelektronikprogram med kraven på funktionell säkerhet (dvs. ISO 26262). En teknik för att kunna införliva generell programvara, inklusive öppen källkod, i ett säkerhetskritiskt system är att använda systemvirtualisering för att isolera säkerhetskritiska komponenter från komplexa kodpaket som inte kan uppfylla säkerhetskritiska standarder.

Via virtualisering kan dessa komplexa delsystem vara fullvärdiga gästoperativsystem som körs i virtuella maskin under kontroll av en säkerhetsklassad hypervisor. Till skillnad från en traditionell hypervisor kan en fordonshypervisor vara värdsystem för både riktiga realtidssäkerhetsapplikationer och gästoperativsystem. Hypervisorns strikta resurshantering och skyddsmekanismer ser till att den virtuella maskinen och dess ingående program inte kan påverka exekveringen av kritiska applikationer.

NÄR DET GÄLLER ADAS måste tyvärr ofta komplexa delsystem användas i säkerhetskritiska sammanhang. Exempelvis kan en högupplöst grafisk 3D-display användas för att informera föraren om risker längs vägen.

Mycket få run-time-mjukvaruplattformar i världen kan göra anspråk på att stödja kombinationen av efterlevnad av ISO 26262 ASIL D och 3D-grafik samtidigt. Till exempel har Green Hills Softwares realtidsoperativsystem INTEGRITY, en välkänd plattform som används av flera säkerhetsystem inom fordonsbranschen, stöd för OpenGL, fullt accelererad grafik och drivrutiner till många populära fordons-SoC:er, som Freescales i.MX, TI:s Jacinto, Renesas R-Car och processorn Intel Atom E3800.

LÅT OSS ÅTERVÄNDA till kraven i ISO 26262! ASIL D är den högsta definierade säkerhetsnivån i ISO 26262, men inte varje komponent eller delsystem i bilen eller ens inom en enda komponent måste uppfylla denna nivå. ISO 26262 inför begreppet ASIL-nedbrytning via mjukvarupartitionering. Till exempel kan ett ASIL C delsystem bestå av en ASIL B-partition och en ASIL A-partition.

Om man tillräckligt väl kan kontrollera att partitionerna inte påverkas av störningar, kan den totala säkerhetsfunktionen av delsystemet valideras och verifieras till ASIL C.

Således kan ett operativsystem eller en hypervisor med hög säkerhet (certifierat enligt ASIL D) minska den totala systemkostnaden genom att minska ASIL-kraven på ingående komponenter och tillåta (försiktig) användning av komplexa programvarupaket som är opraktiska att säkerställa på högre nivåer.

2. Användaren ska inte behöva lita på systemet

Ett av de dominerande diskussionsämnena 2014, och fortfarande 2015, är den uppkopplade bilen och de inneboende säkerhetsrisker som är förknippade med att införa trådlös kommunikation (särskilt WAN) i bilen.

Helst skall säkerhetskritiska delsystem i bilen vara fysiskt isolerade från multimedia och telematikdelsystem som kan dra nytta av en sådan uppkoppling. Emellertid ersätter systemkonstruktörer i allt högre grad fysisk isolation med logisk isolation och programvarubrandväggar för att upprätthålla isolering av delsystemen. Forskare har visat att när ihopkoppling förekommer kan tyvärr sårbarheter i de olika delsystemen utnyttjas för att hoppa över den logiska isolationen mellan säkerhetskritiska och icke-säkerhetskritiska system.

EN ANNAN VIKTIG TREND diskuterades som tidigare: uppdatering i fält. För att uppdatera ett säkerhetskritiskt delsystem, måste det finnas en väg från utvecklaren till det uppdateringsbara delsystemet i bilen. Ironiskt nog är det fjärråtkomst för programuppdateringar, diagnostik, och insamling av andra viktiga data som har gjort det möjligt för angripare att utnyttja det stora utbudet av sårbarheter i programvaruintensiva produkter. I själva verket är detta utan tvekan den allvarligaste säkerhetsrisken för Internet of Things (IoT) idag.

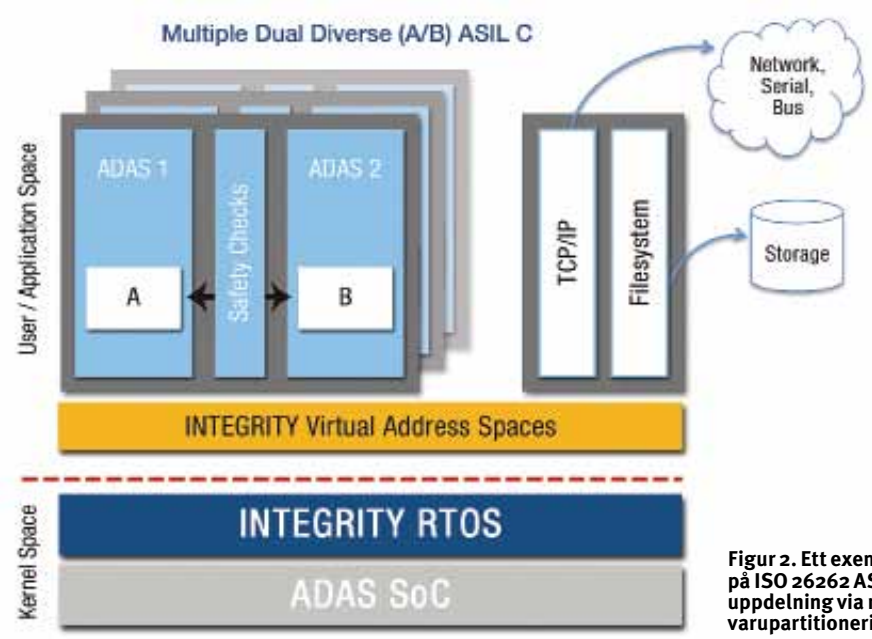
ÅTERIGEN, högsäker logisk isolering kan lösa många av dessa problem. Men ”hög säkerhet” är otroligt sällsynt i modern elektronik. När detta skrivs, har den amerikanska regeringen bara utfört en enda högsäker programvarucertifiering enligt säkerhetsstandarden ISO 15408 Common Criteria (för en enda produkt, Green Hills Softwares INTEGRITY-178B), och regeringsprogrammet för att främja dessa höga Common Criteria-certifieringar avslutades för flera år sedan på grund av kostnader och överskridna tidsplaner (läs: den statliga byråkratin).

Biltillverkare och viktiga underleverantörer är hänvisade till att lita på oberoende bedömningar av säkerhetskonsulter och deras säkerhetsrenommé samt erfarenheten hos sina underleverantörer.

BRANSCHEN MÅSTE OCKSÅ ta steg för att skydda sekretessen för den information som genereras inom ADAS och andra intelligenta delsystem och som distribueras till molnet för analys och monetarisering m.m.

Innehavet av sådana uppgifter kan vara osäkert men är helt klart värdefullt. Aggregering av denna information från många miljontals bilar presenterar ett lockande mål för sofistikerade, välfinansierade angripare. Dataägare måste anta en hållning av så kallat nollförtroende där användare är den som ska kräva ägande och kontroll av de privata nycklar som används för att skydda information.

Genom att behandla dataskydd i samband med valet av systemprogramproto-



Figur 2. Ett exempel på ISO 26262 ASIL-uppdelning via mjukvarupartitionering.

koll och produkter kan skyddet av den personliga integriteten tillgodoses på ett skalbart sätt. 2014 kanske blir känt som året för SSL-fiaskot på grund av en otrolig mängd misslyckanden: POODLE, Heartbleed, Apples goto-fail-misslyckande, och andra. Dessa sårbarheter bör förhoppningsvis skicka några tydliga signaler till industrin som:

– Att slå på SSL (eller andra överföringsprotokoll) är inte en strategi för IoT-dataskydd
– Öppen källkod har ingenting med säkerhetsnivåer att göra
– Hög säkerhet är den enda vägen till att förebygga sårbarhet

1. Bestäm inte hårdvaran förrän punkterna 2 till 5 är behandlade

Alltför ofta fattas kritiska och oåterkalleliga hårdvarubeslut med liten eller ingen hänsyn till de punkter som diskuterats ovan. Databehandlingskapaciteten (FLOPS) och stycklistor (BOM) fortsätter att dominera inköpsbeslut, vilket system- och mjukvaruingenjörer beklagar. Det ska komma en dag, förhoppningsvis snart, när beslutet om att välja en viss ADAS SoC kommer grundas på SoC:ns säkerhets- och säkerhetsfunktioner (t.ex. Trustzone, ARM virtualiseringstillägg, MMU:er, IOMMU:er, skyddad nyckelförvaring ”on-chip”, högkvalitativa RNG:er, debugfunktioner som trace m.m.) och tillgängliga programvaruekosystem som kan utnyttja sådana funktioner då betyder lika mycket som enhetens processorkraft per dollar. ■