EXPERTARTIKEL

Spärra smygvägar till

En färsk ISO-standard och ett certifierat RTOS hjälper dig hindra angripare från att komma åt bilens säkerhetskritiska system

Av Ryan Kojima, Green Hills Software

Ryan Kojima är mjukvarukonsult för avancerade produkter inom området inbyggda system. Han lärde sig om elektronik och IT på Suzuka National College of Technology i Japan. Tidigt i karriären arbetade han som systemingenjör med konstruktion och implementering av utskrifts-automationssystem. 2018 började han arbeta på Green Hills Software.

Fordon innehåller alltmer avancerade och komplexa mjukvarusystem. Tillverkarna tävlar om att kunna bjuda på de bästa upplevelserna i bilen.

Detta har bland annat medfört att ny kommunikationsteknik och nya gränssnitt stoppats in i bilen. De används inte bara av passagerarna utan även av tillverkarna och i trafikinfrastrukturen för att ansluta trådlösa nycklar, strömma musik och video, uppdatera programvara trådlöst (OTA, over-the-air), för V2X-kommunikation, med mera – se figur 1.

Var och en av dessa datakanaler är en potentiell riskfaktor för cyberattacker av ett slag som när de sker kan drabba samtliga tillverkade bilar i en årsmodell.

Artificiell intelligens och autonoma system används alltmer för att fatta beslut på data som samlats in i realtid. Besluten omfattar merparten av kritiska by-wire-system i bilen, inklusive broms och styrning. Därmed är det viktigt att konstruera bilens elektronik från grunden med cyber- och personsäkerhet för ögonen. Det är inget som kan adderas i efterskott.

Fordonstillverkarna är väl medvetna om utsattheten och att det finns sårbarheter. Men frågan är:

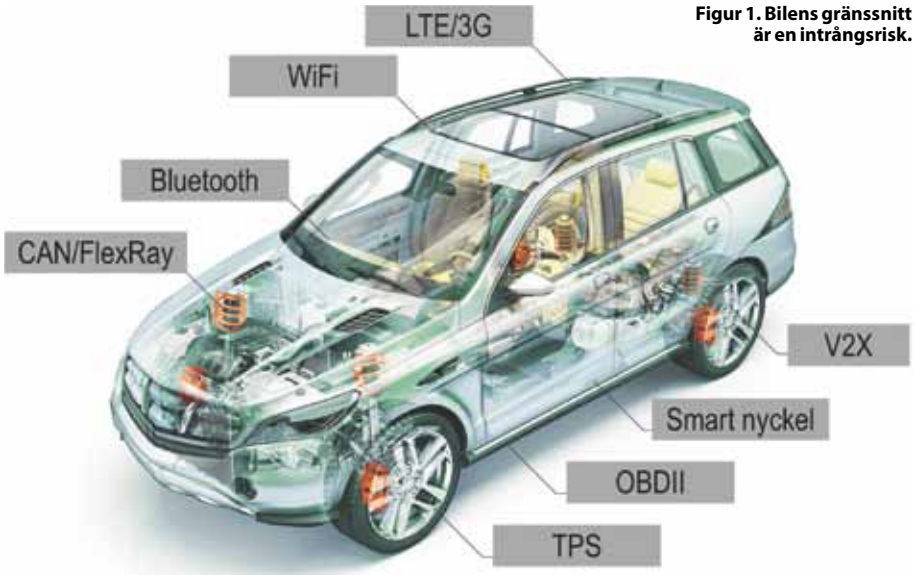
- Vad ska de egentligen använda för metoder och verktyg för att upprätthålla cybersäkerhet och för att bedöma och analysera risk?
- Vad ska de göra när de hittar en sårbarhet?
- Hur kan de minimera effekten på kundernas säkerhet – och på sitt varumärke?

Säkerhetsbekymmer i fordon

Det har under det senaste decenniet påvisats flera allvarliga sårbarheter som har fått säkerhetskritiska konsekvenser. Att attackera systemet genom kommunikationsgränssnitt som Bluetooth, Wi-Fi och LTE är standardförfarandet att skaffa sig tillgång till kritiska system, eftersom de är kopplade mot varandra internt i systemet.

Angripare utnyttjar typiskt en känd sårbarhet i informationshubben eftersom de vet att infotainmentsystemet ofta kör ett generellt operativsystem som Linux eller Android.

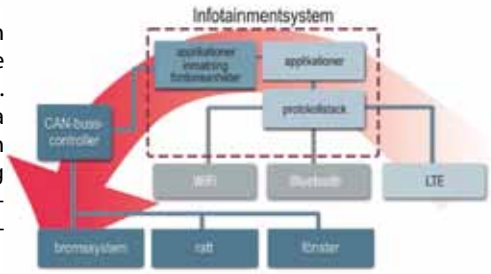
Efter att ha trängt sig in i systemet försöker programkod ta sig vidare till CAN, FlexRay, LIN eller andra bussprotokoll. CAN-bussen konstruerades och blev standard långt innan någon hade börjat oroa sig för att det skulle kunna finnas cybersäkerhetsrisker i en bil. Den kan vara ansluten till säkerhetskritiska moduler såsom motorsensorer, bromsar och transmission. Genom att skaffa sig tillgång till fordonet går det att analysera protokollen genom att spionera på trafiken på CAN-bussen.



Figur 1. Bilens gränssnitt är en intrångsrisk.

Som visas i figur 2 kan en typisk attack bestå av två faser. Den första är att attackera infotainmentsystemet och den andra att attackera fordonsbussens processor.

Tillverkaren kan placera en brandvägg och annan isolering mellan delsystem för att öka säkerheten. De måste dock utformas och utvärderas på ett korrekt sätt.



Figur 2. Möjliga attackvägar för en angripare.

Så kom ISO 21434 till

Med tanke på det rika utbud som finns av komplexa programkodsmoduler – varav vissa är från tredjepart och öppen källkod, som Linux och Android – vad kan utvecklare göra för att minimera risken för ett kritiskt systemhaveri?

Ett svar är att använda sunda processer för systemutveckling och kodning. Detta kan förhindra att sårbarheter uppkommer. Varje komponent måste granskas, inklusive hur den interagerar med andra kodkomponenter.

Historiskt har det inte funnits någon standard kring cybersäkerhet för bilar. Företag har utvecklat sina egna processer för att hantera den utmaningen.

När en sårbarhet upptäcks måste samtliga kunder och intressenter informeras. Programkoden måste korrigeras och ändringen distribueras. Alternativa möjliga scenarier för sårbarhet måste åtgärdas för att skydda de viktigaste, mest kritiska modulerna mot att vara fortsatt utsatta.

När det gäller funktionella aspekter på personsäkerhet är som bekant ISO 26262 en etablerad standard. Den ställer krav på granskning av kodkomponenter. Den tar dock ingen hänsyn till att mjukvara har en livscykel, exempelvis via OTA-uppdateringar. Och den utvecklades inte som en standard för datasäkerhet (security).

ISO 21434 däremot, är ett ramverk som uttryckligen adresserar cybersäkerhet i fordon och är en av de säkerhetsstandarder som

cyberattack mot bilar

stöds av realtidsoperativsystemet INTEGRITY från Green Hills Software.

ISO 21434 har vuxit i betydelse alltefter-som regeringar världen runt antagit ny lagstiftning baserad på UNECE WP.29 (UNECE World Forum for Harmonization of Vehicle Regulations) – en reglering som adresserar system för CSMS (cybersecurity management systems) i fordon.

ISO 21434 ger vägledning till den som vill realisera CSMS-kraven i UNECE WP.29. Den täcker hanteringen av cybersäkerhet från koncept och utveckling till drift. Den definierar ett gemensamt språk för att diskutera cybersäkerhet.

Standarden hjälper till att skapa förståelse för vad som kan gå fel, hur en cybersäkerhetsavdelning kan organiseras och hur man kan kontrollera och hantera problemen. Den definierar termer för risk inom cybersäkerhetsområdet – det är viktigt att använda samma terminologi för att organisationer och företag ska kunna kommunicera internt utan missförstånd.

ISO 21434 täcker hanteringen av en komplett livscykel snarare än bara en specifik teknik, metod eller system. Traditionell säkerhetsmetodik tar inte hänsyn till så mycket annat än serietillverkning. När utvecklingen är klar och certifierad fryses koden.

Livscykelhantering täcker ett bredare område och inkluderar även drift och underhåll. ISO 21434 beskriver hur riskbedömningar kan göras i varje del av livscykeln.

Standarden ger vägledning för att identifiera vilka resurser som behöver skyddas. Den adresserar riskscenarier och utvärdering av riskernas dignitet. Vilka möjliga sätt finns att ta sig in i fordonsnätverket? Kan det göras på distans, eller måste angriparen befinna sig nära fordonet? Behöver angriparen komma åt fordonet fysiskt?

Vissa resurser är direkt relaterade till säkerhet. Andra är inte det. Om bromssystemet slutar fungera kan det resultera i allvarliga skador medan stöld av personlig information visserligen är ett problem, men inte ett säkerhetskritiskt sådant. Standarden visar hur man gör riskvärdering på ett systematiskt sätt och ger verktyg för att bedöma effekten av attacker.

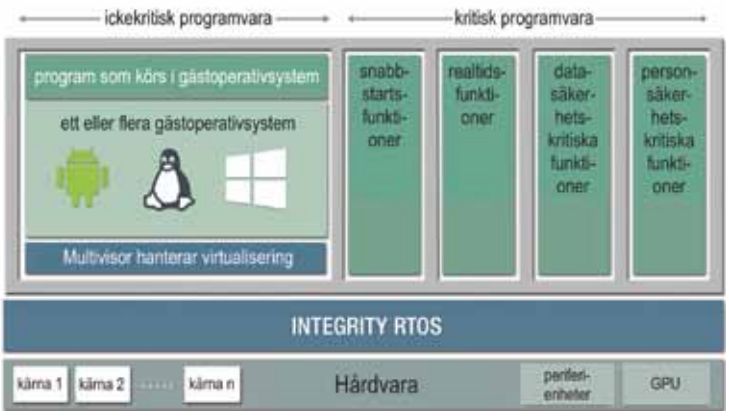
Den som vill ha de bästa produkterna måste använda de bästa utvecklingsmetoderna.

Med rätt verktyg och rätt processer blir det enklare att hantera en produkts livscykel. Ett person- och datasäkerhetscertifierat realtidsoperativsystem (RTOS) är avgörande för den som vill utveckla kodmoduler som är ogenomträngliga för cyberattacker. Ett sådant RTOS eller en sådan separationskärna använder minnesskydd i hårdvara för att isolera och skydda såväl drivrutiner och tredjepartskod som kommunikation och inbyggda applikationer. Det kan till och med ladda en eller flera instanser av Android eller Linux.

Säkrad partitionering garanterar att användarnas funktioner hålls separerade. Lösningen är mer robust än den som typiskt används i generella operativsystem som Linux. Till exempel är heapen (en minnespool) separerad, så att en minnesläcka i en applikation inte kan spilla över till andras adressutrymmen. Genom att minimera störningsvägar mellan applikationer blir riskbedömning mer hanterbar och det skapas fler möjligheter att mildra och prioritera risk.

Titta på diagrammet i figur 3. Det visar vad en strikt separerande realtidsarkitektur kan göra. Den exekverar diverse olika gästoperativsystem samtidigt med verksamhetskritiska realtidsprogram. Applikationernas och gästoperativsystemens processer schemaläggs på en eller flera cpu-kärnor. De kan kommunicera effektivt med varandra och ges enligt strikta regler åtkomst till gemensam kringutrustning, såsom GPU och Ethernet.

Separationsarkitekturen gör att RTOS:et strikt kan isolera partitioner från varandra. Det går att därmed att bestämma vilka moduler som kan prata med bussgränssnittet, vilket ökar systemseparationen och därmed säkerheten.



Figur 3. Ett realtidsoperativsystem certifierat för personsäkerhet (safety) och datasäkerhet (security). Det isolerar gästoperativsystem och funktioner från varandra.

ISO 26262-certifierade utvecklingsverktyg är ytterligare en nyckel till att garantera cybersäkerheten i ett system. ISO 21434 tar upp MISRA C, ett regelverk för utveckling i programspråket C, som något som kan användas för att minimera risk. MISRA (Motor Industry Software Reliability Association) räknar upp språkkonstruktioner i C som bör undvikas på grund av de är tvetydiga eller lätt används fel av misstag. Ta till exempel följande kod, som illustrerar två vanliga misstag i C:

if (flagga && (totalt = antal++)) {…}

Programmeraren ville troligen skriva *"totalt == antal++"* (observera det dubbla likhetstecknet). Så koden ger inte det väntade resultatet.

Det andra misstaget gäller variabeln *antal* – kommer den att ökas med ett eller inte? Det beror på. Om *flagga* är falsk kommer inte *antal* att ökas. MISRA-riktlinjerna styr bort från att konstruera uttryck på detta sätt, och reducerar därmed denna typ av misstag.

MISRA C är en uppsättning regler för mjukvaruutvecklare. Det är inte en specifikation för en kompilator. Att inspektera koden för hand vore en mödosam process så det är en bättre idé automatisera så att riktlinjerna tillämpas konsekvent.

Därmed blir det även centralt att välja en C-kompilator som stöder MISRA C 1998, 2004 och 2012 (den senaste versionen) och de vanligaste processorerna i fordonssystem, som Arm, RH850, Power, MIPS och x86.

Slutsats

Med tanke på det växande antalet externa kommunikationsgränssnitt och de diverse olika applikationer och operativsystem som tagits i bruk, har moderna bilar en stor angreppsyta för cyberattacker. Även när sårbarheter identifierats och motåtgärder tagits fram, är det en extremt kostsam och utmanande process att på ett säkert sätt uppdatera system och installera kodrättelser i stor skala.

Standarden ISO/SAE 21434 publicerades i augusti 2021 och tillhandahåller ett ramverk speciellt utformat för att hantera cybersäkerhet i fordon.

ISO 21434 är avgörande för att omsätta de CSMS-krav som finns i UNECE WP.29 (som nu antas över hela världen) till praktik. Följaktligen är det viktigt att använda ett RTOS som är certifierat för person- och datasäkerhet och har stöd för ISO 21434, som Green Hills INTEGRITY. Dessutom är det centralt att använda en certifierad, kompatibel verktygskedja för att garantera säkerhet vid utveckling av inbyggda system för användning i fordonstillämpningar. ■