FFI
FORDONSSTRATEGISK
FORSKNING OCH INNOVATION

BeSafe –
BEnchmarking of Functional SAFEty

Projekt inom FFI Fordonsutveckling

Mats Olsson, Volvo Technology AB

2014-05-20

FFI
FORDONSSTRATEGISK
FORSKNING OCH INNOVATION

Innehåll

FFI
FORDONSSTRATEGISK
FORSKNING OCH INNOVATION

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 hälften.

För närvarande finns fem delprogram Energi & miljö, Fordons- och trafiksäkerhet, Fordonsutveckling, Hållbar produktionsteknik och Transporteffektivitet. Läs mer på www.vinnova.se/ffi

FFI
FORDONSSTRATEGISK
FORSKNING OCH INNOVATION

1. Sammanfattning

På grund av det ständigt ökande behovet av elektriska och elektroniska (E/E) system i fordon blir begreppet funktionssäkerhet allt viktigare. Införandet av ISO 26262, som är en ny standard för funktionell säkerhet i vägfordon, har påskyndat utvecklingen med att införa ett systematisk angreppssätt för att utvärdera funktionssäkerhet. Dock är inte standardiserade utvärderingssmetoder för benchmarking av funktionssäkerhet i fordonssystem tillgängliga i dag. Det är här som projektet BeSafe (Benchmarking of Functional Safety) kommer in i bilden och målet är att lägga grunden för benchmarking av funktions-säkerhet i komplexa E/E system i fordon.

I det här dokumentet presenteras en kort översikt av projektet tillsammans med de benchmark-mål som har identifierat som relevanta för fordonsindustrin med införande av tre abstraktionlager, nämligen modeller, mjukvara och hårdvara. Därefter definieras och föreslås en uppsättning benchmark-mätpunkter med tillhörande ramverk som omfattar fel (fault/error)-modeller, metoder och nödvändiga verktyg för att kunna utföra benchmarking av funktionssäkerhet. Slutligen presenteras några preliminära resultat där också potentiella framtida arbeten belyses.

BeSafe's konsortium består av Chalmers, QRtech, Scania, SP, Volvo Cars och Volvo Technology. Volvo Technology är projektsamordnare och huvudsökande. Planerad projekttid var tre år, med start i januari 2011 och avslut i mars 2014. Projektbudgeten var 17 550 500 kronor, varav 8 775 200 kronor offentligt finansierat.

2. Bakgrund

Säkerhet har alltid varit en viktig egenskap inom fordonsindustrin. Säkerheten som idag erbjuds kan grovt delas in i passiv säkerhet, som syftar till att mildra effekterna av en kollision, och aktiv säkerhet, som syftar till att förhindra en kollision helt och hållet. En aspekt av säkerhet, som blir allt viktigare inom fordonsindustrin, är funktionssäkerhet. Det beror på det faktum att elektronik har införts i praktiskt taget alla fordonsfunktioner och i ca 90 % av alla fordonsinnovationer finns mjuk- och hårdvara [1] som bas . Till skillnad från passiv och aktiv säkerhet, som tillhandahålls av särskilda system och funktioner, är funktionssäkerhet en inneboende egenskap i system och som anger deras förmåga att förbli säkra under olika förhållanden, med eller utan uppkomna fel. ISO 26262 [2], en ny standard för funktionell säkerhet i vägfordon, definierar funktions-säkerhet som: *frånvaro av orimliga risker på grund av fara som orsakas av felfungerande E/E system*.

Grunderna för funktionssäkerhet är undvikande av fel (t.ex. systematiska mjukvarufel) eller upptäckten och hanteringen av fel (t.ex. slumpmässiga hårdvarufel) för att mildra effekterna av dessa och på så sätt förhindra att ett inbyggt system [3] missar sitt säkerhetsmål. I dagsläget finns, i ISO 26262 [2], krav på ett fordons livscykel avseende

säkerhet för elektriska och elektroniska (E/E) system. Dessutom är AUTOSAR (AUTomotive Open System ARchitecture) en central teknik för att hantera den växande E/E komplexiteten och tillhandahålla mekanismer och en systematisk designstrategi för att underlätta uppnåelsen av funktionssäkerhet hos mjukvarubaserade system [3]. Däremot finns idag inga standardiserade utvärderingsmetoder för funktionssäkerhet att tillgå.

3. Syfte

BeSafe Projektet syftar till att lägga grunden för benchmarking av funktionssäkerhet hos fordons E/E system. En standardiserat metod för utvärdering av funktionssäkerhet kommer att förbättra industrins förmåga att erbjuda säkrare fordon. Benchmarking är också ett sätt att utvärdera till vilken grad de förväntade kraven på ett sådant system har uppfyllts. Följaktligen blir benchmarking av funktionssäkerhet en värdefull hjälp vid utvärdering av hur säkerhetsmål och säkerhetskrav uppfylls. Det blir också en språngbräda för uppfyllande av de krav som härrör från standarder som ISO 26262 [2] och IEC 61508 [4].

I projektet definieras ett antal benchmarkmål (BT –Benchmark Targets). Ett BT kan i princip vara vilket system eller undersystem som helst som har tydliga avgränsningar. Ett BT motsvarar ordet ”element” som används i ISO 26262 [2]. För varje BT definieras ett antal mått som är relevanta för att anvisa ett användbart benchmark tillsammans med metoder för utvärdering av dessa mått och för att sedan kunna utvärdera måtten på de valda BT:s.

Vid sidan av utarbetandet av mått för valda BT:s defineras ett allmängiltigt ramverk inom vilket benchmarks skall verka. Ramverket omfattar metodik och process samt verktygsstöd –dels i form av vertyg för genomförandet av faktiska benchmarks och dels i form av stöd för benchmarksmått i utvecklingsverktyg. Innehållet i benchmark-resultatet utgörs av ett flertal mått som definierats i projektet. Både kvantitativa och kvalitativa mått ingår och framtagningen av måtten tar hänsyn till analytiska mätningar, den process genom vilken elementet är utvecklat och empiriska mätningar som baseras på realiseringarna av elementet (t.ex. felinjicering eller robusthettest).

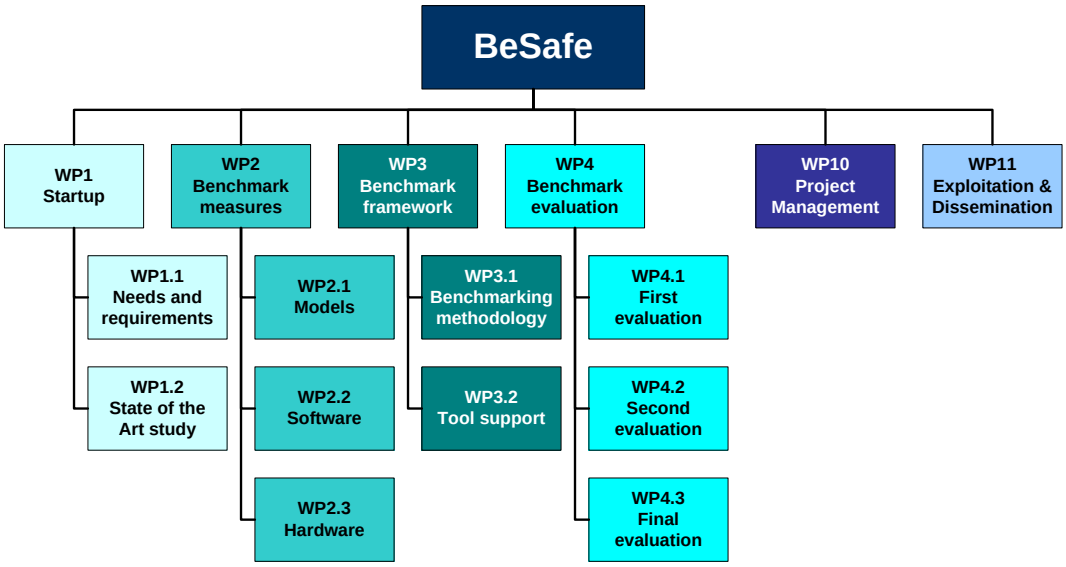
Varje ingående mått har en tydlig relation till de funktionella säkerhetsegenskaperna hos aktuellt BT. Dock är ett enskilt mått normalt inte tillräckligt för att BT resultaten skall vara användbara. Istället tas hänsyn till en hel rad av mått för en specifik användning av ett BT-resultat. Fokus ligger på fyra generella användningsområden som är av särskilt intresse för benchmarking av funktionssäkerhet: (a) J*ämförelse*. Jämför lämpligheten av ett element med avseende på funktionssäkerhet under systemutveckling/integration; (b) *Profilering*. Karakteriserar ett element för att identifiera och lyfta fram starka och svaga sidor med avseende på säkerhet; (c) *Krav*. Säkerhets-relaterade krav på systemet, eller dess beståndsdelar, kan kommuniceras med hjälp av benchmark information för en gemensam förståelse; och (d) *Egenskaper*. På ett kompositionellt sätt kan säkerhets-

benchmarks hjälpa till i utväderingen av systemets säkerhetsegenskaper givet säkerhetsprofilerna för sina element.

En generell "V" processmodell presenteras som vår referensprocess för att möjliggöra rättfram mappning mellan BeSafe och ISO 26262. Dessutom definieras en användningsfallsmängd för att identifiera domänen där användningsfallen för BeSafe projektet finns. Denna användningsfallsmängd är en allmän beskrivning av roller/aktörer (t.ex. funktions-säkerhetsutvärderare, systemutvecklare, programvaruleverantörer, E/E arkitekter), aktiviteter (t ex, specifikation, utvärdering, verifiering, bedömning), processteg (t.ex. konceptfas, produktutveckling, produktion och drift), artefakter (t.ex. E /E arkitektur, funktion, ECU design, Programvaruelement) o.s.v.

4. Genomförande

Projektet är indelat i tre iterationer i tid och ett antal arbetspaket, strukturerade som enligt figur 1 nedan.



Figur 1. Projektets arbetspaket.

Tabell 1 nedan ger en mer detaljerad bild över arbetspaketen och deras innehåll. Parterna inom parentes är resp arbetspakets ledare.

WP1 Uppstart – Ledare: VTEC	
I WP1 definieras kraven för de efterföljande arbetspaketen, bl a övergripande mål, state-of-the-art analys, utredning av behov och krav, användningsfall för benchmarking och BT.	
WP1.1	Behov och krav (VTEC). WP1 undersöker vad benchmarking av

	funktionssäkerhet är och hur det skulle kunna användas av olika intressenter i produktframtagningsprocessen. Behoven hos de identifierade intressenterna mappas till användningen av säkerhets-benchmarks. Vidare definieras detaljerna i projektplanen, målet och visionen med projektet, för att se till att alla parter arbetar i samma riktning, samt en detaljerad form för samarbetet mellan projektparterna. En uppsättning BT:s kommer att väljas ut för projektet.
WP1.2	State-of-the-Art studie (Chalmers). Många utmaningar som uppkommer från allt mer digitaliserade system är generella, och andra discipliner, t.ex. konsumentelektronik och telekom, har en relativt lång tradition av sådana frågor. Syftet med detta arbetspaket är att identifiera olika metoder och mekanismer för att bedöma och jämföra alla dimensioner av funktionssäkerhet och att skapa state-of-the art inom detta område.
WP2 Benchmark mätningar – Ledare: Scania	
Utifrån kraven från WP1 definieras måtten på ett antal utvalda BT:s. Här ges också en definition av bedömningsmetoder för att tillhandahålla värden för de utvalda måtten (t.ex. felinjicerings-tekniker samt principer för analys), definition av fel- och arbetsbelastning. Följande underarbetspaket finns.	
WP2.1	Modeller (SP). Detta område handlar om benchmarking på modeller av applikationen. På genomförandenivå är dessa modeler skapade i Simulink och på mer abstrakta nivåer definierar de hur Simulink modellen skall se ut. Arkitekturlösningar i modellerna (säkerhetsmönster och distribution) och kontroll-programvara som genereras från modellerna, och som utvärderas i WP2.1, kommer att användas som BTs i WP2.2 för att möjliggöra jämförelser mellan benchmarks från mjukvara och modeller.
WP2.2	Mjukvara (VTEC). Det här arbetspaketet jobbar med benchmarking av enskilda komponenter och delsystem som är integrerade i fordonens programvara. Några exempel på sådana komponenter kan vara antingen enskilda moduler eller hela AUTOSAR BSW/RTE. Angreppssätt för bedömningen av SW-Cs är också av intresse, i synnerhet för att kunna korrelera resultaten från benchmarks som utförs på modeller med resultat från benchmarks som utförs på automatgenererad programkod från dessa modeller.
WP2.3	Hårdvara (QRTECH). Fokus i dett arbetspaket ligger på hårdvaruelement, såsom ECU:er och kraftelektronik. Följande områden skall undersökas: Styrelektronik –utvärdering av HW mätetal definierade i ISO 26262 och liknande standarder; Kraftelektronik –utvärdering av vilka mått och mål som är applicerbara på kraftelektronik i HEV och EV. Felmodeller relaterade till förpackning och monterings måste undersökas för att jämföra säkerheten i denna typ av system. Släktskapet med EV standarder såsom ECE-R100 skall belysas; och sensorelektronik –utvärdering av säkerhetsegenskaper hos sensorer och sensormodeller.
WP3 Benchmark ramverk – Ledare: Chalmers	

WP3 definierar den övergripande metodiken för hur man använder benchmark resultat samt definierar hur benchmark bör användas inom ramen för ISO 26262 och andra relevanta standarder och processer. Inkluderat är också en redogörelse för nödvändiga verktyg som krävs för införandet av ramverket.	
WP3.1	Benchmark metodik (Chalmers). Denna del definierar metodiken för att utföra benchmarking aktiviteter, hur resultaten används o.s.v.
WP3.2	Vertygsstöd (SP). Definierar de verktyg som behövs för införandet av ramverket och dess interaktioner. Användningen av en gemensamt databas för lagring och åtkomst av benchmark resultat diskuteras.
WP4 Benchmark utvärdering – Ledare: QRTECH	
Efter varje iteration utvärderas resultaten från WP2 och WP3 på fallstudier och exempel. T ex, här säkerställs det att resultaten inte står i konflikt med interna metoder och tekniker som används av projektdeltagarna. Dessutom ser vi till att mätningarna är användbara för de aktiviteter som har definierats. Insatserna innebär verifiering och validering av kraven från WP1.	
WP4.1	Första utvärderingen. Resultaten från iteration 1 utvärderas och ger input till Iteration 2 ang nödvändiga ändringar eller möjliga förbättringar.
WP4.2	Andra utvärderingen. Resultaten från iteration 2 utvärderas och ger input till iteration 3 ang nödvändiga ändringar eller möjliga förbättringar.
WP4.3	Tredje utvärderingen. Här genomförs den slutliga utvärderingen av resultaten i projektet. Fokus ligger på nya tillägg och ändringar införda i den andra iterationen.
WP10 Projektledning – Ledare: VTEC	
Övergripande projektledning utförs från detta arbetspaket. Även de projektavslutande aktiviteterna sker inom detta arbetspaket.	
WP11 Exploatering & kunskapsspridning – Ledare: VTEC	
Detta delprojekt handlar om att sprida resultat och utnyttja relevanta och tillämpbara resultat på de olika projektpartnerorganisationerna inkl den akademiska världen. Speciellt planeras workshops, seminarier och undervisningsenheter.	

5. Resultat

Projektets resultat är ett ramverk för benchmarking av funktionssäkerhet inom en rad olika områden, relevanta för utvecklingen av elektroniska system till fordonsindustrin. Resultat och upptäckter från resp arbetspaket (se kapitel 4) är dokumenterade i leverablerna som kortfattat beskrivs i följande kapitel.

D1.1 Needs and requirements

Detta dokument beskriver roller och artefakter i samband med benchmarking av funktionssäkerhet. D1.1 presenterar dessutom ett antal fordonsanvändningsfall för att realisera behov och krav för benchmarking av funktionssäkerhet.

Dokumentet beskriver också vad benchmarking av funktionssäkerhet är och hur det kan användas av olika intressenter i produktframtagningsprocessen. Behoven hos de identifierade intressenterna mappas till användningen av säkerhets-benchmarks (jämförelse, profilering, krav och egenskaper). Dokumentet beskriver också BT som valts ut för projektet.

D1.2 State of the Art

Presenterar en state-of-the-art studie som relaterar BeSafe's arbete med arbeten gjorda i andra domäner och andra applikationsområden samt med vetenskapliga resultat inom den akademiska världen. Ger en översikt över funktionssäkerhetsstandarder för fordon och beskriver forskning inom området driftsäkerhets-benchmarking. Tekniker för felinjicering, robusthettester och modellbaserad bedömning av funktionssäkerhet diskuteras också.

D2 Benchmark measures

Beskriver begrepp relaterade till säkerhetselement i (SEooC, Safety Elements out of Context) och ur sitt sammanhang med avseende på ISO 26262 och en referensmodell för experimentell och analytisk benchmarking. För varje BT definierat i D1.1 Needs and Requirements, ges en uppsättning benchmarkmått med tillhörande utvärderingsmetoder.

D3 Benchmark framework

Ger ett ramverk för benchmarking av funktionssäkerhet för inbyggda system inom fordonsindustrin. Ramverket beskriver processer samt metoder och verktyg för att utföra benchmark-aktiviteter kopplade till processtandarder som ISO 26262 och ISO 15998.

D4 Evaluation

Utvärderar de föreslagna benchmarks-mätningarna, bedömningsmetoderna och själva ramverket. Visar resultatens lämplighet att användas för utveckling av inbyggda system inom fordonsindustrin. Utvärderingen utförs på flera demonstrations- och valideringssystem som lämpar sig för valda BT.

5.1 Bidrag till FFI-mål

Här följer vår uppskattning av hur BeSafe bidrar till de mål som anges i programmet FFI Fordonsutveckling 2011-02-01.

Vision Svensk text har tagits från programbeskrivningen, version 2011-02-01. Engelsk översättning av Volvo Technology. *Swedish text is taken from the programme description, version 2011-02-01. English translation by Volvo Technology*	**Level** (Låg, Medium, Hög)
Specific for FFI Fordonsutveckling	

FFI
FORDONSSTRATEGISK
FORSKNING OCH INNOVATION

Vision Svensk text har tagits från programbeskrivningen, version 2011-02-01. Engelsk översättning av Volvo Technology. *Swedish text is taken from the programme description, version 2011-02-01. English translation by Volvo Technology*	**Level** (Låg, Medium, Hög)
Svensk fordonsindustri ligger i framkant med fordon, fordons-komponenter och utvecklingstjänster som är säkra, miljöanpassade och energieffektiva. *The Swedish automotive industry is at the forefront with vehicles, vehicle components and development services that are safe, environmentally friendly and energy efficient.*	Hög
Fordonsel och elektronik / Inbyggda system och mjukvara	
Etablera nationell kompetens som förmår att utveckla komplexa inbyggda mjukvarusystem Gröna, Säkra och Anslutna fordon kräver hög nationell kompetens vilken är kapabel att utveckla komplexa elektriska system som nyttjar både ett nationellt och ett globalt utbud av forskning och teknik. *Establish national competence that is able to develop complex embedded* *software systems. Green, Safe and Connected vehicles require high national skills which are capable of developing complex electrical systems that use both a national and a global range of research and technology.*	Hög
Materialteknik för effektivare fordon	
Fordonsindustrin har fått användbara och innovativa material samt tillgång till nydanande materialanvändning. Substantiell (mätbar) viktreduktion Substantiell kostnadsreduktion Väsentligt bättre materialegenskaper *The automotive industry has got useful and innovative materials and access to* *innovative use of materials.* *Substantial (measurable) weight reduction* *Substantial cost reduction* *Significantly better material properties*	 Låg Medium Låg
Metoder och verktyg för fordonsutveckling	

FFI
FORDONSSTRATEGISK
FORSKNING OCH INNOVATION

Vision Svensk text har tagits från programbeskrivningen, version 2011-02-01. Engelsk översättning av Volvo Technology. *Swedish text is taken from the programme description, version 2011-02-01. English translation by Volvo Technology*	**Level** (Låg, Medium, Hög)
Etablera världsledande metoder och verktyg för fordons-utveckling. *Establish world-leading methodologies and tools for vehicle development.*	Hög

Svensk fordonsindustri ligger i framkant med fordon, fordonskomponenter och utvecklingstjänster som är säkra, miljöanpassade och energieffektiva
Säkerhet är ett av de viktigaste utvecklingsområden för fordon. Förutom nya säkerhetssystem så finns ökade krav och större fokus på funktionssäkerhet, dvs. ett systems förmåga att förbli i ett säkert tillstånd även om fel uppkommer under körning. EuroNCAP har sedan många år utvärderat förmågan hos nya fordon att skydda förare, passagerare och fotgängare i händelse av olyckor. Förutom att dessa tester har bidragit säkrare bilar har de också bidragit till en ökad medvetenhet bland allmänheten kring säkerhet.

I dagsläget inte finns ingen motsvarande standardiserad utvärderingsmetod för funtionssäkerhet. BeSafe har därför bidragit till en vidareutveckling inom funktionssäkerhetsområdet genom att identifiera utvärderingsenheter, utvärderingsmått samt utveckla en metodik för att effektivt och tillförlitligt genomföra sådana utvärderingar. Ett standardiserat tillvägagångssätt för att mäta funktionssäkerhet kommer att förbättra industrins förmåga att snabbare tillhandahålla säkrare, mer miljöanpassade och energieffektivare fordon.

Etablera nationell kompetens som förmår att utveckla komplexa inbyggda mjukvarusystem Gröna, Säkra och Anslutna fordon kräver hög nationell kompetens vilken är kapabel att utveckla komplexa elektriska system som nyttjar både ett nationellt och ett globalt utbud av forskning och teknik
De stora svenska OEM (Volvo AB, Volvo Personvagnar, Scania) har tillsammans med ledande småföretag och forskningsinstitut bildat BeSafe konsortiet. För att upprätthålla Sveriges ledande position inom säkerhet och kvalitet är framtagandet av nya koncept och metoder, för kvantifiering av funktionssäkerhet för komplexa elektriska och elektroniska (E/E) fordonsystem, av yttersta vikt. BeSafe's resultat har hög potential att bidra till detta.

De aktiviteter som utförts inom BeSafe stärker Volvos och andra projektpartners plats inom forskning kring funktionssäkerhet för komplexa E/E fordonsystem. Projektet har även rönt en hel del uppmärksamhet och intresse både inom Volvo och inom de andra deltagande företagen och fört upp området funktionssäkerhet (eng. functional safety) på

ett flertal interna dagordningar för att belysa behovet av utökad aktivitet inom detta område. Vidare kommer en del av projekt-resultaten att användas för uppfyllande av kraven i ISO 26262. På kort sikt säkras konkurrenskraft och arbetstillfällen genom att nya forskningsprojekt, som baserar sig på resultat från det här projektet, startas.

BeSafe är ett så kallat horisontellt projekt inom FFI och således deltar ett flertal bolag i projektet. Detta möjliggör uppbyggandet av forsknings- och innovationsmiljöer som även sträcker sig utanför Volvos koncerngräns. Här skall också tilläggas att informations-spridning från projekt till akademi och forskningsinstitut (Chalmers och SP), inom området funktionssäkerhet, har skapat starka band mellan Volvo, Chalmers och SP och diskussioner pågår kring nya idéer till framtida projektförslag. Vidare används BeSafe's projektresultat i ARTEMIS-projektet VeTeSS. Dess sammansättning erbjuder en internationellt konkurrenskraftig forskningsmiljö där akademi, institut och industri samverkar.

Delar av projektresultat från Besafe har direkt återanvänts i andra nystartade forskningsprojekt (både nationella och internationella). Utöver projekt som redan nämnts har Volvo varit med i framtagandet av projektförslaget SafeAdapt, vilket är ett projektförslag inom EUs sjunde ramprogram. Här har Volvo bidragit med såväl idéer och förslag som baseras på erfarenheter från BeSafe och från ett tidigare avslutat internt projekt med namn DEDICATE.

Fordonsindustrin har fått användbara och innovativa material samt tillgång till nydanande materialanvändning. Med mål som substantiell (mätbar) viktreduktion, substantiell kostnadsreduktion och väsentligt bättre materialegenskaper

Substantiell (mätbar) viktreduktion och Väsentligt bättre materialegenskaper har inte adresserats i projektet, och således bidrar vi inte till uppfyllelse av dessa mål.

Trots initiativ som AUTOSAR finns det fortfarande problem med felande E/E-system i fordon. I mars 2014 rapporterades det att nästan 60-70 % av alla återkallelser av fordon i Nordamerika och Europa orsakades av programvarufel [5]. År 2009 hade Toyota problem med oavsiktlig acceleration av bilar som visade sig bero på programvarufel [6]. Nyligen tvingades General Motors till en stor återkallelse av fordon på grund av ett dåligt fungerande tändningslås i flera bilmodeller. Felet kunde också senare kopplas till flera dödsolyckor [7].

Fel liknande de som beskrivts ovan orsakar enorma kostnader för fordonstillverkarna. Vi tror att genom att standardisera implementering och tolkning av funktionssäkerhets-analyser som utförs under utvecklingsfasen, kan stora kostnadsbesparingar göras på sikt.

Standardisering minskar också utvecklingskostnader eftersom konkurrensen bland tredje-parts tillverkare kommer att öka. Med en standard som bas blir det möjligt att enkelt jämföra funktionellt identiska produkter, kommunicera krav och mätningar av

systemegenskaper. Detta leder i sin tur till ett större urval av säkrare, tillförlitligare och billigare produkter.

Etablera världsledande metoder och verktyg för fordonsutveckling
BeSafe har påbörjat framtagandet av en generell standardiserad metod för säkerhetskvantifiering av komplexa E/E fordonssystem. En strukturerad metod för benchmarking av funktionssäkerhet som dessutom enkelt kan integreras i befintliga utvecklingsprocesser bidrar till effektivare och tillförlitligare utvecklingsmetoder.
Till de innovativa koncepten hör:

- Identifiering av målsystem – modeller, mjukvara och hårdvara
- Tekniker för att ta fram mätvärden för dessa system
- Framtagning av verktyg och metodik för mätning och tolkning av mätresultat kopplat till etablerade utvecklingsprocesser och ISO 26262
- Utvärdering av benchmarks, mättekniker samt metoder

Effektiva metoder och verktyg leder till fler aktörer med fokus på funktionssäkerhet vilket i sin tur leder till ett större urval av säkrare och billigare produkter.

6. Spridning och publicering

6.1 Kunskaps- och resultatspridning

Information, d v s leverabler och andra rapporter, som beskriver resultat och slutsatser från BeSafe-projektet är tillgänglig för alla anställda inom Volvokoncernen, projekt-partner och för vissa externa parter. Ett antal aktiviteter för spridning av projektresultat har anordnats i form av externa och/eller interna seminarier och workshops. Dessutom har delar av projektresultaten från BeSafe återanvänts i andra forskningsprojekt (t.ex. VeTeSS) och i tre examensarbeten.

Spridningsaktiviteter som utförs inom projektet tidsram är följande (tabell 3):

Table 3. Genomförda kunskapsspridningsaktiviteter inom Besafe-projektet.

Date	Event	Main Topics
2011-11-01	Första öppna workshopen	• Introduction to BeSafe (Martin Hiller, Volvo) • Framework and tools for benchmarking of functional safety (Daniel Skarin, SP, Johan Karlsson, Chalmers) • Benchmarking functional safety using models (Jonny Vinter, SP, Mattias Nyberg, Scania) • Benchmarking the functional safety of software (Martin Hiller, Volvo)

		• Benchmarking the functional safety of hardware (Andreas Käck, QRTech, Sylvester Vertetics, Saab)
2012-02-09	Öppet seminarium	• Some observations on the ISO 26262 Functional Safety standard (Olle Bridal, Volvo)
2012-03-08	Öppet seminarium	• Evaluation-driven design of fault handling mechanisms (Prof. Johan Karlsson, Chalmers)
2012-04-12	Öppet seminarium	• ISO 26262: Functional Safety Process Capability Determination –An Automotive SPICE approach (Ola Örsmark, Volvo Cars)
2012-05-29	Andra öppna workshopen	• Introduction to BeSafe (Patrik Isaksson, Volvo) • General Introduction to Benchmark Measures (Mafijul Islam, Volvo) • Analytical Benchmarking (Andreas Käck, QRTECH and Mattias Nyberg, Scania) • Fault Injection Benchmarks (Jonny Vinter, SP) • Tools (Behrooz Sangchoolie, Fatemeh Ayatolahi, Chalmers, Jonny Vinter SP, Johan Haraldsson, Sigurjon Thorvaldsson, Volvo)
2012-11-14	ICES seminarium	• Introduction to BeSafe (Patrik Isaksson, Volvo) • Fault injection-based benchmarking of software components (Johan Karlsson, Fatemeh Ayatolahi, Behrooz Sangchoolie, Chalmers) • Simulation of sensor failures using model-implemented fault injection (Jonny Vinter, SP)
2012-11-29	Opet lunch-seminarium	• Safe cooperative autonomous vehicles in an uncertain environment (Rolf Johansson, SP)
2013-05-30	Tredje öppna workshopen	• Benchmarking functional safety using Continuous Time Markov Chains (Andreas Käck, QRTECH) • Functional Safety Benchmarking Using Bayesian Networks Derived from Safety Requirements (Mattias Nyberg, Scania) • Do We Need to Inject Double Bit-flip Errors When Benchmarking the Hardware Error Sensitivity of Software Components? (Behrooz Sangchoolie, Chalmers) • Testing Robustness of Software Components in AUTOSAR (Johan Haraldsson, Volvo) • Model-based fault injection in the context of

		ISO 26262 (Jonny Vinter, Daniel Skarin, SP) • Demo section –fault injection tools
2013-06-27	Presentation examensarbeten	• Binary-level fault injection for AUTOSAR-based systems (NITHILAN MEENAKSHI KARUNAKARAN) • Robustness testing of AUTOSAR software components (VICTOR JANSSON, JERRY LINDAHL)
2014-03-13	Fjärde öppna workshopen	• Welcome and BeSafe Project Summary (Mats Olsson, Volvo • Overview of Activities and Results (Johan Karlsson, Chalmers) • Automatic Hardware FMEA:s Using SPICE (Andreas Käck, Qrtech) • Towards Benchmarking Hardware Error Sensitivity (Fatemeh Ayatolahi and Behrooz Sangchoolie, Chalmers) • Functional Safety Benchmarking Using Bayesian Network (Mattias Nyberg, Scania) • Mapping Model-Implemented Fault Injection to ISO 26262 (Daniel Skarin, SP) • Software Metrics in the Context of ISO 26262 (Mafijul Islam, Volvo)

6.2 Publikationer

An Investigation of the Fault Sensitivity of Four Benchmark Workloads (Sangchoolie, Behrooz; Ayatolahi, Fatemeh; Karlsson, Johan).
Presented at SOBRES workshop in Braunschweig, Sep 16-21, 2012.

On the Impact of Hardware Faults – An Investigation of the Relationship between Workload Inputs and Failure Mode Distributions (Leo, Domenico Di; Ayatolahi, Fatemeh; Sangchoolie, Behrooz; Karlsson, Johan; Johansson, Roger).
SAFECOMP conference in Magdeburg, Sep 25-28, 2012.

Benchmarking the Hardware Error Sensitivity of Machine Instructions (Sangchoolie, Behrooz; Ayatolahi, Fatemeh; Barbosa, Raul; Johansson, Roger; Karlsson, Johan).
SELSE workshop in Stanford, Mar 26-27, 2013.

Towards Benchmarking of Functional Safety in the Automotive Industry (Islam, Mafijul; Sangchoolie, Behrooz; Ayatolahi, Fatemeh; Skarin, Daniel; Vinter, Jonny; Törner, Fredrik; Käck, Andreas; Nyberg, Mattias; Villani, Emilia; Haraldsson, Johan; Isaksson, Patrik; Karlsson, Johan).

EWDC workshop in Coimbra, May 15-16, 2013.

A Study of the Impact of Single Bit-Flip and Double Bit- Flip Errors on Program Execution (Ayatolahi, Fatemeh; Sangchoolie, Behrooz; Johansson, Roger; Karlsson, Johan).
SAFECOMP conference in Toulouse, Sep24-27, 2013.

Failure Propagation Modelling for Safety Analysis Using Causal Bayesian Networks (Mattias Nyberg).
2nd International Conference on Control and Fault-Tolerant Systems in Nice, Oct 9-11, 2013.

A Study of The Impact of Bit-flip Errors on Programs Compiled with Different Optimization Levels (Sangchoolie, Behrooz; Ayatolahi, Fatemeh; Johansson, Roger; Karlsson, Johan).
EDCC conference in Newcastle, May 13-16, 2014.

Binary-Level Fault Injection for AUTOSAR Systems (Mafijul Md. Islam, Nithilan Meenakshi Karunakaran, Johan Haraldsson, Fredrik Bernin and Johan Karlsson).
EDCC conference in Newcastle, May 13-16, 2014.

6.3 Examensarbeten

Robustness Testing of AUTOSAR Software Components (Victor Jansson and Jerry Lindahl).
An automatic prototype tool for robustness testing of AUTOSAR software components (SW-C) is presented.

Binary-Level Fault Injection (BLFI) for AUTOSAR-based Systems (Nithilan Meenakshi Karunakaran).
Proposes a binary-level fault injection technique called BLFI, which performs robustness testing on AUTOSAR-based systems.

Evaluation of Error Handling Mechanisms for Automotive Embedded Systems (Andreas Åkesson and Anton Hemlin).
On-going ..Will be finalized in Jun, 2014.

7. Slutsatser och fortsatt forskning

Ett ramverk för benchmarking av funktionssäkerhet för inbyggda system inom fordonsindustrin har presenterats. Tre olika användningsområden för ramverket har diskuterats, nämligen experimentell benchmarking, analytisk benchmarking och användningen av statisk mjukvarauanalys. Olika verktyg, som kan användas för att mappa benchmarks-mätningar till ISO 26262 och till definierade behov och krav.

I den experimentella benchmarking av funktionssäkerhet, var felinjektionsexperiment den huvusakliga metoden för benchmarking. Emellertid har endast en liten delmängd av

tillgängliga verktyg och metoder som använts i denna studie. MODIFI , BLFI och GOOFI - 2 presenterades som de viktigaste verktygen för att utföra felinjektions-experiment på Simulinkmodeller, binärkod resp assemblerkod. För analytisk benchmarking av funktionsäkerhet är felspridning och felintensitet hos ett system de viktigaste indata till analysen. Analysmetoderna kan användas både på mjukvaru- och hårdvarusystem. Två analytiska verktyg har använts i denna studie. Det första använder ”Markov-chain” modeller som möjliggör automatisk beräkning av benchmarking-måttet för funktionssäkerhet med avseende på hårdvarufel och det andra verktyget använder Bayesianska nätverk. Till sist, diskuterades ett ramverk för användandet av mjukvaruanalys för benchmarking av funktionssäkerhet. Ett exempel som diskuterades är statisk kodanalys som i ISO 26262-6:2011, klausul 8.4.5, rekommenderas för ASIL A och starkt rekommenderas för ASIL B - ASIL D som en metod för verifiering av mjukvarudesign och implementation.

Det är värt att nämna att projektresultaten inte bör ses som en generell standard för benchmarking av funktionssäkerhet. En mer realistisk och jordnära syn är att resultaten kan användas som utgångspunkt för framtida forskning inom detta område. Till exempel behövs mer forskning för att korrekt kunna mappa banchmark-mätningarna gjorda i BeSafe-projektet till olika ASIL nivåer. Detta på grund av att informationen, om frekvensen och svårighetsgraden på alla möjliga fel som kan uppkomma, saknas. Som en del av den framtida forskningen, bör resultat som erhållits från analytiska och experimentiella mätningar också jämföras. Detta bör göras både på komponent- och elementnivå. Förbättringen av mjukvarukomponenter (SW-C) med hjäp av mekanismer som föreslagits i AUTOSAR är också en del av det framtida arbetet. Dessutom har BeSafe-projektet i huvudsak riktat in på mjukvarukomponenter instället för BSW-komponenterna (Basic Software Components) i AUTOSAR-plattformen –m a o har projektet främst fokuserat på benchmarking av funktionssäkerhet hos element tagna ur sitt sammanhang. Därför är benchmarking av element satta i sitt sammanhang samt AUTOSAR BSW delar i det framtida arbetet.

8. Deltagande parter och kontaktpersoner

Volvo Technology AB
Mats Olsson
mats.olsson.2@volvo.com
+46 31 323 59 11

Volvo Technology AB
Johan Haraldsson
Johan.Haraldsson@volvo.com
+46 31 3223915

FFI
FORDONSSTRATEGISK
FORSKNING OCH INNOVATION

Volvo Technology AB
Mafijul Islam
mafijul.islam@volvo.com
+46 31 3228296

Chalmers Tekniska Högskola
Johan Karlsson
johan@chalmers.se
+46 31 772 16 70

Qrtech AB
Andreas Käck
Andreas.Kack@qrtech.se

Scania CV AB
Mattias Nyberg
mattias.nyberg@scania.com
+46 8 553 899 57

SP Technical Research Institute of Sweden
Jonny Vinter
jonny.vinter@sp.se
+46 10-516 53 59

Volvo Car Corporation
Fredrik Törner
fredrik.torner@volvocars.com
+46 31 3259271

9. Referenser

[1] K. Lemke, C. Paar and M. Wolf, Embedded Security in Cars, Berlin: Springer-Verlag, 2006.

[2] ISO Standard, [Online] http://www.iso.org/iso/catalogue_detail?csnumber=43464. [Accessed 2013].

[3] Technical Safety Concept Status Report, [Online] http://www.autosar.org/download/R4.0/AUTOSAR_TR_SafetyConceptStatusReport.pdf [Accessed 2013]

[4] IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems, [Online] http://www.iec.ch/zone/fsafety . [Accessed 2013].

[5] B. Fleming, An overview of advances in automotive electronics, Vehicular Technology Magazine, IEEE 9 (1) (2014) 4{9.

[6] EmbeddedGurus: An Update on Toyota and Unintended Acceleration, http://embeddedgurus.com/barr-code/2013/10/an-update-on-toyota- and-unintended-acceleration, Accessed: 2014-04-08.

[7] Reuters: GM expands ignition switch recall to 2.6 million cars, http://www.reuters.com/article/2014/03/28/us-gm-recall-expanded-idUSBREA2R1Y920140328, Accessed: 2014-04-08.

Adress: FFI/VINNOVA, 101 58 STOCKHOLM
Besöksadress: VINNOVA, Mäster Samuelsgatan 56, 101 58 STOCKHOLM
Telefon: 08 - 473 30 00