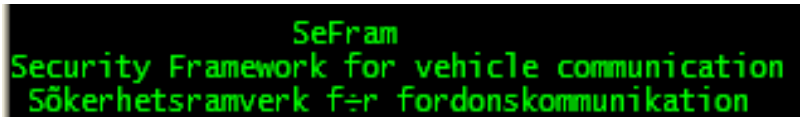
Säkerhetsramverk för fordonskommunikation



Författare: Henrik Broberg
Datum: v1. 2016-01-24
Delprogram Möjliggörande Teknik

FFI Fordonsstrategisk Forskning och Innovation

Innehållsförteckning

Kort om FFI

FFI är ett samarbete mellan staten och fordonsindustrin om att gemensamt finansiera forsknings-, innovations- och utvecklingsaktiviteter med fokus på områdena Klimat & Miljö samt Säkerhet.
Satsningen innebär verksamhet för ca 1 miljard kr per år varav de offentliga medlen utgör drygt 400 Mkr.

För närvarande finns fem delprogram; Energi & miljö, Trafiksäkerhet och automatiserade fordon, Elektronik, mjukvara och kommunikation, Hållbar produktion och Effektiva och uppkopplade transportsystem. Läs mer på www.vinnova.se/ffi

1 Sammanfattning

SeFram projektet startades 2012 för att öka mognadsgraden för information och IT säkerhet i bilar. Tidigare projekt inom FFI som Sigyn I & II och forskning i omvärlden har visat att det finns ett stort behov av bättre kunskap, teknik och arbetssätt.

Projektet har en akademisk del för att skapa spets-teknik och -kunskap och en industriell del som syftar att sprida kunskaper och teknik på en bredare front inom Volvo Cars. Projektets akademiska del har bestått av doktorandtjänst vid institutionen för Data och Informationsteknik vid Chalmers och en industridoktorandtjänst hos Volvo Cars. Båda har fått handledning från institutionen för Data och Informationsteknik vid Chalmers. Projektets industriella del har bestått av 1-3 FTE (FTE = Heltidsekvivalent) som tagit fram teknik och metoder, med tillräcklig mognadsgrad och där bilprojektens behov är störst, och utfört den förutveckling som behövs för tillämpning i bilprojekt.

Projektresultaten har används i regionala samarbeten och internationellt standardiseringsarbete. Under projektets gång har IT-säkerhet i bilar utvecklats från att vara ett obskyrt ämne till att skapa förstasidesnyheter i världspress och är ett högt prioriterat område för myndigheter. Dagens allt mer uppkopplade fordon har tilldragit sig mycket intresse även från allmänheten, och många har börjat ifrågasätta hur säkra dagens fordon verkligen är. Eftersom säkerhetsproblem riskerar att övergå till att vara trafiksäkerhetsproblem, är området oerhört viktigt för oss alla.

Se fram har skapat värdefull kunskap och kontakter med flera viktiga intressenter har kunnat etableras bland annat för att Volvo Cars ska kunna bidra inom både akademisk och tillämpad forskning. Resultaten från projektet används i bilarnas el-plattform som en möjliggörande teknik. Att tidigt ha kunnat beakta säkerhetslösningar för uppkopplade funktioner är strategiskt viktigt för att på ett bättre sätt kunna bemöta det ökade intresset och krav från allmänhet och myndigheter för IT säkerhet i bilar..

2 Executive summary

Today's modern cars can have more than 100 computers (Electronic Control Units, ECUs) and about 100 million lines of code [1]. The vehicle safety is improved, but by increasing the number of ECUs and amount of code, we are at the same time potentially increasing the number of possible attacks. The feasibility of attacks on vehicles in the field has been demonstrated by researches, [2] (2010), [1] (2011) and a recent demonstration raised broad awareness on the criticality of the topic (2015) [3][4].

In this project, founded by VINNOVA FFI, we have conducted research and advanced engineering in order to understand threats, vulnerabilities that can lead to risks and develop countermeasures to manage those risks.

Academic research has been done by 2 PhD students, at Volvo Cars and Chalmers, to advance the state of the art in the fields of automotive secure electronic diagnostics, electronics architecture and electronic communication. As a result 1 PhD thesis has been defended successfully and one licentiate thesis is planned within first half of 2016.

The project results has been used to spread awareness and dialog on risks and how to manage them within the research and development at Volvo Cars and suppliers in particular and to other companies and authorities in general. Several of the projects results are already introduced to market, both as direct functions and as components of several of Volvo Cars electrical platforms (including SPA).

3 Bakgrund

Dagens moderna bilar kan ha mer än 100 datorer (elektroniska kontrollenheter, ECU) och cirka 100 miljoner rader kod [1]. Elektroniken används till förbättrad fordonssäkerhet, miljöprestanda och ökad bekvämlighet,

men genom att öka antalet styrenheter och mängd kod, riskerar man att samtidigt öka antalet brister som kan utnyttjas för att attackera systemet.

Forskningen av Karl Koscher med flera [2] (2010) har visat hög potentiell skada och Checkoway et al [1] (2011) ger belägg för att nätverksattacker är mycket verkliga. Fjärrattacker, har nyligen fått en hel del uppmärksamhet i media, eftersom Charlie Miller och Chris Valasek 2015 demonstrerade en lyckad attack på en bil genom att via internet få kontroll över vitala system i fordonen [3] [4]. Fiat Chrysler tvingades därmed till en kostsam reparationskampanj på 1,4 miljoner bilar.

Otillräcklig medvetenhet om säkerhet innebär en betydande risk för direkta skador och kostsamma reparationer men även att teknik och funktioner måste avvisas eller senareläggas och därmed utebliven nytta för kunder, företag och samhälle.
Under de senaste 5 åren har information och IT säkerhet i fordon utvecklats från ett område med ett fåtal individer globalt, till ett område där många företag försöker växa.

3.1 Referenser

[1] Stephen Checkoway, Damon McCoy, Brian Kantor et al, “Comprehensive Experimental Analyses of Automotive Attack Surfaces”, USENIX Security, 2011
[2] Karl Koscher, Alexei Czeskis, Franziska Roesner et al “Experimental Security Analysis of a Modern Automobile”, University of Washington, 2010
[3] Charlie Miller and Chris Valasek, “Alert (ICS-ALERT-15-203-01)”.[Online]. Available: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-15-203-01, 2015
[4] Andy Greenberg, Wired, “Hackers Remotely Kill a Jeep on the Highway—With Me in It”.[Online]. Available: http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/, 2015

4 Syfte, frågeställningar och metod

Projektet syftar till att öka mognadsgraden på teknik, process och metod området information och IT säkerhet i fordon.

Den centrala frågeställningen handlar om att kunna förstå risker och hantera risker som har med användningen av elektronik för automatisering i kombination med ökat nätverkande mellan elektroniken inom och utanför fordonen. Från ansökan:

Det övergripande projektmålet är att utveckla säkerheten i framtidens uppkopplade bilar. Detta inkluderar bland annat säkring av interna nätverk och säkring av intelligenta trafikstyrningssystem och andra tillämpningar som kräver kommunikation med externa system.
…
utveckla olika metoder för att kunna mäta eller verifiera resultatet av de säkerhetshöjande aktiviteterna.

Projektet har haft en akademisk del för att skapa spets-teknik och spets-kunskap och en industriell del som syftar att sprida kunskaper och teknik på en bredare front inom Volvo Cars. Projektets akademiska del har bestått av en doktorandtjänst på Chalmers och en industridoktorandtjänst hos Volvo Cars. Båda har fått handledning från intuitionen för Data- och informationsteknik vid Chalmers. Projektets industriella del har bestått av 1-3 FTE (varierande över tid) som tagit teknik och metoder, med tillräcklig mognadsgrad och där vagnsprojektens behov är störst, och utfört den för-utveckling som behövs för tillämpning i bil projekt och organisation.

Metoden för att få industriell tillämpning från akademisk forskning följer mönster från Volvo Cars VIPP-program (Volvo Cars Industry PhD Program) där den akademiska forskningen sprids in i organisationen via den industriella handledaren. De koncept och den teknik som identifieras i den akademiska forskningen har vidareutvecklats på Volvo Cars och tillämpning i vagnsprojekt (projekt som leder till introduktion av en ny bilmodell på marknaden). Den akademiska forskningen applicerar den vetenskapliga metoden på aktuella industriella problem som vagnsprojekt och förutvecklingen ställs inför. Mycket av arbetet i projektet är en fortsättning från FFI projektet

Sigyn II (som fokuserade på diagnos) för att generalisera hur man kan säkra upp kommunikationen inuti fordonen och även fordonens kommunikation med omvärlden.

Den akademiska forskningen kan delas upp i två huvudspår. Det första handlar om att säkra upp kommunikationen mellan fordon och omvärlden: ”vehicle to infrastructure” (V2I) och ”vehicle to vehicle” (V2V), kollektivt kallade V2X. Inom denna del har frågorna vi fokuserat på varit hur man lämpligast säkrar upp V2X-kommunikation och dels hur man kan säkerställa att diagnos inklusive uppdatering av programvara kan ske utan oacceptabla risker.

Det andra spåret i forskningen har varit att arbeta med fordonens interna arkitektur med den centrala frågeställningen kring hur man på lämpligast sätt kan säkerställa stabilitet (förutsägbara tillstånd) för system och nätverk i bilen. Vi har här använt oss av ”social networking techniques” för att identifiera kommunikationsmönster i fordonen och sedan automatiskt föreslå olika optimeringar av nätverkslösningar och som på bästa sätt kan isolera eventuella säkerhetsproblem. Mer denna metod kan designers få fram den ur säkerhetssynvinkel bästa arkitekturen och ha denna som referensmodell mot vilken man kan jämföra andra föreslagna lösningar.

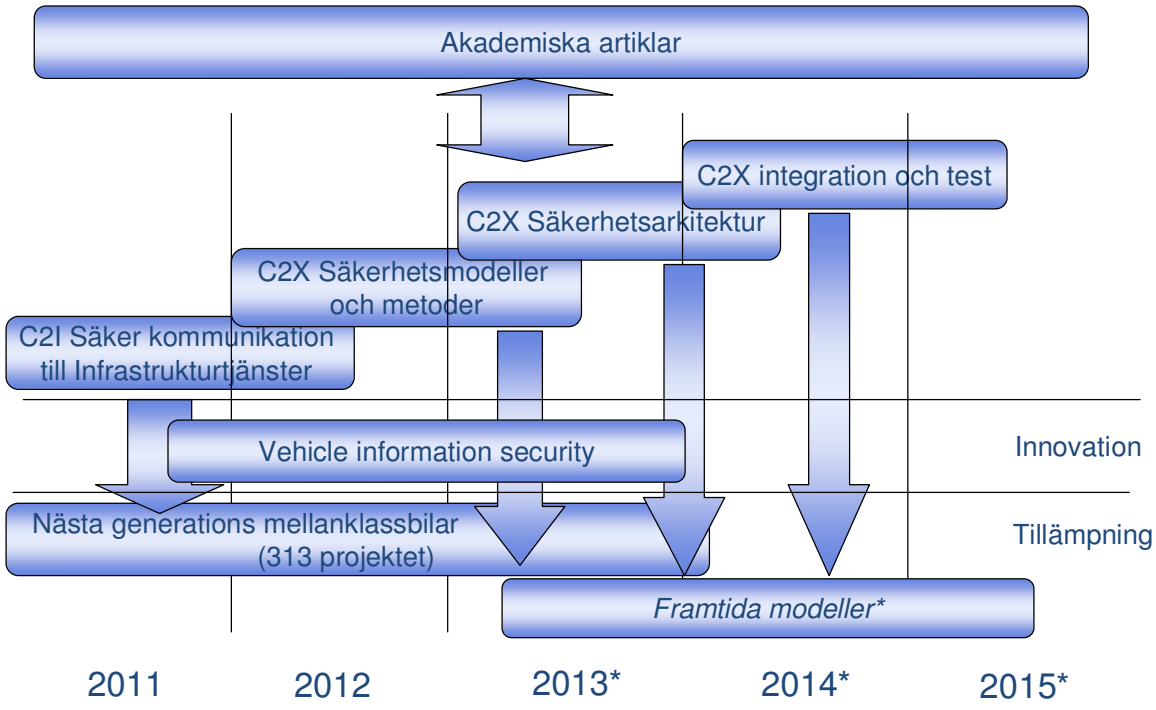
5 Mål

Projektets mål som de angavs i ansökan är inklippt nedan;

Skapa ett integrerat ramverk för IT-säkerhet i fordon som inkluderar:

- säkring av interna nätverk
- extern kommunikation som V2V och V2I
- säkerhetsmodeller för andra applikationer som kommunicerar över Internet.

	Start	*Licentiatexamen*	*Doktorsexamen*
Pierre Kleberger	*2009Q3*	*2012Q3*	*2014Q3*
Asrin Javaheri	*2011Q1*	*2013Q4*	*2015Q4*



Figur 1, Forskningsstrategi och nyttiggörande i projekt

**Gäller planerad budget, dock ej formellt beslutad.*

Arbetspaket säker kommunikation med infrastrukturtjänster

Forskning kring att bilarna ska kunna kommunicera säkert med centrala IT resurser har pågått fram till 2012 och tillämpningsprojekt implementerar detta för tillfället både för bilsystem och för IT system.

Arbetspaket säkerhetsmodeller och metoder

Ett arbetsprojekt för att utveckla processer till nästa utvecklingssteg i bilplattformen har påbörjats på forskningsnivå för att ge input till tillämningsprojekt. Strategin är att öka kvalitén och effektiviteten i säkerhetsarbetet genom att ta vara på lärdomarna från säkerhetsarbetet inom första arbetspaketet (säker kommunikation till infrastrukturtjänster). Resultaten ska vara implementerade i organisationen under 2013 för att kunna vara till nytta som nya processer, metoder och verktyg i arbetet med nästa bilplattform.

Arbetspaket säkerhetsarkitektur

Nästa utvecklingssteg i bilplattformen har fler användningsfall som bygger på uppkopplade tjänster med behov av ytterligare säkerhetsmekanismer och en vidareutveckling av säkerhetsarkitekturen i bilen för att kunna hantera den ökade komplexiteten. Nya koncept måste lämnas av till innovationsprojekt vid början av 2014.

Arbetspaket C2X kommunikation

System för utbyte av information mellan bilar har en annan säkerhetsmodell än uppkoppling till infrastrukturtjänster forskningen främst drivs på regional nivå (EU, USA, Japan). Målprojekt är inte formulerade än, men Volvo Cars är sedan årsskiftet 2011/2012 med i C2C Communication Consortium som driver utvecklingen och standardiseringen av området. Deltagande i forskningsaktiviteter på europeisk nivå ger tillgång till det senaste inom metoder, verktyg och mekanismer på säkerhetsområdet. Utkomsten förväntas vara validering och verifiering (test) metoder för certifiering av bilen som en del i nätverket samt separationen mot övriga interna nätverket. Arbetspaketet behöver levereras under 2014 för att kunna vara till nytta i tillämpningsprojekten.

Kompletterande information begärdes i kvalitetsgranskningen av ansökan:

WP1 - (Research) Säker kommunikation med infrastrukturtjänster

Studie av läget för säkerhet i inbyggda system i bilar och hur man ska utvärdera uppkopplade tjänster i bilar. Ramverk för att beskriva säkerhetsegenskaper och göra utvärdering av inbyggda system.	1. State-of-the art för in-vehicle security. 2. Riktlinjer för säkerhets utvärdering av tjänster i bilen. Artikel. (Dessa två Task avslutades före start av detta FFI-projekt. Ingår ej i budget eller omfattning för detta FFI-projekt.)
Utvärdering av trådlös diagnos i ett verkstadsscenario.	1. Resultat från studie. Forskningsrapport. 2. Licentiatexamen
Applicering av mekanismer för separation i ett bilnätverk.	1. Artikel om säkerhetsnivå för tekniker. 2. Proof of concept
Tester av robusthet för säkerhetsmodeller infrastrukturtjänster.	1. Artikel 2. Doktorsexamen

WP2 -4 (Research) Ramverk för säker kommunikation inklusive C2C kommunikation

Utvärdering av synergieffekter mellan kvalitetsarbete "system safety" och "security".	1. Artikel om metoder och anpassningsbehov av befintlig kvalitetssäkring för att adressera medvetet introducerade fel i systemet. 2. Rapport som input till processutvecklingsprojekt.
Intern säkerhetsarkitektur i bilens inbyggda system.	1. Artikel om urval av säkerhetsmekanismer och dess nivå. 2. Kravmodell, hotmodell som rapport till projekten.
Fallstudie, designmetodik och certifiering för säkerhetsmoduler i inbyggda system.	1. Artikel om applicering av säkerhetsmekanismer och dess nivå. 2. Modeller av krav och hot för ökad formalism i kravuppfyllelse.
Testmetodik på olika systemnivåer inom security. Etablera en minsta nivå av tester på systemnivå och enhetsnivå för olika säkerhetskoncept.	1. Artikel om applicering av säkerhetsmekanismer och dess nivå. 2. Testmetod.
Experimentell utvärdering av attackytor. Utvärdering om nivån har förbättrats i nästa generations uppkopplade bilar jämfört med de problem som lyfts under 2010.	1. Artikel 2. Proof of concept. 3. Doktorsexamen

WP5 - (VCC Advanced Engineering) - Vehicle information security

Framtagning av baskoncept för autentisk programvara	1.Preliminära koncept 2.Benchmark och konceptvalidering (test) 3. Basteknologispecikation.
Framtagning av baskoncept för säkrad kommunikation inom bilen.	1.Preliminära koncept 2.Benchmark och konceptvalidering (test) 3. Basteknologispecikation.
Framtagning av baskoncept för auktoriseringspunkt	1.Preliminära koncept 2.Benchmark och konceptvalidering (test) 3. Basteknologispecikation.
Framtagning av baskoncept för loggning	1.Preliminära koncept 2.Benchmark och konceptvalidering (test) 3. Basteknologispecikation.
Framtagning av baskoncept för virtualisering	1.Preliminära koncept 2.Benchmark och konceptvalidering (test) 3. Basteknologispecikation.
Tillämpning av processer och metodutveckling	1. Processmodell för effektivt och kvalitativt säkerhetsarbete. 2. Analysmall för säkerhetsutvärderingar. 3. Definitioner och utbildningsmaterial.

WP 6 (VCC Industrialiseringsprojekt) Scalable Platform Architecture

Förfining av kravmängd och anpassning till specifik el-arkitektur. Implementation av signerad programvara. Protokoll för kommunikation till VCC infrastruktur. Verifikat för säkerhetsfunktioner med hög konfidens.	1. Krav specifikationer 2. Test specifikationer 3. Verifikat

Funktionsutveckling. Metoder för effektiv och högkvalitativt säkerhetsarbete behöver vara framme innan projektet startar.	1. Arbetsprocess 2. Mallar och instruktioner
Arkitekturutveckling. Integration av säkerhetsmodeller för alla typer av funktioner för den miljön de ska operera i.	1. Arkitekturspecifikation 2. Integrationsplan
Verifiering av funktionalitet med tillräcklig konfidens.	1. Test specifikationer 2. Verifikat

Omprioriteringar mellan tekniker har gjorts, men målsättningarna har i stort legat fast utom för en avvikelse i målsättningen för industridoktoranden. Asrin valde att avsluta doktorandstudier och anställning efter ett år. Målsättningen har fått justeras till att industridoktoranden skulle kunna försvara en licentiat inom projektets ramar. Projekt Vehicle Information Security (VIS) (WP5) har förlängts sedan ansökan gjordes, med både uppdateringar av koncept och nya koncept. Rekrytering av ny industridoktorand fördröjde planen 6 månader och men efter dialog med VINNOVA beslutades att den ursprungliga utbetalningsplanen inte skulle ändras. Volvo Cars tog på sig att finansiera industridoktoranden till halvårsskiftet 2016 (dvs. 6 månader efter ursprunglig plan).

6 *Resultat* och måluppfyllelse

6.1 Resultat och uppfyllelse av projektmål

Den akademiska planen för Pierre Kleberger (wp1) har justerats tidsmässigt och bl.a. av personliga skäl så blev disputationen fördröjd till september 2015 (1 år jämfört med plan). Omfattningen har justerats för att inte inkludera så mycket av testning utan större fokus har lagts på validering i koncept- och systemfas. En kort beskrivning av hur leveranserna och de idéer som utforskats bidraget till målen följer här.

Metoder som används inom telekommunikationsbranschen har varit utgångspunkt i Pierres forskning där han föreslog en förenklad variant för att motivera lämpliga skyddsåtgärder för uppkopplade fordon. I den industriella tillämpningen av diagnos över IP (ethernet/wi-fi) nätverk och fjärrdiagnos har metoden använts för utveckling och vagnsprojekt för att kunna systemera beslutsprocessen för skyddsnivå och konceptval. Metoden har sedan förenklats för tillämpning på mindre projekt och funktioner för att motivera val av skyddsnivå. Metoden har ytterligare utvecklats inom ramen för FFI projektet HeavenS.

Formell verifiering har utforskats på akademisk nivå för att verifiera protokoll-design. Denna metod är intressant som referens, men är för avancerad för någon bredare industriell tillämpning för tillfället. För vissa komponenter (som protokolldesign, kryptomoduler etc.) kan det redan idag vara aktuellt med formell verifiering, men då utförs denna av specialister längre ner i försörjningskedjan. Som fordonstillverkare så handlar det mer om att veta vilka delar som det är önskvärt och möjligt att applicera metoden på.

Den referensmodell för säker arkitektur som Pierre tagit fram används som en referens i designarbetet. Direkt anpassning av modellbaserad utveckling på Volvo Cars är en betydligt större uppgift än vad som ryms inom detta projekt, men metodiken används idag som en referensmodell av experter då team behöver stöttning i utvärderingen.

Som ett direkt resultat av projektet har vi också varit med och påverkat kommande ETSI-standard inom V2X-området och också fått värdefull erfarenhet av hur kommande standard kan och ska användas i egna fordon. Forskningen har också lett till att ett protokoll för auktorisering av serviceutrustning i verkstäder tas fram med målet att skydda fordonen från felaktiga mjukvaruuppdateringar eller oauktoriserad modifiering av fordonens programvara.

Resultatet av denna del av projektet har lett till ett automatiserat verktyg som givet en önskad funktionalitet hos systemet, föreslår hur alla ECU er ska förbindas och hur man på lämpligaste sätt kan dela upp nätverket i ett antal mindre nätverk. Vi har här använt oss av ”social networking techniques” för att identifiera kommunikationsmönster i fordonen och sedan automatiskt föreslå olika lösningar. Den föreslagna lösningen kan sedan användas som en referensarkitektur som designers sedan kan utgå från eller jämföra existerande lösningsförslag med. Detta är ett arbete som lämnats över till arkitekturprojekt som ligger till grund för nästa uppgradering av SPA plattformen genom artiklar och presentation.

Även om tidplaner för artiklar och ingenjörsarbete inte kunnat vara synkroniserade så har resultaten kunnat användas som en referens för att en rimlig nivå av skydd uppnåtts.

Den akademiska planen för industridoktoranden (wp2-4) fick arbetas om från grunden då Asrin valde att avsluta studier och anställning efter ungefär ett år. Nasser Nowdehi rekryterades ett halvår senare efter avslutat examensarbete på Volvo Cars. Idag följer han en plan där licentiatexamen kommer att avläggas under våren 2016. Granskning från både Chalmers och Volvo Industrial PhD Program genomfördes under 2015 med positivt utfall.

Nassers första artikel handlade om svagheter i den kryptografiska designen i ETSI’s föreslagna standard för säker V2X-kommunikation och hur dessa kunde leda till robusthetsproblem för systemet i sig. Artikeln illustrerar en aspekt av säkerhetsproblem som oftast inte är lika uppenbar som att kringgå kryptografi för att få tag i hemligheter eller kringgå access kontroll. I detta fall var det till och med kryptografilösningen som tillförde attackvektorn.

Samarbete med Pierre kring optimering av bilens nätverksarkitektur är redan nämnt ovan.

Projektet ”Vehicle Information Security” (VIS) (WP5) har utvecklat teknik till en mognadsgrad lämplig för tillämpning i bilarnas E/E, för att motverka hoten plattform i ett flertal projekt (313 projekt i figur 1, men även SPA plattformen, med XC90 som första modell).
Alla tekniker som planerades har inte fullföljts till basteknik utan de har avslutats eller förts vidare till funktionsägare (och därmed fallit utom ramen för projektet VIS). I och med avlämningen till Sensus Cloud (313 projektet i figur 1) så övertogs en del funktioner som basteknik.

Flera samarbeten kring säkerhet har gjorts inom Volvo Cars med projekt på flera nivåer (arkitektur och i vissa fall funktioner och subsystem) som resulterat i krav och lösningar i flera olika specifikationer som är svåra att återge liksom att gå in på detaljer i den interna strukturen av Volvo Cars dokumentation.

De processer och metoder som använts i det övergripande ramverket för säkerhetsarbetet har främst sett till Volvo Cars befintliga information och erfarenheter från det IT säkerhetsarbete som bedrivits inom Volvo Cars. I ramverket har man fokuserat på några få ”hard points” i processerna för att erhålla harmonisering mellan IT och R&D. Ett standardiseringsinitiativ för att ta fram en fordonsanpassad utvecklingsprocess (SAE J3061) har bevakats för att kunna välja lämpliga delar, och vi har härifrån även lämnat viktiga bidrag till FFI-projektet HeavenS. Eget arbete för att praktiskt harmonisera säkerhetsabetet med ”system safety”-processer (ISO 26262) har gett praktiska resultat. Resultaten är ej formaliserade i VCC kvalitetsstyrning men ingår som en del av ”best practices” (tex information, kontaktpersoner och mallar på intranät).

6.2 Uppfyllelse av FFI Programmets mål

Programmet Elektronik, Mjukvara och Kommunikation (EMK) har idag följande övergripande mål (FFI, 2014):

Generellt

- *Samverkansprogram och projekt ska inom de övergripande temaområdena Klimat & Miljö samt Säkerhet tydligt bidra till att:*
  - *genom ökad forsknings- och innovationskapacitet i Sverige säkra fordonsindustriell konkurrenskraft och arbetstillfällen på lång och helst även på kort sikt.*
  - *utveckla internationellt uppkopplade och konkurrenskraftiga forsknings- och innovationsmiljöer, i vilka bland andra akademi, institut och industri samverkar.*

- *främja internationell forsknings- och innovationsverksamhet där förutsättningar för och medverkan i EU:s ramprogram och annan internationell forsknings- och innovationssamverkan noga värderas.*

EMK-specifikt

- *Höja den tekniska mognadsgraden (genom att mäta "technology readiness level", TRL) samt effektivisera metoder inom produktutveckling för att snabbare kunna industrialisera resultaten och öka kundvärdet.*

Kommentarer Se Fram:

- Kompetenshöjning på området informationssäkerhet och IT säkerhet har ökat konkurrenskraft för individer Chalmers och företag i regionen (ej endast projektdeltagarna)
- Idag är Västsverige en del av en global forsknings- och innovationsmiljö för säkerhet i bilens elsystem.
- Volvo Cars är inte del i EU:s ramprogram på detta område
- Mognadsgraden har höjts för många tekniker och metoder och dessa har fungerat som möjliggörande teknik i flera projekt.

7 Spridning och publicering

7.1 Kunskaps- och resultatspridning

Hur har/planeras projektresultatet att användas och spridas?	Markera med X	Kommentar
Öka kunskapen inom området	X	Akademisk spets och bredd (tex survey artiklar) Industriell tillämpning via specifikationer nya metoder och kunskapsöverföring till VCC ställda i allmänhet och beslutsfattare (linje chefer, projektledare, arkitekter, funktionsägare, designers, testutvecklare) inom VCC i synnerhet.
Föras vidare till andra avancerade tekniska utvecklingsprojekt	X	Forskningsnivå HeavenS, HoliSec Teknikutveckling: VIS. Sensus Cloud
Föras vidare till produktutvecklingsprojekt	X	För utveckling inom projekt VIS har bedrivits inom projektet, som lämnats av till vagnsprojekt.
Introduceras på marknaden	X	Flera av teknikerna är i produktion i ett flertal projekt (särskilt i SPA plattformen)
Användas i utredningar/regelverk/ tillståndsärenden/ politiska beslut	X	Projektresultat har använts i dialog med myndigheter, inklusive US DoT NHTSA och EU kommissionen.

I FFI projekt HeavenS har AB Volvo och övriga partners fått tillgång till resultat och kontakter för att skapa synergi. I praktiken har arbetet bedrivets tillsammans även om redovisning har hållits separat.

7.2 Publikationer

Titel/författare
#1 Security aspects of the in-vehicle network in the connected car P Kleberger, T Olovsson, E Jonsson IEEE Intelligent Vehicles Symposium, Proceedings. Baden-Baden, 5-9 June 2011
#2 An In-Depth Analysis of the Security of the Connected Repair Shop P Kleberger, T Olovsson, E Jonsson The Seventh International Conference on Systems and Networks Communications (ICSNC), Proceedings. Lisbon, 18-23 November, 2012
#3 A Framework for Assessing the Security of the Connected Car Infrastructure P Kleberger, A Javaheri, T Olovsson, E Jonsson The Sixth International Conference on Systems and Networks Communications (ICSNC), Proceedings. Barcelona, 23-29 October 2011
#4 Protecting Vehicles Against Unauthorised Diagnostics Sessions Using Trusted Third Parties P Kleberger, T Olovsson Proceedings of the 32nd International Conference on Computer Safery, Reliability and Security (SAFECOMP). Toulouse, Sept. 2013
#5 A Structured Approach to Securing the Connected Car P Kleberger Licentiate Thesis, Chalmers University of Technology
#6 Security Concerns in Communication with the Connected Car using DoIP P Kleberger, A Javaheri, V Izosimov, H Broberg 15. Internationaler Kongress Elektronik im Kraftfahrzeug; Baden-Baden, Germany. Oct 2011.
#7 Mapping Systems Security Research at Chalmers M Almgren, Z Fu, E Jonsson, P Kleberger, A Larsson, F Moradi, T Olovsson, … Deliverable D2. 3: 1st Project Workshop Proceedings, 66

#8 Formal Verification of an Authorization Protocol for Remote Vehicle Diagnostics
P Kleberger, G Moulin
IEEE Vehicular Networking Conference (VNC), Proceedings. Boston, 16-18 Dec 2013

1

#9 Securing Vehicle Diagnostics in Repair Shops
P Kleberger, T Olovsson
Computer Safety, Reliability, and Security (SAFECOMP), Florence, Sept 2014.

#10 Experiences from implementing the ETSI ITS SecuredMessage service
N. Nowdehi, T. Olovsson
2014 IEEE Intelligent Vehicles Symposium. June 8 - 11, 2014, Dearborn, Michigan, USA

#11 Towards Designing Secure In-Vehicle Network Architectures Using Community Detection Algorithms
P. Kleberger, N. Nowdehi, T. Olovsson
IEEE Vehicular Networking Conference (VNC), Proceedings. Paderborn, Germany. 3-5 Dec. 2014 (2157-9865). p. 73-80. (2014)

#12 Improving In-Vehicle Network Architectures Using Automated Partitioning Algorithms
Nowdehi, Nasser; Kleberger, Pierre; Olovsson, Tomas
IEEE Vehicular Networking Conference (VNC), Proceedings. December 16-18, 2015, Kyoto, Japan (2015)

#13 Akademisk avhandling för avläggande av doktorsexamen: On Securing the Connected Car - Methods and Protocols for Secure Vehicle Diagnostics
Pierre Kleberger. Institutionen för data- och informationsteknik, Nätverk och system, Chalmers University of Technology, 2015. ISBN: 978-91-7597-241-1.- 197 s.

Konferenser där vi presenterat bidrag:

- IEEE Intelligent Vehicles Symposium, Baden-Baden, June 2011
- The Sixth International Conference on Systems and Networks Communications (ICSNC), Barcelona, Oct 2011
- Internationaler Kongress Elektronik im Kraftfahrzeug; Baden-Baden, Germany. Oct 2011
- The Seventh International Conference on Systems and Networks Communications (ICSNC), Lisbon, Nov 2012
- 32nd International Conference on Computer Safety, Reliability and Security (SAFECOMP), Toulouse, Sept. 2013
- IEEE Vehicular Networking Conference (VNC 2013), Boston, Dec. 2013
- IEEE Intelligent Vehicles Symposium, Dearborn, Michigan, USA, June 2014
- Computer Safety, Reliability, and Security (SAFECOMP), Florence, Sept 2014
- IEEE Vehicular Networking Conference (VNC), Proceedings. Paderborn, Germany. Dec. 2014
- ESCAR Japan September 2015
- IEEE Vehicular Networking Conference (VNC), Kyoto, Japan. Dec. 2015
- Elektronik i fordon, Göteborg, 2 gånger
- We connect / Aact! 2015: ”Security and the connected car” , Berlin 2015

Övrig spridning av resultat
Volvo Cars techonology exhibition är ett årligt event där VIS presenterade resultat 2014 & 2015 för att öka medvetenhet om problematik och lösningar.

Inom HeavenS projektet har Se Fram resultat används som utgångspunkt och därmed har projektresultaten spridits inom regionen, och internationellt inom SAE international (referens i J3061). Flera gemensamma aktiviteter, speciellt angående testning pågår.

C2C Communication Consortium är ett bra forum för att ta in och sprida resultat främst bland europeiska biltillverkare och leverantörer.

Harmonisation Task Group, delar resultat mellan kontinenterna där USA och EU är mest aktiva hittills, men Japan har börjat engagera sig och är intresserade av resultaten från harmoniseringsarbetet.

SAE international, har två undergrupper, säkerhetsmoduler (HSM) och arbetsprocesser. Verksamheten består främst av telefonmöten.

VOLPE/NHITSA/DOT Volpe center utför forskning på uppdrag av NHTSA för tillfället inom ”automotive cyber security”. Dialog och utbyte av resultat pågår.
Möten:

- 2012 november, Washington DC
- 2014 feburari, Washnington DC
- Ca 3 web and telefon tillsammans med FFI HeavenS
- Webmöte för att visa Plikta resultat (med säkerhetskoppling) planerat till 2015

Under VIPP seminarium på Volvo Cars under oktober 2014 har Nasser presenterat sitt arbete.

8 Slutsatser och fortsatt forskning

Nästa steg i utvecklingen är att öka mognadsgraden på befintliga metoder och teknik och komplettera med nya så att en reproducerbar och jämn kvalité kan upprätthållas på att identifiera rätt åtgärder och att kunna implementera och kvalitetssäkra dem på ett effektivt sätt.

Vår målsättning är att fortsätta arbetet med att integrera säkerhetskultur och tekniker i utvecklingen av bilar. Inriktningen är att inte bara kunna hitta en tillräcklig nivå av skydd för att hantera riskerna, utan att effektivisera genom att identifiera risker i allt tidigare utvecklingsskeden där det finns större utrymme för omdesign eller kompenserande åtgärder. Detta innebär att fortsätta metodutveckling för att analysera hot, svagheter och risker att uppnå större skalbarhet, effektivitet och reproducerbarhet. Förbättra harmonisering av metod till övrig kvalitetssäkring (så som robusthetsanalyser och testning) för både vanlig kvalitetssäkring och förstärkt kvalitetssäkring då personsäkerhet är i fråga (ISO 26262).

Tekniskt finns behov av vidare utveckling av tekniker för att kunna hantera risker på ett enklare sätt. Enkelhet och integration i plattform på ett skalbart sätt är områden som behöver förbättras för att kunna möjliggöra att nya idéer kan realiseras utan att information och IT säkerhet blir ett hinder och kunna undvika misstag. Olika tekniker för att öka kvalité och minska ledtider för information om svagheter och uppkommande hot behövs både inom och utanför bilen.

Områden som ligger närmast för fortsatt forskning

- risker och motåtgärder både liknar och skiljer sig från andra risker inom fordonstillverkning
- hur tekniker som kryptografi, brandväggar etc. tillämpas bättre i fordonselektronik
- metoder för att hitta rätt nivå av skydd,
- kvalitetssäkring av säkerhets funktioner och teknik
- kvalitetssäkring av funktioner och teknik för att undvika brister som kan utnyttjas
- integration i ordinarie kvalitetssäkring (produktivitet)
- integration med drift i fält för avvikelsehantering (incidentberedskap)

9 Deltagande parter och kontaktpersoner

CHALMERS

031-77210000
Erland Jonsson (erland.jonsson@chalmers.se)
Tomas Olovsson (tomas.olovsson@chalmers.se)
Pierre Kleberger

VOLVO

031-59 0000

Borg, Jörgen (94140) (jorgen.borg@volvocars.com)
Calais, Kristian (94142) (kristian.calais@volvocars.com)
Nowdehi, Nasser (nasser.nowdehi@volvocars.com)
Broberg, Henrik (henrik.broberg@volvocars.com)