Resumé över IG Programvarusäkerhets verksamhet under år 2005

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 (och 'coach'), vilken lägger fram sin frågeställning och stimulerar till vidare diskussioner och utredningar inom gruppen.

Under 2004 studerades två teman: '*Obemannade farkoster'* samt '*MMI:er i säkerhetskritiska system*'. Arbetet kom att präglas av en utåtriktad seminarieverksamhet med en mängd framstående talare. Det gångna året har i huvudsak ägnats åt det andra temat genom det mikroprojekt, som definierats inom området 'MMI-säkerhet'. Åtta gruppmedlemmar har startat en inventering inom eget företag för att utreda i vilken utsträckning designkriterier, utvecklingsprinciper och metodikstöd adresserar säkerhetskritiska MMI-scenarier. Syftet är flerfaldigt, – dels att få fram vilka möjligheter som finns att redan under design kunna 'visualisera' den dynamiska sekvens av bild, text, ljud och annan information som förmedlas till operatör (t ex reglagerörelser) och därmed kunna utföra olika typer av systemsäkerhetsanalyser på denna typ av informationsflöden, – dels att stimulera till dokumentation av den kunskap på individnivå som finns hos företagens MMI-designers och -utvecklare. Önskvärt är också att identifiera återanvändbara, allmängiltiga mönster (patterns) för olika lösningsstrategier, att kartlägga interna och företagsövergripande nätverk för HMI/ MMI/ HSI etc. En av gruppmedlemmarna har dessutom startat mikroprojektet '*Jämförelse av verktyg för automatisk kodgenerering mot säkerhetskritiska system*', vilket drivs i samarbete med annan SESAM-medlem.

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 angreppssätt eller kanske motstridiga åsikter om lämpligt förfaringssätt.

Under 2005 har ett par nya diskussionsuppgifter ventilerats. Ett av dessa gällde *'Hur mappa programvarans kritikalitet i systemets riskmatris*'. Frågeställningarna gällde vilka angreppssätt, som är att föredra: Mappning av programvaran på 2-dim matris (konsekvens + sannolikhet), på 1-dim (t ex enbart konsekvens)? Kan viss funktionalitet realiseras m h a flera av lägre kritikalitet (enl 00-56 utg. 2 tabell 8)? Kan programvarans bidrag till olyckssannolikhet kvantifieras? Under de diskussioner som följt har bl a framgått fördelar med en 'origo'-orienterad riskmatris, vad mappning på 1-dim innebär, vilka standarder som använder sig av en 1-dim matris, när det är fördelaktigt med ett 3-dimensionellt betraktelsesätt. Likaså: vilka tekniker som finns för att få till stånd en lägre kritikalitetsgradering av programvaran och därmed möjlighet att (om behov föreligger) kunna ta fram siffermässiga skattningar på programvarans bidrag till olyckssannolikheten.

Ytterligare en diskussionspunkt gällde '*Organisatoriska aspekter på Systemsäkerhet –Programvarusäkerhet - Programvaruutveckling'*. Aktuella frågeställningar här har bl a varit: Hur få systemsäkerheten integrerad med programvaruutvecklingen?, Vilket samspel skall råda mellan de delvis konflikterande rollerna: utvecklaren, som skall bygga in safety-egenskaper i systemet samt den oberoende safety-ingenjören, som skall kontrollera att säkerheten tillgodosetts i framtaget system? Ur dessa diskussioner har bl a framkommit förslag att låta en projektoberoende grupp behandla generella safety-aspekter giltiga för samtliga projekt inom visst applikationsdomän (kravbild, riskkällor osv) i stället för spritt och isolerat i skilda, projektspecifika grupper.

Nya studieområden kommer att tas upp. Ett förslag inför nästa år är säkerhetskritiska infokällor/-centraler, ett område av betydelse för klassen lednings- och insatssystem. Det handlar om säkerhetskritiska system, som vilar på data vars relevans kan vara avgörande för systemsäkerhe-

ten – data som ofta tas fram vid sidan om koden och därför inte utsätts för analys stöttade av verktyg i samma utsträckning som kod. En viss forskning bedrivs inom området, bl a för formell dataspecificering (med informell tolkning för ökad förståelse), vilket öppnar för formell verifiering. Här skulle det vara intressant att ordna en seminariedag med några av de personer verksamma inom detta problemområde.