



Cost Efficient Dependable Electronic Systems

# Verksamhetsberättelse

## 2005

Författare	Håkan Edler
Dokumentnr	010
Version	1.0
Datum	28 februari 2006
Tillgänglighet	Allmän
Status	Slutlig

CEDES – Cost Efficient Dependable Electronic Systems – är ett forskningsprojekt inom IVSS. Dess syfte är att möjliggöra aktiva säkerhetssystem som standardutrustning i nyproducerade fordon, vilket höjer trafiksäkerheten och blir därigenom ett medel att uppnå nollvisionen. Det förutsätter att kostnaden för sådana system sänks radikalt vilket är huvudmålet med projektet.

CEDES skall utforska, utvärdera och demonstrera kostnadseffektiva metoder för feltolerans i säkerhetskritiska fordonsbaserade elektronisksystem. Eftersom varje elektronikdel drar med sig en tillverkningskostnad gäller det att minimera omfattningen av elektroniken. Detta strider mot krav på säkerhet, som kan kräva t ex dubbla enheter för en kritisk funktion. Säkerheten måste därför skapas med mekanismer för feltolerans i programvara. De utvecklade mekanismerna skall om möjligt vara modulariserbara och speciellt anpassade för att kunna integreras i en given fordonsarkitektur.

Förutom tekniska lösningar arbetar CEDES med utvecklingsprocesser för programvara för styrsystem i fordon. Av särskilt intresse är hur kund och leverantör samverkar vid utveckling av komponenter.

För verifiering och validering av tekniken utvecklar CEDES realistiska experimentsystem. För tillämpning av tekniken projekterar CEDES demonstratorer.

CEDES tar ett brett grepp på säkerheten i framtida fordon med teoretiska analyser, praktiska metoder och experimentell verifiering och validering.

Partners i CEDES är Volvo Personvagnar, Volvo AB, Autoliv Electronics AB, Chalmers tekniska högskola och SP Sveriges Provnings- och Forskningsinstitut AB.

## 1. AKTIVITETER

### 1.1 WP 1 Utvecklingsprocess

Arbetspaketet skall arbeta fram en kostnadseffektiv process för pålitliga fordonssystem. I det ingår att studera gällande standarder och aktuell praxis för att anpassa utvecklingsprocessen till dem. Hänsyn till säkerhetskrav skall vara en integrerad del av processen. Den skall vara anpassad till fordonsindustrins krav och kunna integreras i nuvarande processer. Av särskilt intresse är, att kunna definiera ett antal kontrollpunkter med tydliga styrparametrar och mätetal för avstämning mellan kund och leverantör vid ett flertal tillfällen under ett kontrakterat utvecklingsarbete.

Krav på funktioner i ett system kan idag hanteras med etablerade metoder. Begränsningar och krav på egenskaper saknar metod och process för sin hantering. Pålitlighet och feltolerans är exempel på sådana egenskaper och arbetspaketet avser hitta metoder att hantera dem och införliva dem i utvecklingsprocessen.

Under året har vi i arbetspaketet gjort studier på användningsfall ur ett antal infallsvinklar. Användningsfall är ett medel att specificera en uppdragstagares åtagande och de kan ge möjlighet att mäta framsteg i utvecklingen. Av särskilt intresse är, att skapa en domänmodell för fordonstillämpningar och en standard för användningsfall.

Projektet planerar SEL – Software engineering laboratory – ett laboratorium för systemutveckling, där man kan mäta hur nya tekniker och metoder påverkar sättet att utveckla ett pålitligt programmerat elektronisksystem.

### 1.2 WP 2 Programvaruanalys

Ett kostnadseffektivt elektronisksystem kan inte replikera elektronikenheter, utan måste lägga redundans och diversitet i programvara. Tidigare forskning har visat att effektiviteten av mekanismer för felhantering beror starkt på var de placeras i programmen. Därför bör man tidigt i en ut-

vecklingsprocess identifiera vilka mekanismer man avser använda och var de skall placeras. Arbetet kommer att baseras på tidigare forskning vid Chalmers om felpropagering och programvaruprofilering.

I ett tidigt skede av en utvecklingsprocess gör man huvudsakligen statisk analys av modeller och programtext. Analysen syftar till att finna fel och att bedöma kvalitet. Idag arbetar man huvudsakligen manuellt, vilket är tidsödande och kostsamt. Dessutom har kvalitet i programvara så många faktorer, att bedömningen blir svår. I arbetspaketet skall vi studera möjligheterna att automatisera analysen, då ett automatiskt verktyg skulle ge reproducerbara resultat och vara kostnadseffektivt. Det kan då användas flerfaldiga gånger på en given produkt under dess uppbyggnad.

Under året har vi i arbetspaketet studerat hantering av undantag/avbrott i C++ med syfte att ge underlag för källkodsbibliotek med mekanismer för felhantering. En studie av hasardanalys på användningsfall har också gjorts.

### 1.3 WP 3 Felhanteringsmekanismer

De fundamentala delarna i ett kostnadseffektivt programmerat elektronisksystem är mekanismerna i programvara för felhantering. Viktiga delar i arbetspaketet är:

- Utforskning av vilka mekanismer som är lämpliga att lägga i programvara.
- Placering av mekanismerna i ett feltoleranslager så att de ingår som komponent i datorns operativsystem.
- Realisering av mekanismerna som aspekter, varigenom de bryts ut ur tillämpningsprogrammen.
- Realisering av mekanismerna som funktioner i ett källkodsbibliotek.
- Utvärdering av alternativen genom experiment med felinjicering.

Arbetspaketet skall resultera i en arkitektur för ett pålitligt, kostnadseffektivt, programmerat elektronisksystem och ett API för användning av mekanismerna för felhantering.

Aktiviteten har under året varit stor inom arbetspaketet. Rubriker på aktiviteterna är:

- Evaluering av användningen av Mamut för COTS
- Studie av möjligheten att använda aspekter för felhantering
- Mamut för C
- Effektiv testning genom mutering av C-program
- Membership agreement på tillämpningsnivå
- Partitionering av datorsystem för samtidig exekvering av flera tillämpningar
- Begränsningar i metoderna för felinjicering med programvara

Flera examensarbeten pågår inom arbetspaketet.

### 1.4 WP 4 Verifiering and Validering

#### 1.4.1 C-version av KeY

KeY är ett verktyg för formell verifiering av källkod som utvecklas vid Chalmers och två tyska universitet. Nuvarande version hanterar en stor delmängd av Java. Målet med denna CEDES-aktivitet är att ta fram en version av KeY som hanterar en stor delmängd av programspråket C (t ex MISRA C). Aktiviteten består dels av implementeringsarbete för att anpassa infrastrukturen i KeY till ett nytt programspråk, dels av arbetet att ta fram en kalkyl för symbolisk exekvering av C-kod.

Hittills har tiden mest använts till implementeringsarbetet. De två huvuduppgifterna inom detta arbete är att integrera en "front-end" (parser + analysverktyg) för C i KeY samt att refaktorisera och utöka datastrukturerna i KeY, som används för att representera program. Uppskattningsvis

har 75% av integreringen samt 25% av refaktoriseringen / utökningen av datastrukturerna utförts. Ett examensarbete som ska fortsätta implementeringsarbetet har påbörjats och kommer att pågå under första halvan av 2006.

#### 1.4.2 Formell verifiering av aspekter för feltolerans

Utgångspunkten för denna aktivitet är idén att använda aspektorienterad programmering för att lägga till feltolerans till programvara. Den separation - av feltoleranskoden från funktionskoden - som detta resulterar i öppnar upp möjligheten att formellt verifiera feltoleranskoden oberoende av funktionskoden. Detta är nödvändigt eftersom funktionskoden alltid har ett korrekt beteende vid verifieringen, medan feltoleranskoden ska bevisas garantera korrekt (eller acceptabelt) systembeteende då funktionskoden betar sig inkorrekt.

#### 1.4.3 Symbolisk felinjicering

I nuläget valideras feltoleransen hos datorsystem m h a diverse felinjiceringstekniker, vilket resulterar i en experimentell validering. Målet med denna CEDES-aktivitet är att ta fram en mer analytisk metod som vi kallar symbolisk felinjicering. Metoden bygger på symbolisk exekvering av källkod. Tanken är att symbolisk felinjicering kan komplettera konventionella felinjiceringstekniker på samma sätt som formell verifiering kompletterar testning.

### 1.5 WP 5 Experimentsystem och demonstrator

För experimentell utvärdering av det teoretiska arbetet skall en realistisk testmiljö byggas upp inom projektet. Den kommer att bestå av datorkort från GAST-projektet som kommunicerar med en omvärldssimulator. I GAST-korten körs styrsystem för valda tillämpningar med de varianter av felhantering, som skall utvärderas. I omvärldssimulatorens körs modeller av fordonets fysiska delar och den väg man kör på under experimentet. Experimenten sker genom injicering av fel i styrsystemen under körning. För styrsystemen kommer vi att använda förenklade modeller av verkliga system. Projektets industripartners bidrar med modeller för såväl styrsystem som omvärld.

Förutom experimentsystemet kan projektet behöva demonstratorer, dels för att visa effekterna av elektronisksystem i väsentliga funktioner i fordon, dels för att visa utvecklingsmetoder och utvecklingsverktyg.

Experimentsystemet är under utveckling genom ett antal examensarbeten. Demonstratorerna projekteras för tillfället.

### 1.6 WP 0 Projektledning

Projektledningen under året har inneburit konventionella projektledningsaktiviteter som:

- Löpande planering och uppföljning av projektet internt och externt
- Kontakt med andra organisationer
- Presentation av projektet externt
- Initiering och drift av öppna seminarier
- Möten med kallelse, dagordning, ledning av möten samt anteckningar och protokoll
- Utformning och uppbyggnad av experimentsystem och demonstratorer
- Skapande av Webbsidor och e-postlistor
- Utformning av logotyp och mallar för presentationer och dokument

## 2. PUBLIKATIONER

CEDES har fått åtta publikationer accepterade under året:

Alexandersson, Ruben, Öhman, Peter (2005). Aspect oriented software implemented node level fault tolerance. *IASTED International Conference on Software Engineering and Applications (SEA)*.

Alexandersson, Ruben, Öhman, Peter (2005). A technique for fault tolerance assessment of COTS. *International Conference on Computer Safety, Reliability and Security (SAFECOMP)*.

Alexandersson, Ruben, Larsson, Daniel (2005). Formal Verification of Fault Tolerance Aspects. *International Symposium on Software Reliability Engineering (ISSRE)*.

Bergenheim Carl, Sivencrona Håkan, Cost Efficient and Dependable: CAN in Advanced Applications, *International Conference on Dependable Systems and Networks 2005, (DSN)*.

Ivarsson, Martin, Pettersson, Fredrik, Öhman, Peter (2005). Improved control of automotive software suppliers. *Product focused process improvement (PROFES)*.

Pettersson, Fredrik, Ivarsson, Martin, Öhman, Peter (2005). An initial study of an automotive software engineering laboratory. *Conference on Software Engineering Research and Practice in Sweden (SERPS)*.

Pettersson, Fredrik, Ivarsson, Martin, Öhman, Peter (2005). Automotive use case standard for embedded systems. *ICSE workshop on Software Engineering for Automotive Systems*.

Törner, Fredrik, Ivarsson, Martin, Pettersson, Fredrik, Öhman, Peter (2005). An Empirical Quality Assessment of Automotive Use cases. *Conference on Software Engineering Research and Practice in Sweden (SERPS)*.

## 3. SEMINARIER

CEDES håller öppna seminarier för fordonsindustrins utvecklingsingenjörer, andra forskare inom området och övriga intresserade. Seminarierna har varit uppskattade och runt 40 personer har kommit till varje. Under året har CEDES presenterat seminarierna:

- 12 maj Martin Ivarsson och Fredrik Pettersson, ”Förbättrad styrning i fordonsindustrins leverantörskedja”
- 2 jun Roger Johansson, ”Schemaläggning av tids- och händelsestyrd kommunikation på CAN-bussen.”
- 5 sep Sibylle Schupp, “Generic software libraries: Design once, run anywhere”
- 13 okt Ruben Alexandersson, ”Aspektorienterad programmering”
- 3 nov Reiner Hähnle, “Formal verification of source code”
- 1 dec Martin Hiller, ”Propagering av fel i programvara”

## 4. EXAMENSARBETEN

### 4.1 Avslutat

Daniel Örstadius, ”Formal methods and aspect oriented programming”

### 4.2 Pågående

Gustav Munkby, “Analysis of exception behaviour to support libraries”

Mohamd Ali Qadir, “Byte code fault injection”

Johan Magnusson, "Aspect C++ Set and Get Joinpoints"

Mattias Pettersson och Petter Uvesten, "En experimentmiljö med GAST och FlexRay"

Erik Bengtsson, "Demonstrator G1/FlexRay"

Magnus Källvik och Jonas Eriksson, "Aktuatorer och sensorer för GAST G2"

Olof Johnsson och Fredrik Johansson, "Simulinkmodeller för by-wire applikationer"

## 5. ORGANISATION

Interna möten har hållits på tre nivåer:

- Möte med ledningsgrupp
- Projektmöte
- Veckomöte.

Ledningsgruppens möten har som huvudsyfte haft målstyrning och uppföljning.

Projektmöten har syftat till att ge samtliga projektmedlemmar en helhetssyn och vara ett diskussionsforum för idéer om kommande aktiviteter.

Veckomötena är till för projektstyrning och uppföljning. I dem gör man den detaljerade aktivitets- och tidsplaneringen och diskuterar teknik.

Möten med ledningsgrupp och projektmöten har hållits halvårsvis.

Organisationen ändrades i december 2006, så att projektmötet blir ett månadsvis möte med projektledningen, ansvariga för arbetspaket och examinatorer för doktorander. Dess uppgift är styrning av den operativa verksamheten.

En workshop för alla medverkande i projektet och andra intressenter kommer att organiseras vid behov. Tanken är, att en sådan workshop kan vara årligen återkommande.

## 6. PERSONAL

Doktorander i CEDES var den 31 december 2005:

Martin Ivarsson, Daniel Larsson, Fredrik Pettersson och Daniel Skarin, som är finansierade av projektet.

Ruben Alexandersson som är finansierad av Chalmers stiftelsemedel.

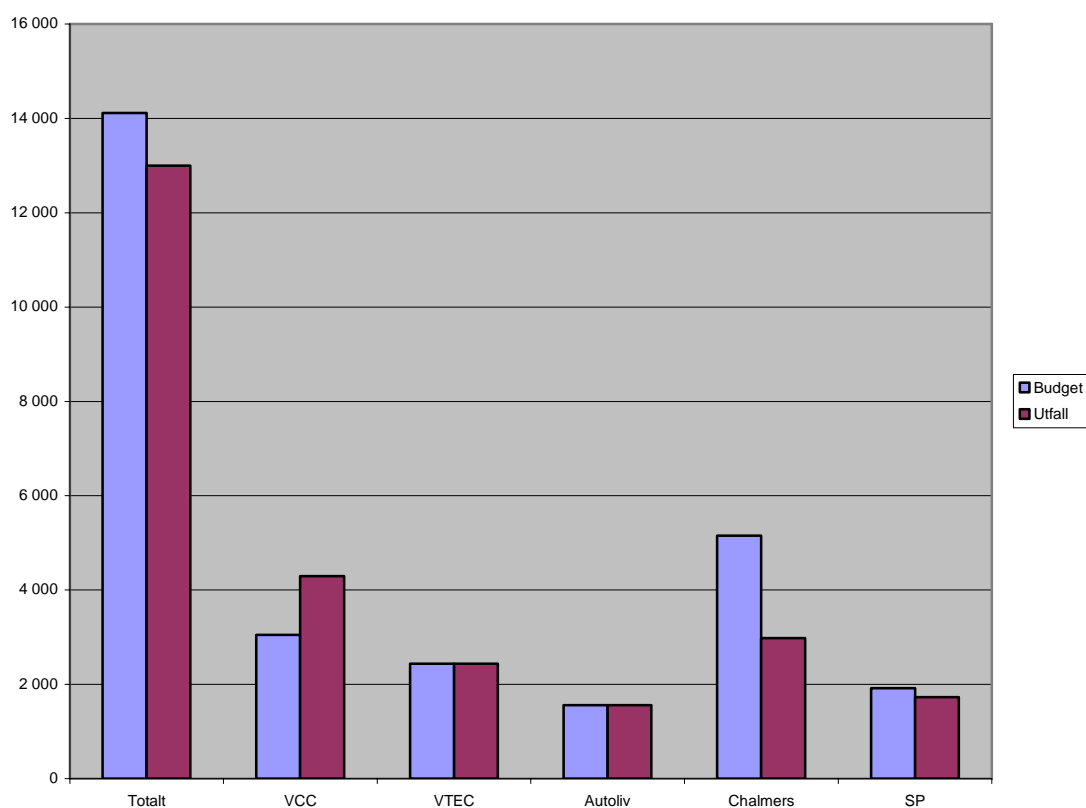
Carl Bergenhem, SP, och Fredrik Törner, Volvo PV, som är industridoktorander.

Tio examensarbetare är engagerade i projektet och en har just avslutat sitt examensarbete.

### 7. EKONOMI

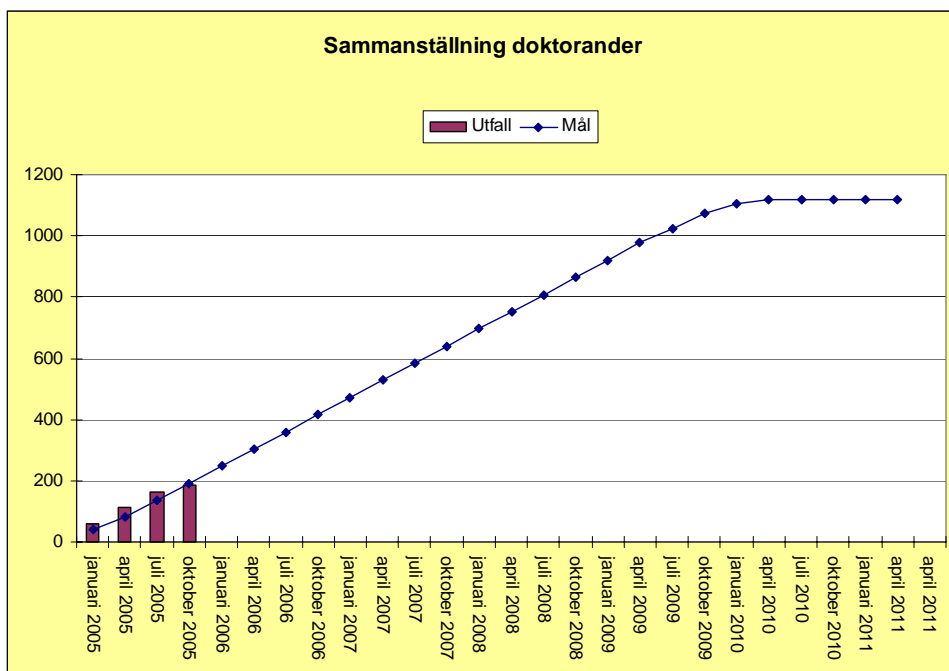
Kostnader i kkr t o m december 2005:

	Totalt	VCC	VTEC	Autoliv	Chalmers	SP
Budget	14 113	3 046	2 438	1 558	5 155	1 916
Utfall	13 002	4 297	2 438	1 558	2 978	1 731
Löner*	11 590	4 297	2 438	1 558	1 835	1 462
Maskinkostnad**	116				116	
Utrustning (inköp)	139				139	
Material	0					
Resor	141				108	33
Patent	0					
Övrigt	465				229	236
Förvaltning***	551				551	
Övrigt	0					



## 8. AVKLARADE DOKTORANDPOÄNG

För doktorsexamen krävs 160 studiepoäng. 40 poäng ges för avklarade kurser och 120 poäng för publicerade verk. I figuren visas prognosen för avklarade poäng som mål och doktorandernas aktuella framsteg som utfall. Värdena gäller t o m kvartal 4 2005 och är summerade för alla doktorander. För kurserna har kursplanens poäng använts och för publikationer en bedömning av tillgoräknade poäng.



## 9. FORTSATT ARBETE

Den närmaste tidens planering:

- Åtta bidrag vid givna vetenskapliga konferenser är i dagsläget planerade.
- Arbete med uppbyggnad av ett laboratorium för systemutveckling pågår.
- Domänmodeller skall studeras som ett sätt att höja kvaliteten på användningsfall.
- Arbete med pålitlighetsanalyser baserade på användningsfall fortsätter.
- Arbete med aspektbaserade mekanismer för felhantering fortsätter.
- ”Membership handling” inom distribuerade tillämpningar studeras.
- En översikt över betydelsen av partitionering i fordonstillämpningar skall göras.
- Automatisk analys av programkod i Misra-C utvecklas.
- Experimentsystemet byggs upp och en första version skall vara driftklar i juni 2006.
- En större demonstrator planeras.