OMVÄRLDSBEVAKNING
- MÖJLIGGÖRANDE ELEKTRONIK & MJUKVARA

TEMA
Robusta
System av System

Detta är en omvärldsbevakning som genomförs inom FFI fokuserande på möjliggörare inom elektronik och mjukvara. Avsikten är att inspirera svensk produkt-utveckling och forskning till nya innovationer.

Temat i denna utgåva av omvärldsbevakningen är robusta system av system. På lång sikt är fullt autonoma fordon i samverkan givetvis ett tydligt exempel på behovet av robusta system av system, men redan nu börjar system av system i form av delad information för strategisk och taktisk planering av körning att komma nära marknaden.

I denna omvärldsbevakning har vi valt att länka till flera rapporter som kräver abonnemang från t.ex. IEEE. Universitetsbibliotek eller bibliotekstjänster på företag kan ofta hjälpa till att ta fram artiklarna.

Innehåll:

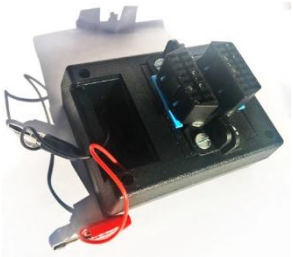
Denna omvärldsbevakning produceras av SICS Swedish ICT som en del av FFI satsningen Möjliggörande Elektronik och Mjukvara i delprogrammet EMK. Se http://www.vinnova.se/sv/ffi/FFI-PROGRAM/FFI---Fordonsutveckling/
För mer information kontakta Eilert Johansson, SICS Swedish ICT. eilert@sics.se

HOT NEWS:

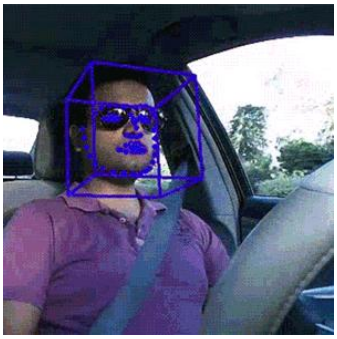
Nära realtidsvideo över Ethernet
Ethernet Audio Video Bridging (Ethernet AVB) är ett samlingsbegrepp för digital video med låg fördröjning över IEEE802 nätverk. Renesas har just tagit fram ett nytt chipset R-Car T2 som stödjer Ethernet AVB. Enligt tillverkaren stödjer man komprimerad HD video men med låg fördröjning, mindre än 1ms. R Car T2 kompletterar de tidigare R-Car produkterna med Ethernet AVB stöd.

Komplexiteten i fordonselektronik nära ett skifte
Mängden funktioner i nya fordon ökar lavinartat och att lägga till fler styrenheter är inte längre hållbart enligt en ny studie. Samtidigt konstaterar studien att alla betydande trender inom fordons-branschen möjliggörs av funktionalitet realiserad i mjukvara och elektronik. Studien konstaterar att steget över till multicore-processorer behöver tas så snart som möjligt. Det innebär betydande kostnadsbesparingar och ökad prestanda.

Nytt pilotprogram kring fordonskommunikation
Amerikanska Department of Transportation har beslutat att finansiera tre pilotprogram för nästa generations sammankopplade fordon. På Manhattan kommer tusentals bilar och trafiksignaler delta i en studie av kommunikation mellan fordon samt mellan fordon och infrastruktur. I Florida kommer kommunikation mellan fotgängares smartphones och fordon utvärderas, medan forskare i Wyoming ska fokusera på att insamla trafikinformation från lastbilar på motorvägar. Förhoppningen är att datainsamlingen ska ligga till grund för framtidens smarta trafik-lösningar.



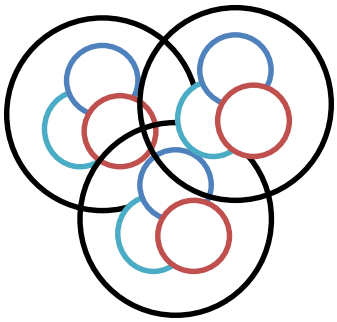
Hackerverktyg som öppen källkod
Vid den årliga hacker-konferensen DerbyCon i slutet av september presenterades ett verktyg utvecklat för att hitta sårbarheter vid uppdatering av mjukvara i bilar. Verktygsutvecklaren Craig Smith, känd som författaren till "Car Hacker's Handbook", förklarade att med hårdvara för ett par hundralappar och hans mjukvara kan flera avgörande säkerhetsbrister identifieras. Källkoden ligger fritt tillgänglig på GitHub.



Deep learning förutspår förarens nästa manöver
En studie från Cornell University och Stanford visar att en dator kan tränas att känna igen förarens kroppsspråk, t.ex. inför en omkörning. Med hjälp av s.k. *deep learning* förutspår deras system filbyten med över 90% träffsäkerhet. Forskarna tänker sig att tekniken kan användas för framtida varningssystem i samband med riskfyllda manövrar, särskilt i kombination med kameraövervakning av "döda vinkeln" eller framtidens sammankopplade fordon.

Denna omvärldsbevakning produceras av SICS Swedish ICT som en del av FFI satsningen Möjliggörande Elektronik och Mjukvara i delprogrammet EMK. Se http://www.vinnova.se/sv/ffi/FFI-PROGRAM/FFI---Fordonsutveckling/
För mer information kontakta Eilert Johansson, SICS Swedish ICT. eilert@sics.se

TEMA
Robusta System av System



Vad är system av system?

Ett system av system (SoS) består av flera system som samverkar för att uppnå ett mål men där systemen utvecklas vart och ett för sig och uppfyller sina enskilda ändamål oberoende av helheten. Fordon uppträder allt oftare i SoS. När en förare använder en app på sin smarta telefon för att navigera så är det ett tydligt exempel på hur två system – bilen och telefonen – som både utvecklats och fungerar separat samverkar för att skapa en smartare transport.

Tack vare billigare plattformar för informations- och kommunikationsteknologi tillsammans med ökad digitalisering av de flesta produkter blir SoS en allt viktigare trend. Läs gärna mer i omvärldsbevakningen från april förra året.

Vad är robusthet i system av system?

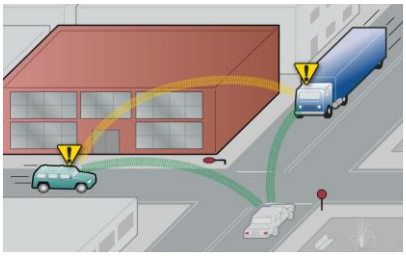
Trenden mot allt fler SoS väcker många nya frågeställningar. Hur kan man säkerställa att system som används ihop inte är farliga för förare, passagerare och fotgängare? Vad händer om något del-system börjar uppträda oväntat, eller om trafiksituationen plötsligt förändras på ett oförutsett vis? Hur hanteras icke anslutna fordon? Kan ett angrepp med skadlig kod på ett system sprida sig i hela systemet av system? Fungerar allting både på landet och i stads-miljö, under olika väderförhållanden eller i närheten av starka radiosändare?

Den här typen av frågeställningar sammanfattas ibland med begreppet robusthet. IEEE definierar robusthet som hur väl ett system eller en komponent fungerar trots ogiltig indata eller påfrestande förhållanden. Robusthet ersätter inte andra egenskaper som tillförlitlighet eller säkerhet (varken *safety* eller *security*). Däremot tillför robusthet ett relevant perspektiv, inte minst på SoS där traditionella metoder inte går att tillämpa. Ett robust system behöver inte vara (helt) säkert, däremot är säkra system ofta robusta. Ett SoS som konstruerats med robusthet i åtanke når kanske inte kraven på formell verifierbarhet med temporallogik– men det är troligen säkrare, i informell mening, än ett SoS som konstruerats utan robusthetshänsyn. Översikten nedan gör ett antal nedslag på olika områden i syfte att teckna en bred bild av vad robusthet i SoS kan innebära.

Person- och fordonssäkerhet

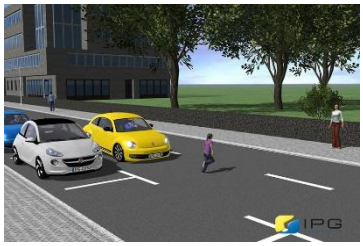
Ett av de främsta skälen att eftersträva robusta SoS i fordons-branschen är att främja säkerheten på vägarna. En uppsjö av forskning utlovar lösningar som bidrar till säkrare trafik-SoS, men om robustheten brister faller förslagen ofta platt. En av utmaningarna med att etablera robusta säkerhetslösningar är att det krävs en omfattande samordning av datakommunikation, signalbehandling och reglerteknik – en samordning som ska implementeras i mjukvara!

Denna omvärldsbevakning produceras av SICS Swedish ICT som en del av FFI satsningen Möjliggörande Elektronik och Mjukvara i delprogrammet EMK. Se http://www.vinnova.se/sv/ffi/FFI-PROGRAM/FFI---Fordonsutveckling/
För mer information kontakta Eilert Johansson, SICS Swedish ICT. eilert@sics.se



National Highway Traffic Safety Administration i USA meddelade förra året att de välkomnar så kallade *public comments*, dvs. underlag inför en kommande utredning kring ett tvingande regelverk gällande Vehicle-to-Vehicle-kommunikation (V2V) i nya fordon. I en tillhörande rapport bedöms två V2V-tillämpningar, stöd för vänstersväng och korsningar, tillsammans kunna förebygga 592 000 olyckor och rädda över 1 000 amerikanska liv per år.

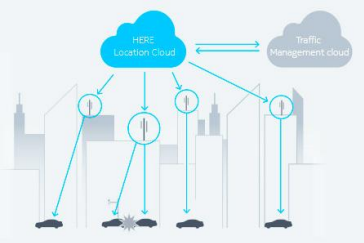
En stor del av forskningen behandlar tekniker för att undvika kollisioner mellan fordon. En vanlig olyckstyp är påkörning bakifrån som ligger bakom cirka 10 % av dödsfallen i trafiken. Ett problem med säkerhetslösningar som bygger på kommunikation via exempelvis WLAN, Bluetooth eller infrarött ljus är att systemen av system då behöver samverka kring en helt ny telekom-infrastruktur. Benedetto et al. (2015) föreslår istället en betydligt mer lättviktig lösning, åtminstone för en initial fas av övergången till så kallade intelligenta transportsystem (ITS). Forskarna har visat att en lösning med radiosändare och mottagare på varje fordon kombinerat med tillämpad signalbehandling effektivt kan varna för kollisioner i trafiken.



På motorvägar bedöms olämpliga filbyten orsaka 20 % av trafikolyckorna. Flera olika forskargrupper har föreslagit automatiserat beslutsstöd som ska varna föraren för riskfyllda filbyten. Samiee et al. (2015) presenterade i somras en algoritm baserad på hastighet, avstånd till närliggande fordon samt friktion mellan däck och vägbana. Vidare presenterade de en ny modellbaserad utvärderingsmetod för assisterade filbyten i IPG CarMaker.

Att öka säkerheten i vägtunnlar är en annan säkerhetsorienterad tillämpning av SoS. Transport av farligt gods utgör en av de största riskerna i tunnlar. Forskning har visat att farliga transporter genom tunnlar av säkerhetsskäl bör begränsas till en åt gången. Chen et al. (2015) presenterade nyligen hur ITS kan användas för att koordinera denna typ av godstrafik med Förbifart Stockholm som konkret exempel.

Ett område som lätt glöms bort vid diskussioner av smarta SoS och ITS är fotgängarna – en oskyddad typ av trafikant som ofta är inblandad i dödsolyckor. Tahmasbi-Sarvestani et al. (2015) rapporterar i samverkan med forskare från Hyundai att Vehicle-to-Pedestrian-kommunikation (V2P) fått betydligt mindre uppmärksamhet än V2V och Vehice-to-Infrastructure (V2I). En förklaring är bristande data-kommunikation mellan fotgängare och fordon. Forskarna menar att situationen kan förändras då antalet smarta telefoner som erbjuder WiFi genom *tethering* ökar och de presenterar ett utkast på ett varningssystem för att förhindra att fotgängare blir påkörda.



HERE, i somras uppköpta av ett konsortium bestående av Daimler, BMW och Audi, har presenterat ett pilotprojekt som ska utveckla en plattform för att skicka ut varningar enligt EU:s direktiv för ITS. Plattformen, som kallas C-ITS Safety messages platform, är en molnlösning som inte kräver ny infrastruktur utan förlitar sig på det befintliga mobiltelefonnätet. När ett anslutet fordon detekterar en olycka skickas ett meddelande via 4G-nätet till HEREs moln, vilket därefter skickar ut meddelanden till övriga berörda fordon.

Trafik- och flödesplanering

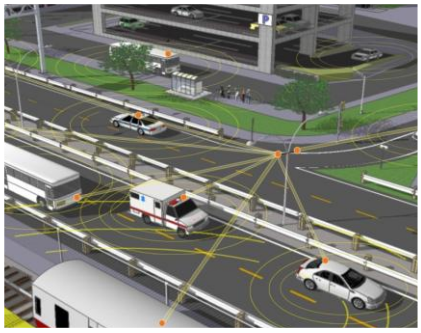
Trafiksituationen i ett större geografiskt område kan också betraktas som ett stort SoS. Papageorgiou et al. (2015) konstaterar i en översikt att individuellt ”smarta” fordon ändå kan uppträdda kollektivt ”dumt” och ge upphov till trafikstockningar och ineffektiva flöden – om inte trafikplaneringen börjar ta hänsyn till hur fordonsflottan utvecklas. Dagens trafikplanering måste ta hänsyn till exempelvis farthållare, valbara bränslebesparingslägen, fordonståg, navigations-hjälpmedel och system som hjälper föraren vid filbyten.

En annan nyligen publicerad och bra översiktsartikel, som sammanfattar befintliga tekniska lösningar och projekt inom trafikplaneringssystem (eng. *Traffic Management Systems* – TMS), är skriven av Djahel et al. (2015)

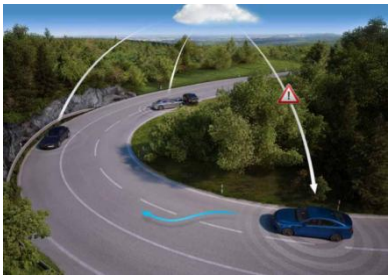
I september 2015 kungjorde amerikanska Department of Trans-portation att man investerar 42 miljoner dollar i ett pilotprogram för fordon som är uppkopplade mot varandra (V2V) och mot infrastruktur (V2I). Målsättningarna är flera, men i Tampa, Florida, syftar programmet till att lösa problemen med trafikstockningar i rusningstid – samt att skydda fotgängare som kan få varningar direkt till sina smarta telefoner.

Robusta VANET

Vehicular Ad Hoc Networks (VANET) är ett samlingsbegrepp för kommunikationsnätverk som skapas ad hoc främst mellan fordon (V2V) men även med infrastruktur som vägtullar eller sensorer längs vägarna (V2I) samt med fotgängare (V2P). Kommunikation kan ske via exempelvis WLAN, Bluetooth, infrarött eller synligt ljus. I april i år offentliggjorde Audi att de tillsammans med Autotalks har utvecklat en ny smart takantenn som integrerar all V2X-kommunikation.



Många av utmaningarna med VANET är gemensamma med vanliga mobila ad hoc-nätverk (MANET) – hur stor är risken att tappa signalen, hur robusta är nätverken när deltagare kommer till och försvinner? Det finns dock också specifika svårigheter som hänger ihop med trafikmiljön och de tillämpningar som fordonsbranschen vill lösa. Forskningslitteraturen innehåller många intressanta exempel på hur man uppnår robusta VANET – nedanstående exempel är alla från 2015.



Osman & Ishak (2015) introducerar en *CONnectivity ROBustness model* (CONROB) för att underlätta bedömningen av robustheten i kommunikation mellan fordon (V2V). Modellen tar hänsyn till bland annat fordonens rörelsemönster och avstånd, samt de olika kommunikationsmedlens räckvidder och förekomst på marknaden. Modellen är empiriskt validerad med hjälp av en testtrafikmiljö i Oregon.

Wang et al. (2015) har tagit fram en matematisk modell där fordonens rörelser kombineras med vågutbredningsförhållanden och protokollets datalänkoperationer för att beräkna bland annat throughput och sannolikheten för paketförlust.

VANET-trafikmiljöer skiljer sig drastiskt åt mellan exempelvis stad och land. Ali et al. (2015) studerar robusthet hos routing-protokoll i olika trafikmiljöer, inklusive förekomst av så kallade *road side units* i glesbygd och pekar ut vissa protokoll som mer stabila än andra. I en annan artikel föreslår Ren et al. (2015) så kallade differentiella successiva reläer placerade i fordon eller längs vägen som kan motverka problemen med instabila direktlänkar i VANET. Ett annat sätt att hantera risken att tappa uppkopplingen är att dynamiskt förutsäga när en länk kopplas ner, baserat på geografi och på hur fordonen rör sig. Kim et al. (2015) har designat protokollet *Robust link-oriented Routing* (ROR) utifrån den principen och visar lovande simuleringsresultat. Nguyen & Kong (2015) estimerar riskerna för VANET-avbrott genom att ta fram matematiska modeller för avbrottssannolikheter i tre olika kommunikationsprotokoll. En fritt tillgänglig översikt över litteraturen om VANET-protokoll som är robusta mot fördröjning ges av Kang et al (2015).

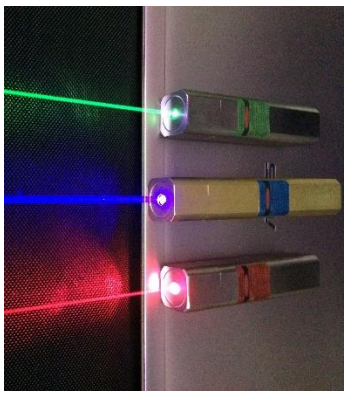
I samband med naturkatastrofer kan ett stort antal VANET-noder plötsligt försvinna helt. Ho & Chen (2015) visar hur virtualiserings-tekniker – för routrar och länkar – även under sådana omständlig-heter kan upprätthålla 80 % funktionalitet med bara 50 % av de ursprungliga noderna.

Picone et al. (2015) tar fasta på att VANET är system av system. Idag finns det en smart telefon i snart sagt varenda bil. Då borde man kunna upprätthålla en uppkoppling – med 3G, LTE, WiFi eller något annat – i väldigt många olika miljöer. Författarna berättar om resultaten av projektet X-NETAD, föreslår en arkitektur där smarta telefoner möjliggör realtidsutbyte av information och visar lovande experimentella resultat.

Antagonistiska attacker

Robustheten i VANET hotas inte bara av vågutbrednings-förhållanden och en ombytlig trafikmiljö. Illasinnade aktörer kan medvetet gå till angrepp. Sharma & Singh (2015) diskuterar metoder att avvärja *denial-of-service*-attacker i VANET. På liknande sätt går Sumra et al. (2014) systematiskt igenom tolv tänkbara attacker mot säkerheten (*confidentiality, integrity, availability*) i VANET.

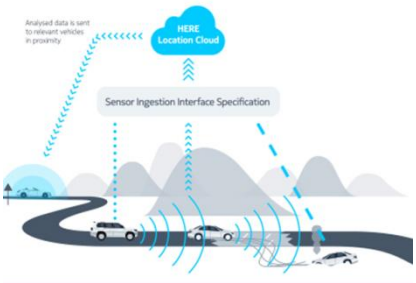
En säkerhetsanalys av VANET måste dock gå bortom rent datalogisk funktionalitet. Som ett SoS är VANET också känsliga för exempelvis radiostörning. Puñal et al. (2015) har studerat effekterna av störsändning och konstaterar att såväl konstant som periodisk och reaktiv störning kan omöjliggöra kommunikation i stora områden. Vissa typer av störsignaler kan vara effektiva trots att de är fem storleksordningar svagare än den störda signalen. I Sverige har Totalförsvarets forskningsinstitut FOI sedan flera år varnat för att den tidigare strikt militära förmågan att störa radiosystem nu sprider sig civilt och att billig störutrustning finns tillgänglig för gemene man via Internet.



Störsändning behöver inte ske på radiofrekvenser. En lämpligt programmerad laserpekare kan lura ett lidar-system i ett fordon att det finns andra bilar eller fotgängare när det egentligen inte finns några. Ett sådant system kostar bara några hundralappar.

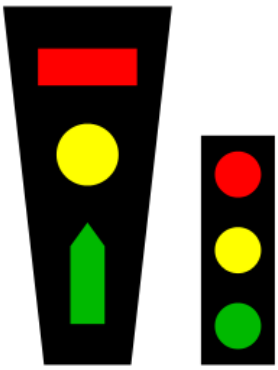
Standardisering

Ett naturligt steg mot robusta SoS är att utveckla tekniska standarder för kommunikation och samverkan. Framtidens fordon kommer att utbyta stora mängder data, vilket givetvis måste samordnas på något vis. Inom ITS-området finns en rad initiativ inom kommunikations-standarder med delvis överlappande ambitioner. ETSI (European Telecommunications Standards Institute), erkända av EU som ett standardiseringsorgan, publicerade i december 2014 två standarder för ITS: Cooperative Awareness Basic Service och Decentralized Environmental Notification Basic Service. Den förstnämnda hanterar kommunikation av position, dynamik och attribut mellan fordon och infrastruktur, medan den senare beskriver kommunikation av faror och trafikförändringar inom ett begränsat område, både V2V och V2I.



HERE publicerade i somras Vehicle Sensor Data Cloud Ingestion Interface Specification (*Sensor Ingestion*), en specifikation för att kommunicera sensordata från fordon. *Sensor Ingestion* uppmuntrar till industrisamarbete genom publicering under *Creative Commons*-licens. Specifikationen beskriver både gränssnitt och protokoll för att kommunicera data, från grundläggande information som position, hastighet och vikt till mer avancerad information som vägbeläggning, upptäckta vägskyltar och grad av assisterad körning.

Denna omvärldsbevakning produceras av SICS Swedish ICT som en del av FFI satsningen Möjliggörande Elektronik och Mjukvara i delprogrammet EMK. Se http://www.vinnova.se/sv/ffi/FFI-PROGRAM/FFI---Fordonsutveckling/
För mer information kontakta Eilert Johansson, SICS Swedish ICT. eilert@sics.se

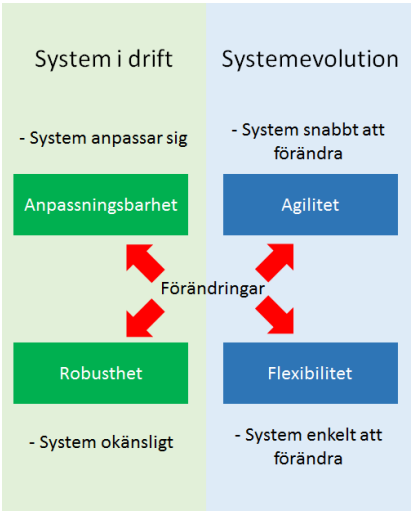


Det är värdefullt att studera utveckling av ITS-standarder även utanför Europas gränser. EU finansierar samverkan inom VRA-projektet (Vehicle and Road Automation), ett nätverk av forskare och ett konsortium av industripartners som syftar till att öka ITS-samarbetet mellan Europa, USA och Japan. I USA har flera steg mot framtidens SoS tagits, främst pådrivet av organisationen ITS America. I juni mottog USA:s kongress också propositionen Future Transportation Research and Innovation for Prosperity Act, eller kortare ”Future TRIP Act”, med syfte att låta Department of Transportation dra igång ett forskningsprogram för bred lansering av autonoma och sammankopplade fordon. Propositionen hävdar att ITS kommer att både rädda liv och effektivisera trafikflöde, men poängterar vikten av en tydlig färdplan för att nå de högt uppsatta målen. Ett konkret förslag i propositionen är att strikt begränsa 5,9 GHz-bandet till V2V-kommunikation.

Antagonistiska attacker blir som redan nämnts ett allt större hot mot framtidens fordon. Även denna typ av säkerhet kommer delvis att hanteras genom uppdaterade industristandarder och förändrade krav på certifiering. Schoitsch et al. (2015), fordonsforskare från Österrike, pekar på att framtidens funktionssäkerhet kommer att behöva hanteras på SoS-nivå snarare än för enskilda fordon, samt att vikten av *security* ökar med alla nya gränssnitt. Att hantera samspelet mellan *security* och *safety* är viktigt, vilket den senaste versionen av den generella standarden IEC 61508 lyfter fram genom att explicit uttrycka att *security* ska analyseras med avseende på *safety*. Schoitsch påpekar att sådan samordnad kravhantering försvåras av att *security* och *safety* kommer från olika skolor: Där *security* kräver regelbundna uppdateringar innebär en *safety*-certifiering snarare att man undviker förändringar. SoS är adaptiva till sin natur med nya system som läggs till och tas bort, vilket kommer att kräva viss dynamik inom framtidens fordonsutveckling. Slutligen rapporterar forskarna att olika branscher hanterar samspelet mellan *security* och *safety* på olika sätt, antingen som separata standarder (t.ex. i flygindustrin) eller integrerat (t.ex. inom kärnkraft).

Utveckling med robusthet i fokus

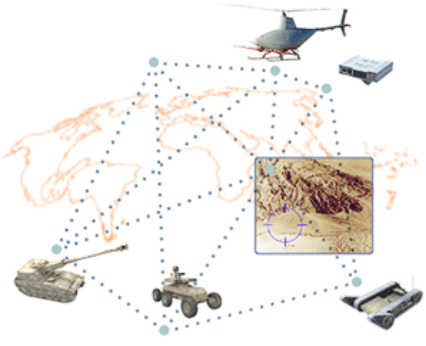
Trots vikten av att utveckla robusta system och SoS finns ännu ingen industristandard för robusthet. Utveckling med robusthet i fokus är till sin natur paradoxal: Om man specificerar beteendet för situationer utanför normalt verksamhetsområde flyttar man samtidigt gränsen för vad som betraktas som robusthet – eftersom robusthet per definition gäller det som ligger bortom specifikationens gräns!



Enligt Fricke & Schultz (2005) är robusthet bara ett av fyra angrepps-sätt för att utveckla och underhålla ett system som ska fungera i en föränderlig miljö. *Robusthet* innebär enligt författarna en okänslighet inför förändrade förutsättningar. En alternativ lösning är att utveckla system som *anpassar* sig vid förändrade villkor. De övriga två angreppssätten gäller istället att utveckla en arkitektur som under-lättar systemevolution, antingen med fokus på *flexibilitet* (enkelt att förändra) eller *agilitet* (snabbt att förändra). De fyra angreppssätten står inte i motsättning till varandra; ett fordon ute på vägarna kan vara robust samtidigt som systemarkitekturen är flexibel.

Även vad gäller verifiering av robusthet i mjukvaruintensiva system saknas riktlinjer för industrin och varje tillverkare tvingas istället hitta sina egna lösningar. I en framtid präglad av SoS växer utmaningen ytterligare, då olika tillverkare ansvarar för separata system. Problemet har på senare tid hamnat högt på dagordningen inom testforskningen. Verifiering av så kallade icke-funktionella krav är en erkänd utmaning och robusthet utgör inget undantag. Hassan et al. (2015) rapporterar att forskning kring robusthetstestning främst studerat felaktig indata, t.ex. extremvärden och brus, medan övriga aspekter av robusthet behöver studeras ytterligare. Vidare drar de slutsatsen, baserat på en genomgång av vetenskapliga studier, att ett ökat fokus på testbarhet generellt för med sig ökad robusthet.

Pape & Dagli (2013) har forskat på arkitekturer för SoS och definierar robusthet som en kvalitetsaspekt omvänt proportionell mot förlorad systemprestanda när enskilda system kopplas bort. Detta perspektiv innebär att de systematiskt kan jämföra alternativa arkitekturer genom att under kontrollerade former koppla bort enskilda system och därefter mäta förlorad systemprestanda – den arkitektur som totalt sett förlorar minst prestanda anses vara mest robust.



Militära tillämpningar har drivit mycket av utvecklingen inom SoS. Modern krigföring domineras av samverkande system, t.ex. *US Brigade Combat System* som ökar enskilda soldaters förmåga genom samverkan mellan markfordon, flygfarkoster, drönare och soldater. Centralt för militära SoS är begreppet *värderobusthet*, dvs. förmågan att leverera nytta även när operationsmiljön förändras. De asymmetriska hot som kriget mot terrorismen uppvisat utpekas som ett samtida exempel på SoS som uppvisat bristande värderobusthet i situationer de inte var designade för. Koo (2010) poängterar vikten av att låta hela utvecklingskedjan genomsyras av strävan efter värderobusthet, till skillnad från att bara betrakta det som ett avslutande verifieringsarbete. Ross & Rhodes (2008) har i sin forskning valt att särskilja *passiv värderobusthet* (systemet okänsligt för förändrade förutsättningar) och *aktiv värderobusthet* (arkitekturen anpassad för att enkelt kunna förändras vid nya förutsättningar), begrepp som liknar Frickes och Schultz perspektiv.

Denna omvärldsbevakning produceras av SICS Swedish ICT som en del av FFI satsningen Möjliggörande Elektronik och Mjukvara i delprogrammet EMK. Se http://www.vinnova.se/sv/ffi/FFI-PROGRAM/FFI---Fordonsutveckling/
För mer information kontakta Eilert Johansson, SICS Swedish ICT. eilert@sics.se

Även i Sverige har Försvarsmakten identifierat vad man kallar system i samverkan som en viktig tekniktrend inom högteknologisk krigföring. Totalförsvarets forskningsinstitut FOI studerar därför hur tillfälligt sammansatta nätverk av sensorer, plattformar och vapen ska kunna konfigureras dynamiskt för maximal effekt.

Framtiden för robusta system av system

Med tilltagande digitalisering och billigare IT ökar möjligheterna att skapa helt nya produkter och att koppla samman dem i system av system. Att det inte råder någon brist på uppslag i fordonsbranschen framgår av sammanställningen ovan. Samtidigt medför även de enklaste tjänster stora utmaningar: Antag att vi vill dela temperatur-mätresultat mellan bilar i samma trafikmiljö. Särskilt intressant är det såklart att få veta vad framförvarande fordon uppmäter för temperatur den närmaste kilometern – speciellt när det pendlar kring 0 °C. En enskild tillverkare kan relativt enkelt implementera detta i sina bilar – men vad händer när en Volvo ska skicka information till en Škoda? Och mätvärden kanske inte måste komma från bilar – SMHI och Trafikverket tillhandahåller också data från egna mätstationer. För att inte tala om företag som HERE. Hur bör man fusionera all data? Hur sållar man bort orimliga mätvärden? Vad gör man när en leverantör får driftavbrott eller stänger sitt API utan förvarning?

När en så pass enkel tjänst väcker så stora frågor ger det också lite perspektiv på frågan om självkörande bilar. En framtid där självkörande bilar från olika tillverkare ska samsas i en komplex trafikmiljö kräver utan tvekan robusta SoS. Utan robusthet når vi aldrig dit!

Idag har alla branscher ett tryck på sig att förändras och leverera nya smarta tjänster med hjälp av IT. Den som inte klarar det dukar under. I fordonsbranschen illustreras omvandlingstrycket inte bara av Volkswagen-skandalen, utan även av bråken mellan utmanarna Apple och Tesla. Konsumenterna förväntar sig att kunna dra nytta av den senaste tekniken i alla sammanhang och den som kan möta den efterfrågan med nya smarta produkter får ett försteg på marknaden.

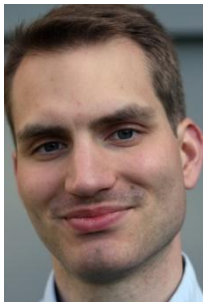
Att omvandla spännande teknik till nya arkitekturer och fungerande affärsmodeller är dock inte alltid så lätt. Det är inte heller uppenbart om det är de befintliga marknadsaktörerna eller utmanarna som har övertaget. I framtidens system av system blir emellertid robusthet en fundamental egenskap som också kan skapa en konkurrensfördel på marknaden.

Kanske står vi inför ett paradigmskifte. I det enskilda fordonet var det på ett helt annat sätt möjligt att kontrollera miljön och att testa systemet under alla relevanta förhållanden. Inte sällan var det till och med möjligt att formellt verifiera säkerheten. Den kunskapen är viktig

och ska absolut inte glömmas bort. Samtidigt är det ett faktum att miljön i ett SoS är mycket mer oförutsägbar. Nya produkter, gränssnitt, tjänster och användningsmönster medför en dynamisk miljö, där det är svårt att samverka utan oväntade effekter, driftavbrott eller risker. Till och med den enkla temperaturmätningen skapar nya utmaningar.

Här blir robusthet – och besläktade begrepp som anpassningsbarhet, agilitet och flexibilitet – nyttiga tankemönster. På SoS-nivån blir frågan hur vi dynamiskt kan hantera oväntat beteende, snarare än hur vi kan bevisa att det aldrig kommer att ske.

Tjänster som uppvisar konstiga beteenden eller bara fungerar intermittent får nämligen svårt att slå igenom på marknaden. Bara den som lyckas möta efterfrågan med rätt funktionalitet levererad på ett robust sätt går en ljus framtid till mötes.



Ulrik Franke och Markus Borg, båda på SICS Swedish ICT, bidrog med sakkunskaper och textproduktion för Robusta System av System temat.

Denna omvärldsbevakning produceras av SICS Swedish ICT som en del av FFI satsningen Möjliggörande Elektronik och Mjukvara i delprogrammet EMK. Se http://www.vinnova.se/sv/ffi/FFI-PROGRAM/FFI---Fordonsutveckling/
För mer information kontakta Eilert Johansson, SICS Swedish ICT. eilert@sics.se