IG Programvarusäkerhet: Möte #15, 06-04-07. Antal mötesdeltagare: 5 (se aktuell medlemslista).

1. Inledning, Dagordning: Den inplanerade presentationen av JAS MMI har skjutits upp till påföljande möte.
2. μ-projektet SäkAnalysMetoder: a) Underlag: *Ordf*/*Koberstein* tog fram o sände ut följande material inför mötet*:* Systembeskrivning (RaketstolEnvelop), Faktablad (PHL, PHA, HAZOP, GenHzChecklist, GenSwHzList) samt Analysresultat (PHL_Eject) –det senare ett resultat av de kompletteringar som utförts i en mail-stafett efter feb-mötet.
b) Mailstafetten: En förbättring föreslogs: Den som står på tur att ta över och inte har tid att göra en insats i närzonen sänder till nästa person och uppger när stafettpinnen önskas åter. Detta för att inte arbetet skall stoppas upp i onödan.
c) PHL_Eject: En diskussionpunkt i samband med den aktuella PHL-analysen gällde **c1)** distinktionen ***riskkälla*** (*hazard*) – ***riskkälleorsak*** *(hz cause):* en riskkälleorsak skulle ju mycket väl kunna betraktas som en riskkälla i sig. Idealt utgår man vid start av PHL-analysen dock från riskkällor vid den yttersta systemgränsen (där bakomliggande faktorer från omgivning etc utgör s k ***bidragande orsaker*** till att en riskkälla aktiveras o startar en händelsekedja, som för systemet mot ett risktillstånd o slutligen olycka: *hz causes→hz→unsafe system state→accident*). Allt eftersom analysen fortskrider, flyttas fokus från det yttersta systemet in till underliggande system, för att identifiera riskkällor för vart och ett av dessa samt 'bidragande orsaker' utanför det nu aktuella systemet. Den ökade detaljeringen av systemet leder till en olyckskedja med ytterligare noder i en allt mer finförgrenad graf, där en tidigare identifierad riskkälla i stället kan utgöra en riskkälleorsak till nu aktuellt system. Vilken systemgräns man betraktar har m a o betydelse. I vårt studieexempel (Ejection system) har vi förenklat arbetet genom att förutsätta att tidigare riskkälleanalyser redan utförts på aktuell flygplanstyp, för att i studien kunna fortsätta med ett av dess delsystem. Oavsett beteckningar är det huvudsakliga för varje analysgrupp att till systemkonstruktörer/-mottagare klargöra hela olyckskedjan samt för varje riskkälla de typer av olycksutfall (effekt/skadegrad) som är möjliga.
c2) Ytterligare en diskussionspunkt var möjligheten/nyttan av att redan vid PHL-analys beakta –inte som traditionellt riskkällans '***värsta möjliga konsekvens***' (dvs allvarlighetsgrad)– utan snarare '***värsta troliga konsekvens'*** (en mindre allvarlig konsekvens kan vara så pass frekvent att den står för det högsta riskbidraget). Detta kräver värderingar av ***troligheten*** (*likelihood*) att en olycka inträffar ($\mathbf{P_{oly}}$), vilket omfattar flera sannolikhetsbegrepp: dels det troliga ($\mathbf{P_h}$) att en riskkälla föreligger/triggas, dels det troliga/rimliga ($\mathbf{P_e}$) att denna leder till olycksutfall av olika skadegrad. Vidare diskuterades möjligheten att kunna värdera dessa sannolikheter kvanti-/kvalitativt för riskkälla, där flera olycksutfall är möjliga. Huruvida P_e, P_h eller båda ($P_{oly}=P_e*P_h$) skall anges beror på omständigheterna: **i)** Mest kostnadseffektivt är att först skatta P_h. Lågt värde betyder att riskkällan är mindre sannolik, varför en ansträngning att dessutom försöka skatta P_e inte är det mest angelägna. Ett högt värde är en indikation på att konstruktionen behöver ändras (för att undvika riskkällan, minska P_h, t ex genom diversitet, eller på annat sätt motverka dess effekt). Först när denna möjlighet är uttömd bör tillägg i form av olika skyddssystem övervägas. För ett P_h-värde mellan dessa ytterligheter krävs dock en värdering även av P_e för att 'värsta troliga konsekvens' skall kunna identifieras. **ii)** Möjligheten att skatta P_e beror på underlagets detaljeringsgrad och torde vara svårt i ett tidigt analysskede (t ex vid PHL under konceptuell design) jämfört med PHA (eller snarare SSHA) på ett mer eller mindre färdigt system. Detta kan dock underlättas där tillförlitlig statistik finns att tillgå (som inom flyg), även om slutsatser ur statistiskt underlag inte alltid är tillämpliga på ny systemversion. **iii)** En helt annan sak är, att nyttja PHA för att budgetera ut den högsta risk olika ingående systemdelar får bidraga med (m h a den risktolerans som specats för systemet totalt, dvs systemets riskmatris). Har man lyckats skatta P_h kan i princip högsta tolerans för varje enskild P_e sättas, mot vilket utvärderingen av realiseringens verkliga riskbidrag sedan mäts. Jfr H ProgSäk: fotnot 244 + 6.1.4, Safeware: 9.4 samt referat av Eurocontrols guide (se länk från Dagordningen) varifrån f ö beteckningarna P_h resp P_e härrör.
I och med att vår riskkälleanalys nu börjat beakta med vilken sannolikhet/trolighet/rimlighet olika utfall kan inträffa, så har PHL-analysen övergått i en PHA. Resultatet av dagens analys införs efter mötet i filen PHA_Eject.
d) Faktabladen utgör ett starkt koncentrat och förutsätter viss kunskap i programvarutekniska detaljer (inte minst av realtidsanknutna aspekter). Några tillägg identifierades. Fler förslag till kompletteringar välkomnas av *Ordf* . Avsikten är att lägga ut materialet på SESAM:s hemsida, vilken är mer fristående från företagsspecifika o personliga hemsidor och därför mer robust mot organisatoriska/personella förändringar (med en högre grad av kontinuitet o åtkomlighet som följd).
e) IG-medlem som missat vara med vid de senaste analysproven: tag chansen att gå med nu. Det är inte för sent!
4. Övrigt: **a)** *Ordf* visade två klassiska ARP-guider för civilflyget (Aerospace Recommended Practice): SAE ARP 4761 med beskrivningar över olika säkanalysmetoder samt ARP 4754 med certifieringsaspekter.
a) ***Diskussionspunkter:*** F n inget behov av fler: Pågående mikroprojekt alstrar i sig tillräckligt med diskussionspunkter.
b) ***Fler typexempel?*** Nya typex för systemsäkerhetsanalys enl STPA/STAMP efterlystes (nuvarande typex ej lämpat). Lösa idéer: Friendly-fire, ATC, Trafikledningsoly i Schweiz, NBF, Myndighetshantering vid Tsunamin, Samverkan luftvärnssystem-flyg, Torped fr Hkp14, Skandinaviska luftrummet, Samverkan målmarkering. IG-medlemmarna uppmanas fundera vidare och komma med förslag.
c) ***Fler μ-projekt?*** Inga nya förslag: Tillräckligt med aktiviteter i nuvarande studieprojekt.
d) ***Framtida mötespunkt*****:** Ny lägesrapport om kommande flygstandarder (främst Do-178C) från Mikael Thorvaldsson.
e) ***Nästa gruppmöte:*** 06-05-23 kl 9:00-16.30 på WTC, Saab Corporate, Kungsbron 1, Plan 6, Sthlm med bl a Johan Holmberg om JAS MMI. Anmälan till gruppmötet via mail till *Ingemar Johansson* senast fre 06-05-19 (cc till *Ordf*). Inför detta tas fram: uppdaterade faktablad, analysresultat, studieunderlag anpassat för HAZOP (Kobersteins beskrivning över parameterutväxling mln fpl- o stolsprocessor).
f) ***Återigen, ett diskussionsrikt och givande möte!***

Aktivitetslista IG Programvarusäkerhet	**Nr**	**Klar till**	**Ansvarig**
Mötesnotiser senaste möte (#15)	15.1	06-04-18	Ordf
Bokning lokal nästa möte	15.2	06-04-18	P Nummert
Agenda för nästa möte	15.3	06-03-15	Ordf
Uppdatera studieunderlag (detaljer inför HAZOP)	15.4	06-05-09	Koberstein, Ordf
Kontakta Johan Holmberg, Saab ang nästa möte	15.5	06-04-30	Ordf
Riskkällelista över HW	15.6	06-04-30	Strandberg
Transformera Event-tree-tabell till graf	15.7	06-04-30	Strandberg
Referat från EUROCONTROLs FHA-kurs	15.8	06-04-18	Nummert
Kontakta Redmill om HAZOP-Oh till hemsida	15.9	06-04-30	Ordf
Uppdatera faktablad, PHL-resultat etc	15.10	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.