**Resumé över IG Programvarusäkerhets verksamhet under år 2006**

SESAM:s grupp i Programvarusäkerhet studerar frågeställningar aktuella för säkerhetskritiska programvarusystem. Arbetet är organiserat i olika teman (med ett eller flera mikroprojekt) samt ett antal diskussionsuppgifter – vart och ett med en utsedd inledare (’*coach*’), vilken lägger fram sin frågeställning samt stimulerar till vidare diskussioner och utredningar inom gruppen.
Idén med att definiera olika diskussionsuppgifter inom programvarusäkerhet har varit, att kunna ta upp problemområden, som deltagarna finner värdefulla att diskutera i en vidare krets, för att få dem belysta från olika synvinklar. Det kan t ex gälla fall, där det saknas lösningar, finns olika angrepps-sätt eller kanske motstridiga åsikter om lämpligt förfaringssätt.

Under 2004 studerades två teman: ’*Obemannade farkoster’* samt ’*MMI:er i säkerhetskritiska system*’ bl a genom att arrangera öppna seminarier med en mängd framträdande talare.
År 2005 ägnades i huvudsak åt det andra temat genom mikroprojektet ’**MMI-säkerhet**’, där grupp-medlemmarna gjorde en inventering inom det egna företaget av i vilken utsträckning designkriteri-er, utvecklingsprinciper och metodikstöd adresserar säkerhetskritiska MMI-scenarier. Ett flertal diskussionsuppgifter ventilerades även, bland dessa *’Hur mappa programvarans kritikalitet i systemets riskmatris*’ samt ’*Organisatoriska aspekter på Systemsäkerhet –Programvarusäkerhet– Programvaruut-veckling’*.

Under 2006 har några ytterligare MMI-inventeringar avrapporterats, bl a över land- & luftbaserade system samt från JAS MMI. Grupparbetet har därefter helt inriktats mot ett nytt mikroprojekt, ’**SäkAnalysMetoder**’. Syftet med detta har varit, att utreda vilka av de analysmetoder, som finns inom systemsäkerhetsområdet, som lämpar sig för programvarusystem samt under vilka analysfa-ser. De metoder, som hittills studerats, är HAZOP, FMECA, FTA. Aktuella analysfaser bland de, som definierats för olika skeden i systemutvecklingen, har varit PHL-analys, PHA, SHA, SSHA.
Ett stort arbete bestod i att ta fram underlag inför dessa prov. Som typexempel valdes ’Ejection System’, ett hypotetiskt system för utskjutning av raketstolar. En hel del automatik bakades in i systemet, för att kunna rikta in analyserna mot säkerhetskritiska programvaruaspekter. Ett antal faktablad har också sammanställts över olika analysfaser och analysmetoder samt över nyckelord och allmänna riskkällor _ däribland en unik lista över programvarans riskkällor. Underlag samt resultat från dessa analysmöten (bl a systemets riskkällelista kompletterad i successiva versioner) har sedan dokumenterats i mötesnotiser samt som självstudiematerial[1].
Nya diskussionspunkter uppstod under dessa analyser, t ex distinktionen riskkälla_riskkälleorsak (*hazard_hazard cause*), nyttan av en analys baserad på riskkällans ’värsta troliga konsekvens’ snarare än ’värsta möjliga’, begreppet *Success Tree* som komplement till *Fault Tree*.
Fem analysmöten har hittills hållits _ ibland kompletterad med en ’mailstafett’ bland deltagarna _ i ett försök att driva analysen vidare mellan mötena. Mikroprojektet kommer att fortsätta med fler metodprov. På väntelistan står bl a ETA, STPA/STAMP.

Gruppmötena har förutom dessa prov även ägnats åt nyheter från konferenser, kurser och arbets-gruppsmöten, ibland med någon inbjuden talare. Bl a har en redovisning erhållits över det senaste årets revisionsarbete med flygstandarden RTCA Do-178C (EUROCAE ED-12B) och frågan huruvida denna även skall inkludera nuvarande standarder för markbundna anläggningar (Do-248, Do-278). Likaså har erfarenheter från FTA på programvara i ett stort ledningssystem förmedlats.

Sammanfattningsvis kan konstateras att dessa möten _ trots tidsbrist och begränsade insatser _ varit både givande och stimulerande.

---

[1] Se t ex http://sesam.smart-lab.se: Arbetsgrupper: Programvarusäkerhet under **a)** Möten: Möte 14-18, **b)** Utbildning och Kurser: Självstudiematerial samt **c)** Teknik/Metodik: SESAM:s faktablad.