IG Programvarusäkerhet: Möte #17, 06-08-22. Antal mötesdeltagare: 8 (se aktuell medlemslista).

1. Mikroprojektet SäkAnalysMetoder:
a) Underlag FMECA-studie: *Ordf* sände ut följande material före mötet: Felhanteringssystem uppdaterad/anpassad för FMECA-provning (Funktionsmoder), Faktablad (nytt: FMECA, uppdaterade: HAZOP, GenHzChecklist, GenSwHzList, PHA), ny artikel om hierarkisk FMEA samt självstudiefil (för hemsidan). Gruppen gick under mötet igenom detta material, där checklistan över programvarans riskkällor förmodas vara unik (om motsv finns någon annanstans: berätta var!).
b) Resumé föreg analysmöte: Se mötesanteckningar #16. HAZOP-tabellen för *Ejection system* kompletterades vid efterföljande mailstafett: ändrad tolkning av några nyckelord. Ytterligare uppdateringar under detta möte: löpnumrering, avvikelse, orsak. De avvikelser, som bedömdes vara säkerhetskritiska, överfördes därefter till PHA:s riskkällelista.
c) FMECA-prov: Diverse ansatser gjordes att prova metoden på en uppdaterad beskrivning av tidigare 'Felhanteringssystem', men antingen var underlaget inte tillräckligt detaljerat eller också passar inte metoden på programvara, som ännu ej implementerats. De litteraturexempel som ges för programvarusystem verkar egentligen mest handla om felmod hos hårdvara (ventil fastnad i öppet/stängt läge osv). Är metoden endast effektiv för redan implementerad programvara, COTS etc, så har programvaran andra typer av mer specialiserade analysmetoder att ta till. De riskreduceringar/ designförändringar som visar sig nödvändiga kommer i så fall in i ett alltför sent skede (kostsamt). De felmod, som identifierades under mötet var huvudsakligen av generella typ (deadlock, ohanterad exception, minnesbrist) snarare än specifika för studerat system. Kan det vara så, att där FME(C)A utförts på programvara, detta har varit ett krav, inte att metoden anses effektiv för programvara? Se Hemläxa under 4c.

2. EUROCAE/RTCA:s flygstandarder: *Mikael Thorvaldsson* från Knowit Technowledge gav en resumé över hur flygstandardernas revisionsarbete fortskridit sedan vårt möte #11 (april 2005). Wg-71 (300 pers) ser bl a på 178C. De 7 undergrupperna har ombildats. Bland nya tekniker, som skall in, finns MBD (Modellbaserad design), OO-teknik, IMA, Formella metoder, Återanvändning/COTS. Två möten har hållits sedan sist. Konsensus gäller o arbetet går långsamt (COTS-gruppen har ej startat, CNS/ATM:s domänspecifika problem har inte börjat avhandlas). Formerna för 178C är ännu ej lösta (tex huruvida Do-178 o Do-278 skall slås samman). Likaså diskuteras att ta bort de vägledande avsnitten (t ex tabellerna i Annex A). Dock förväntas mycket hända det sista året (2008), då allt skall vara klart. Bland nyheterna: Förslag på hur verktyg skall certifieras, uppdelning av MBD (Boundary-HW-Mapping-Verifiering), Anpassning av 178C till systemsäkstandarder som ARP-4754 (vilken nyttjar riskbegreppet), FAA, EUROCONTROL: IEC61508. Förutom Mikael finns två nyare svenska deltagare: Rikard Johansson o Thomas Jansson (Saab). Mer info: http://forum.pr.erau.edu/SCAS + OH:s.

3. Exempel på Safety Case & systemsäkerhetsarbete för flyget: *Mikael* beskrev de säkerhetsanalyser som utförts vid LFS/LFV:s införande av EUROCAT 2000E (projekt MATS). Målsättningen är att olycksbidraget från systemet högst skall vara 1 på 10^7 flygtimmar. Ett Safety Case togs fram per delsystem. Risker identifierades (*hazard log* upprättades), konsekvenser analyserades, riskmål identifierades på systemranden, olika analysmetoder tillämpades (FTA; FMEA osv). Dessa analyser ledde till vissa arkitekturändringar (t ex införande av ett oberoende back-upsystem: det gla ATCAS-systemet) och förnyade analyser för att kontrollera om tilldelad riskbudget därmed var uppnådda.

4. Övrigt:
a) ISSC´06: ***(a1)*** Standardrevisioner: *Mil Std 882E*-arbetet blev stoppat i feb, då ansvaret överfördes från AirForce till DoD. Fortfarande verkar ingen veta när det kommer igång igen. Ansvarig konsult vill samordna standarden med motsv för Health & Environment och verkar _ enl de som arbetat med 882E _ ej se värdet av det arbete som hittills lagts ned. *Def(AUST)5679* från -98 är under uppgradering. Ny version klar i september (kopia från Tony Cant). Liksom 882E är denna ej '*goal*-baserad' (nöjer sig ej med översiktliga mål/krav som t ex *882D*, *MS 00-56*). Bland nya begrepp: *Danger level* (hur pass mycket arbete som krävs för att bygga upp förtroendet).
(a2) Övriga nyheter: *Swalloms riskmatris* (med jordens undergång längst upp till vänster o 'origo' längst ned) möjliggör att alla system/vapenslag etc kan använda samma matris (underlättar bl a riskbedömningen vid integrering till system-av-system) o att lågkritiska (del)system endast behöver använda matrisens nederdel. Allvarlighetsgraden uttrycks kvantitativt (kostnad i en 10-potens/logaritmisk skala), vilket undanröjer problemet med tolkningar av konsekvens uttryckt i kvalitativa termer: ofta har t ex värsta klassen ('Katastrofal') fått stå för såväl förlust av människoliv/mindre UAV:er ($\$2*10^6$) som Nimitz-klassens hangarfartyg ($\$4{,}5*10^9$).
Unmanned Systems Safety Precepts, rev D: UAV-förutsättningar i form av skall-krav i preliminär utgåva för kommentarer.
(a3) Nästa års konferens: Baltimore 13/8-17/8 (http://www.system-safety.org), då bl a de svenska systemsäkerhetssatsningarna kommer att presenteras. Den som har synpunkter på vilka Programvarusäkerhetaktiviteter som bör tas upp kan kontakta *Ordf* (Inga-Lill).
b) Nästa gruppmöte*:* 06-10-03 kl 9:00-16.30 på WTC, Saab Corporate, Kungsbron 1, Plan 6, Sthlm. Anmälan till gruppmötet via mail till *Ingemar Johansson* senast fre 06-09-29 (cc till *Ordf*). Vi kommer att prova FTA på Ejection system. *Ordf* distribuerar nya faktablad inför mötet.
c) Hemläxa till dess: Leta efter exempel där FME(C)A visat sig effektiv i att identifiera felmod hos programvara.
d) OH:n visade under mötet finns som vanligt länkade till motsv dagordningspunkt (givet godkännande från författaren).
e) Tack för ett möte med överraskande slutsatser!

Aktivitetslista IG Programvarusäkerhet	**Nr**	**Klar till**	**Ansvarig**
Mötesnotiser senaste möte (#16)	17.1	06-09-10	Ordf
Bokning lokal nästa möte	17.2	06-09-10	P Nummert
Hemläxa: Ex där FMECA använts på renodlad programvara	17.3	06-10-02	Samtliga
Faktablad över FTA	17.4	06-10-02	Ordf
Uppdatering av hemsidans självstudiematerial	17.5	06-10-02	Ordf
Synpunkter på svenska SW Safety aktiviteter inför ISSC´07	17.6	06-10-02	Samtliga
Riskkällelista över HW	15.6	06-04-30	Strandberg
Transformera Event-tree-tabell till graf	15.7	06-04-30	Strandberg
Kontakta Redmill om HAZOP-Oh till hemsida	15.9	06-04-30	Ordf
Förteckn över innehåll i nödutrustning	15.11	06-04-30	I Johansson
Förslag till kompletteringar av faktablad	15.12	06-05-20	Alla
Studiematerial till hemsidan	14.5	06-03-31	Ordf
Förslag på typexempel för STPA/STAMP-analys	14.8	06-xx-xx	Alla
Kontakt med J Knight	14.9	06-xx-xx	Ordf
Sammanställn av inkomna MMI-enkätsvar	8.4	04-10-14	I Johansson + Ordf
Kontakt med Dekker (1:a den 31/8, förnyad i januari)	8.6	06-01-28	Ordf.
Inventering av företagets MMI-metodik (papper till Johansson)	6.3	05-03-31	Medl (se µprojektplan MMI-safety)

Avklarade punkter ligger som överstruken, dold text.