SESAM
Försvarssektors användargrup
för
Sofware Engineering

Uppdragsspecifikation
SäkAnalysMetoder

FMV dokumentbeteckning
14910:88774/2005

Ver
1.1

Förslagställare (namn och företag)
I-L Bratteby-Ribbing, FMV

Datum
2006-06-26

Mottagare
SESAM VU, Combitech, FMV, Kockums, Saab Aerotech, Saab Systems(Land & Air, Naval), S&T

Fastställd (VU-SESAM alt deltagande medlemmar)
Se avsn. 7

Informationsklass
Intern SESAM

1 Bakgrund

SESAM är ett samverkansnätverk för projektövergripande och företagsneutral kunskapsuppbyggnad och kunskapsspridning inom området programvaruintensiva försvarssystem.
Arbetet utförs i arbetsgrupper, bl a i form av mikroprojekt.

SESAMs intressegrupp för Programvarusäkerhet studerar programvaruegenskaper av betydelse för säkerhetskritiska system[1] samt tekniker och metoder som stödjer systemsäkerhetsverksamheten på programvarunivå. Ett av de områden som gruppen funnit intressant att studera närmare är vilka metoder för systemsäkerhetsanalys, som speciellt lämpar sig för programvarusystem vid olika skeden i systemutvecklingen[2].

2 Uppgift

- Att ta fram ett eller flera typexempel tillräckligt förenklade för att en oinitierad person snabbt skall kunna sätta sig in i tillämpningen, [2].
- Att framställa faktablad inför varje systemsäkerhetsanalysfas och metodprov[3].
- Att prova och utvärdera olika metoder för systemsäkerhetsanalys på ett typexempel.
- Att överväga om provad metod behöver kompletteras m a p programvaruaspekter[4].
- Att avgöra vilka systemsäkerhetskrav ur H SystSäk resp H ProgSäk som kan vara relevanta.
- Att dokumentera frågeställningar och resultat från varje analysmetod.
- Att lagra dokumenterat material på SESAM:s hemsida för självstudieändamål.

3 Syfte

Att öka förståelsen för hur och när olika analysmetoder kan tillämpas – både hos dem som deltar i projektet och de som senare tar del av resultaten på hemsidan.

4 Mål

Att hålla hemsidan uppdaterad med olika analysmetoder allt eftersom dessa blir tillgängliga.

5 Avgränsningar

Resultatet begränsas av de tidsramar och resurser som ges för SESAM-uppdrag.

6 Genomförande

Inventering av hur aktuell analysmetod hanteras på det egna företaget (mallar m m).
Insamling av referenser som beskriver aktuell analysmetod.
Sammanställning av ett faktablad för varje metod.
Inläsning av aktuell analysmetod före prov.
Prov av analysmetod under gruppmöten.
Ensning av teknik, mallar etc.
Dokumentation, utvärderingar etc genom email-kommunikation.

---

[1] System med risk att kunna skada person, egendom eller miljö.
[2] Metod för systemsäkerhetsanalys (hur): t ex FTA (för distinktion mellan metod resp typ, se [1]: sid 174, 205).
Typ av systemsäkerhetsanalys (vilket skede i systemutvecklingsprocessen, dvs när & på vad). Ex: PHL, PHA, SHA.
[3] Där bl a referenser till metodbeskrivningar inkluderats, se t ex [3].
[4] T ex 'Dolda förutsättningar' som exempel på riskfylld programvaruaspekt att inkludera i PHL:s generella riskkällelista (fler exempel kan vaskas fram ur fallstudier/handböcker, se [1],[5]). Ett tänkbart resultat kan vara [4].

Metoderna betas av i den ordning som normalt tillämpas för ett system.
Först ut blir därmed PHL-analys, [3].

7 Deltagare

Namn[5]	Företag	Roll	Delområde
Inga-Lill Bratteby-Ribbing	FMV	Projektledare	Projektförutsättningar, Sammanfattningar.
Lars Forsell	S&T	Analysdeltagare	
Ingemar Johansson	Saab Aerotech	-”-	
Björn Koberstein	FMV	-”-	Projektförutsättningar
Peter Nummert	Combitech	-”-	
Mari Persson	Kockums	-”-	
Stefan Pettersson	Saab Systems, Land & Air	-”-	
Carl-Erik Strandberg	Saab Systems, Naval	-”-	

8 Avrapportering

- Under gruppmöten samt SESAM:s höstmöte.
- Skriftliga slutrapporter vid avslut innehållande bl a
  - Grundläggande förutsättningar och antaganden
  - Ingångsparametrar (t ex faktablad med beskrivningar av olika analysmetoder)
  - Slutsatser, rekommendationer, förslag till fördjupningar etc.

9 Tidplan

Start: 06-02-02
Etappindelning/Milstolpar: En analystyp/-metod per gruppmöte.
Maildiskussioner/-kompletteringar mellan möten.
Avslut[6]: Under -06 eller -07.

10 Referenser

[1] Försvarsmaktens handbok för programvara i säkerhetskritiska tillämpningar, M7762-000531 H ProgSäk.
[2] Ejection system – ett typexempel för systemsäkerhetsanalys, FMVdokument 14910:88824/2005.
[3] PHL-analys, Faktablad för Preliminär riskkällelista, FMVdokument 14910:2662/2006.
[4] Checklista Programvarans riskkällor, FMVdokument 14910:12183/2006.
[5] Programvarusäkerhet –en introduktion, FMVdokument KC Ledstöd 14910:38346/02.

11 Dokumenthistorik

Version	Datum	Beskrivning
1.0	06-01-12	1:a version.
1.1	06-02-28	Uppdateringar efter den första genomförda systemsäkerhetsanalysfasen 06-02-14.
1.2	06-06-26	Ny projektdeltagare (se avsn 7).

[5] Medlemmar som tillstyrkt sitt deltagande i projektet.
[6] Projektet kan återupptas då nya analysmetoder/-typer dyker upp.