Verksamhet inom SESAMs Programvarusäkerhetsgrupp 2002-2009

SESAM är ett samverkansnätverk för projektövergripande, företagsneutral kunskapsuppbyggnad och kunskapsspridning inom området programvaruintensiva försvarssystem. Uppgiften att samla, skapa samt sprida information och kunskap sker huvudsakligen i arbetsgrupper, som verkar inom avgränsade tekniska områden och som efter behov inrättas och avvecklas.

SESAM styrs av ett Råd med representanter för gruppens medlemmar. Rådet har till sin hjälp ett Verkställande Utskott (VU) samt ett Sekretariat.

Detta dokument är en sammanställning av de verksamhetsbeskrivningar för SESAMs Programvarusäkerhetsgrupp, vilka publicerats på hemsidan http://sesam.smart-lab.se under gruppens första ordförandeskap, perioden oktober 2002 – augusti 2009.

1. Sammanfattning

Kännetecknande för verksamheten inom programvarusäkerhetsgruppen har varit erfarenhetsutbyte genom mikroprojekt / teknikprov samt diskussioner och info-utbyte under seminarier och möten, där gemensamma frågeställningar formuleras och fördelas mellan olika deltagare. Resultat och upplägg från den, som tidigt kommit igång med sitt projekt /prov utnyttjas för ett snabbare genomförande hos de, som startar senare. Därigenom undviks dubbelarbete och lämpliga kompletteringar kan identifieras. Genom SESAM – en kunskapsbefrämjande, icke-vinstdrivande organisation – underlättas möjligheten att kostnadsfritt få tillgång till verktyg för utvärderingar. Ett exempel på detta är SpecTRM. Under 2003 valde några företag att via examensarbetare prova verktyget. En bonuseffekt av detta blev ett ökat utbyte mellan deltagande industrier och högskolor.
’MMI:er i säkerhetskritiska system’ var ett stående tema under 2004-2006. Inom ramen för mikroprojektet ’MMI-säkerhet’ arrangerades seminarier i temat, och en kartläggning av det egna företagets analystekniker, designprinciper och hjälpmedel för konstruktion av människa-system-interaktion utfördes.
Ett annat tema som studerades under året var programvara i obemannade farkoster.
Åren 2006-2008 drevs mikroprojektet ’SäkAnalysMetoder’ för prov av olika analystekniker på programvara. Projektet avslutades med studium av den senaste tekniken, STAMP/STPA samt inbjudan till prof. Leveson att under sina kursdagar belysa tekniken på de tillämpningsexempel gruppen använts sig av.
Resultaten av dessa analysprov finns lagrade som självstudiematerial på hemsidan under http://sesam.smart-lab.se : IG Programvarusäkerhet: Utbildning och kurser: Självstudiematerial: Systemsäkerhetsanalysmetoder.
De faktablad som tagits fram inom detta projekt återfinns på http://sesam.smart-lab.se : IG Programvarusäkerhet: Teknik/Metodik: SESAM faktablad.
Under 2008-2009 och som avslutning på första ordförandeperioden sammanställdes ’Frågor-och-svar-om-Programvarusäkerhet’, vilka därefter gjordes tillgängliga på hemsidan tillsammans med en nyinspelad videokurs inom ämnesområdet.

1.1. Översikt över möten och seminarier

Mötesform	***Datum***	***Tema/Mikroprojekt/Disk-uppg***	***Kommentarer***
Möte 1	02-10-24	• OS i säkerhetskritiska tillämpningar	3 externa talare.
Möte 2 + Sem 1	03-02-04	• Teknikprov inom FoTA P12 • Systemsäkerhetsanalys i olika företag	9 talare varav 2 externa.
Seminarium 2	03-03-26--27	• Safeware:s SpecTRM-verktyg	2 Leveson-doktorander
Möte 3	03-05-07	• SpecTRM-prov, • Design by contract, • Återanvändning o interoperabilitet	Enbart interna talare
Sem 3 (Leveson)	03-08-20--21	• System Safety for Sw-Intensive Systems	Öppet (även för icke-medlemmar)
Möte 4 + Sem 4	03-09-18	• Tidsstyrd programmering/nätverk	5 externa talare.
Möte 5 + Sem 5 (höstsem)	03-10-21--22	• Arbetsgruppsredovisningar • Informationssäkerhet i en NBF-miljö	Gruppmöte+SESAMgruppredovisn Öppet SESAM-seminarium.
Möte 6 + Sem 6	04-02-11	• Programvara i obemannade farkoster	6 externa talare.
Möte 7 + Sem 7	04-06-08	• Människa-System-Interaktion i säkerhetskritiska situationer	Gruppmöte + 7 externa. Öppet SESAM-seminarium
Möte 8 + Sem 8	04-09-21	• Säkerhetskritisk MSI (forts på föreg sem)	Gruppmöte + 4 externa Öppet SESAM-seminarium
Möte 9	04-10-21	• Ag-redovisningar: Programvarutekniska aspekter på s-k MMI:er, företagsenkäter	Gruppmöte+SESAMgruppredovisn
Möte 10	05-02-01	• Planering av 2005-års verksamhet	Gruppmöte+SESAMstartmöte
Möte 11	05-04-27	• MMI-säkerhet, • Kritikalitets- & säkerhetsbegrepp, • Kommande flygstder	Gruppmöte (inbjuden talare)
Möte 12	05-09-01	• MMI-säkerhet, • Riskmatris f pgmvara	Gruppmöte
Möte 13	05-10-19	• MMI-säkerhet, • Org-aspekter system- och pgmvarusäkerhet	Gruppmöte+SESAMgruppredovisn
Möte 14	06-02-14	• MMI-säkerhet, • SäkAnalysMetoder: PHL	Gruppmöte
Möte 15	06-04-07	• PHA-analys, • FHA (EUROCONTROL)	Gruppmöte
Möte 16	06-05-23	• HAZOP-prov, • Gripen MMI-säkerhet	Gruppmöte (inbjuden talare)
Möte 17	06-08-22	• FMECA-prov, • Flygstandarder	Gruppmöte (inbjuden talare)
Möte 18	06-10-03	• FTA-prov	Gruppmöte
Möte 19	06-12-07	• FTA på programvara, Erf från stort lednsyst	Gruppmöte (inbjuden talare)
Möte 20	07-01-25	• Vad kan vi lära oss av spelindustrin? • Gruppredovisning 'SäkAnalysMetoder'	Öppet SESAM-seminarium SESAMgruppredovisning
Möte 21	07-10-12	• STPA-prov på Adaptive Cruise Control	Gruppmöte
SESAMmöte	07-11-07	• Gruppredovisning 'STPA/STAMP'	SESAMredovisning
Möte 22	08-02-14	• STAMP-prov på kollisionen över Überlingen	Gruppmöte
Möte 23	08-05-13	• STAMP-prov Überlingen-olyckan (forts).	Gruppmöte
Sem 9 (Leveson)	08-05-21--22	• System Safety in Sw-Intensive Systems	Öppet SESAM-seminarium.
Möte 24	08-11-19	• FAQ (Frequently Asked Questions)	Gruppmöte
Möte 25	09-04-02	• FAQ, • Hemsida, • Framtida ledning	Gruppmöte + SESAM VU- representant
Möte 26	09-06-08	• FAQ, • GEIA-STD-0010, • Framtidsplaner	Gruppmöte

2. Programvarusäkerhetsaktiviteter under år 2002

Våren 2002 beslutade SESAMs rådsmöte att inrätta en ny intressegrupp med inriktning mot området Programvarusäkerhet (*Software Safety*). Ett upprop sändes ut och gruppen startade med ett första möte den 24 oktober 2002 i samband med SESAMs seminarie- och arbetsgruppsdagar.

Mötets tema var ’OS i säkerhetskritiska tillämpningar’. Tre inbjudna talare delade med sig av sina erfarenheter från systemsäkerhetscertifiering av operativsystem, nedskalning av Windows NT för inbyggda applikationer samt användning av Windows operativsystem i projekt med krav på systemsäkerhet.

Under mötet drogs riktlinjerna för den fortsatta verksamheten upp och framtida delområden identifierades. Högst på listan placerades Operativsystem följt av Metoder, Verktyg, Återanvändning, Arkitekturer, Design, Utbildning samt Verifiering & Validering.
Till tema för nästföljande möten valdes ’Provning av verktyg för systemsäkerhetsanalys av programvara’. Beslut fattades att undersöka möjligheterna att kostnadsfritt få prova ett nytt metodhjälpmedel, SpecTRM – ett passande mikroprojekt för valt tema.

Formerna för gruppens fortsatta arbete fastlades. Som modell för verksamheten föreslogs det under 2002 avslutade projektet FoTA P12, ’Överföring till industrin av programvaruteknik för säkerhetskritiska system. Härifrån kom f ö många av gruppens första medlemmar. Till ordförande valdes Inga-Lill Bratteby-Ribbing, FMV, som därefter lett verksamheten fram till den 1 september 2009. Ny ordförande från detta datum är Björn Koberstein, FMV.

2.1. Inriktning

Gruppens inriktning är programvarusäkerhet, dvs programvarans roll för systemsäkerheten – ett område av speciell betydelse för säkerhetskritiska programvarutillämpningar, där risk finns att systemet kan orsaka skada på person, egendom eller miljö.
Programvarusäkerhet är därför inte enbart en sammanfattande benämning för de egenskaper som programvarukomponenter i ett säkerhetskritiskt system bör inneha, utan betecknar även den disciplin, som berör användare, beställare och leverantörer samt de programvaruprocesser och verktyg dessa använder sig av för utveckling, underhåll och drift av sådant system.

2.2. Målsättning

Till målsättningarna med gruppens verksamhet hör att

- belysa och diskutera frågeställningar av betydelse för programvarusäkerheten (t ex delområde arkitektur, design, återanvändning, operativsystem/runtime-kärnor, V&V, underhåll).
- ta del av den verksamhet inom övriga arbetsgrupper som berör programvarusäkerhet.
- bjuda in utomstående med speciell erfarenhet inom visst delområde att medverka vid möten och seminarier.
- prova/demonstrera lämpliga verktyg för analys av programvara m a p systemsäkerhet.
- sprida information om programvarusäkerhet (metoder, verktyg, utbildning, litteratur) t ex genom att
  – göra informationen tillgänglig via SESAMs hemsida, http://sesam.smart-lab.se,
  – genomföra utbildning betr. detaljaspekter inom programvarusäkerhet

2.3. Mötesformer

Ett heldagsmöte per kvartal hålles på FMV i Stockholm eller hos något av de deltagande företagen. Detta lämnar utrymme för övriga insatser med 6 dagar per deltagare och år.

2.4. Medlemskap

Intressegruppen är avsedd för personer från företag och organisationer med medlemskap i SESAM, vilka aktivt kan bidra till gruppens verksamhet. En medlemslista hålls tillgänglig för gruppmedlemmarna.

3. Programvarusäkerhetsgruppen år 2003 –september 2009

En strukturering av arbetsformerna för de studier som genomfördes och de frågeställningar som aktualiserades kom att vidareutvecklas under dessa år.

Arbetet organiserades 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 var, att kunna ta upp problemområden, som deltagarna finner värdefulla att diskutera i en vidare krets och p s s kunna belysa dessa från nya synvinklar. Det kan t ex gälla fall, där inga lösningar tycks föreligga, där det finns olika angreppssätt eller motstridiga uppfattningar om lämpligt förfaringssätt.

Uppbyggnaden av en hemsida för Programvarusäkerhet inleddes (http://sesam.smart-lab.se: ’IG Programvarusäkerhet’), vilken fortlöpande har byggts på och uppdaterats. Transparens och spårbarhet har eftersträvats, genom att där samla allt material från gruppens verksamhet samt övrig information av betydelse för programvarusäkerhetsområdet. I och med SESAMs företagsneutrala och personoberoende inriktning blir detta en värdefull tillgång, som kan stå emot organisations- och personalförändringar, något som är oundvikligt och kännetecknande för varje dynamisk verksamhet.

3.1. År 2003

Vid det första Programvarusäkerhetsmötet hösten 2002 hade temat för nästkommande möten fastlagts: ’Provning av verktyg för systemsäkerhetsanalys av programvara’. Detta kom att bli styrande för de totalt 8 heldagsaktiviteter som genomfördes under 2003.

Gruppverksamheten hade som modell det under 2002 avslutade projektet FoTA P12, ’Överföring till industrin av programvaruteknik för säkerhetskritiska system. De teknikprov som där utförts avrapporterades därför under 2003 års första möte i februari. Deltagarna redovisade då även sina erfarenheter av medlemsföretagens systemsäkerhetsmetoder och -verktyg.

Som del av årets tema fanns idén att starta ett mikroprojekt för prov av SpecTRM, ett verktyg, utvecklat av prof Nancy G Leveson, för stöd vid modellering och uppbyggnad av säkerhetskritiska system. Detta understödjer bl a avsiktsspecificeringar, spårbara motiveringar och beskrivningar av systemmålsättningar samt dokumentation av designbeslut, riskkällor, systemsäkerhetsrestriktioner.

Beslut hade tagits föregående möte, att undersöka möjligheterna till kostnadsfria prov. Två av Levesons doktorander bjöds därför in i mars. Dessa genomförde en tvådagars presentation av verktyget och dess tillämpning inom ett NASA-finansierat forskningsprojekt (konstruktion av återanvändbara rymdmodeller) samt en avslutande demo. Bland åhörarna ingick gruppmedlemmar, några kollegor, samt de exjobbare som engagerats för provning och utvärdering inom mikroprojektet från högskolor i Linköping och Växjö.

Ytterligare ett tillfälle till introduktion i SpecTRM arrangerades i augusti som del av en tvådagarskurs i ’System Safety for Software-Intensive Systems’, ett seminarium öppet även för icke SESAM-medlemmar. Denna gång var det prof Leveson som lockats över – en karismatisk talare, som fängslade drygt 120 personer. Även deltagare utanför försvarssektorn ingick och många återkom senare med förfrågan om att ordna fler, liknande Leveson-evenemang (det skulle dock dröja 5 år).

Vid höstens möten ventilerades och avrapporterades de teoretiska och praktiska erfarenheter som exjobbare och gruppmedlemmar gjort – ett givande utbyte för båda parter. Att SESAM kan spela en viktig roll i bryggan mellan industri-myndighet-universitet visades här. Sex år senare – efter utträde i arbetslivet – sökte f ö en av dessa exjobbare medlemskap i gruppen Programvarusäkerhet.

Ytterligare teman under hösten var ’Tidsstyrd programmering’, och ett _-dagsprogram arrangerades inom gruppmötets ramar med talare från universitet (KTH, CTH) och industri (Arcticus, Volvo CE). En uppföljare till gruppens allra första möte 2002 blev några presentationer under titeln ’Kommersiella operativsystem i säkerhetskritiska system’ med två externa talare – denna gång presenterat i en vidare SESAM-krets.

Till de diskussionspunkter som avhandlades under årets gruppmöten hörde: B Myers teknik ’Design by Contract’: ett sätt att m h a invarianter, constraints samt pre-/postconditions specificera – för att efteråt kontrollera – vad ett system ej får göra. ’Riskinformation integrerad i företags kravdatabaser’ samt ’Återanvändning och interoperabilitet mellan konceptuella modeller för simulering’ är ytterligare några exempel.

Bland de nyheter på verktygsfronten som presenterades för gruppen var: NRLs SCR (Software Cost Reduction), en uppsättning verktyg, som bl a möjliggör specning i en tabellorienterad notation (jfr SpecTRMs logiska and-or-tabeller). En första presentation av Leveson-hjälpmedlet STAMP, en systemövergripande säkerhetsanalys baserad på styrflöden, gjordes också. Fyra år senare skulle gruppen visa sig redo för prov av detta.

3.2. År 2004

Aktiviteterna under 2004 kom att präglas av en utåtriktad seminarieverksamhet med deltagande från en mängd framstående talare. Två teman från motsatta klasser av tillämpningar med vitt skilda systemsäkerhetsaspekter behandlades: ’Obemannade farkoster’ samt ’MMI:er i säkerhetskritiska system’. Båda är högaktuella och innebär integration mellan flera olika discipliner.

Det första temat tillhör klassen autonoma system, dvs säkerhetskritiska system utan mänsklig interaktion. I samband med gruppmötet i februari hölls ett eftermiddagsseminarium på temat ”Programvara i obemannade farkoster”, där inbjudna talare från industri, myndigheter och universitet gav exempel på säkerhetskritiska aspekter i flygande, markbundna samt över- och undervattensbaserade farkoster. Här redogjordes också för en teknik att hårdvarumässigt samt i en och samma CPU kunna partitionera säkerhetskritiska delar från icke säkerhetskritiska. Partitionering, dvs möjligheten att logiskt eller fysiskt kunna separera delar av olika kritikalitet, har betydelse både för att kunna hålla nere kostnaderna vid utveckling och underhåll av säkerhetskritiska system samt för att uppnå ökad systemsäkerhet. I och med separeringen behöver inte hela systemet betraktas som säkerhetskritiskt av dess högsta grad. Tidigare separeringstekniker handlade till stora delar om fysisk separering, där man lade kritiska processer i separata CPUn, vilket vikts- och volymsmässigt (samt då det föreligger dynamiska samband mellan fysiskt separerade delar) har vissa nackdelar. Mer moderna och mjukvaruinriktade ansatser bygger i stället på logisk separering av tid och minne, vilken medger, att delar av olika kritikalitet kan ligga på samma CPU. Logisk separering kan realiseras genom RTOS/RTK som kan bevaka att en icke säkerhetskritisk /lågkritisk process förhindras stjäla resurser från process av högre kritikalitet. Exempel är t ex Lynuxworks LynxOS-178, Green Hills INTEGRITY-178B, Windrivers VxWorks AE 653 (♦ Safety-Critical ARINC 653) samt Aonix SmartKernel.

Den andra klassen av tillämpningsområden som studerades var – i motsatts till den första – säkerhetskritiska interaktioner mellan människa och system. Detta visade sig vara så intressant att två seminarietillfällen ordnades, även här med experter från myndigheter, industri, högskolor med erfarenheter från kontrollrum, ledningscentraler, cockpit, fordonshytter och fartygsbryggor.

Till de frågeställningar, som gruppen önskade belysta hörde bl a i vilken utsträckning det finns lämpliga metoder att i förväg systemsäkerhetsmässigt analysera en designlösning m a p det dynamiska flödet av text-ljud-bild som presenteras för en operatör i kritiska situationer. Att detta har aktualitet illustrerades samma vecka av vetenskapsradions rapport om nya forskningsrön beträffande behovet av dynamik i skärmbildslayouten – vanligtvis har presenterad information (åtminstone inom civilflyg) varit alltför statiskt orienterad.

Ett litet exempel på betydelsen av kunskap om människans kognitiva kapacitet inför design av säkerhetskritiska MMI-system förmedlades under dessa seminarier. Bandbredden när det gäller förmågan att ta in och hantera information i medvetandet är här ca 40 bits/sek, medan ett omedvetet, ryggmärgskodat beteende kan klara ca 11 Mbits/sek. Detta visar också vikten av att träna operatörer i olika säkerhets- och tidskritiska scenarier. Har man å andra sidan väl

fått in ett omedvetet reaktionsmönster, krävs det en enorm energi både att lära in ny information och radera tidigare – rester finns ofta kvar, vilka kan medföra en tendens under stress att återgå till tidigare inlärt beteende. Att ändra och förbättra en välbekant design eller layout kan m a o vara vanskligt och måste i extremfall kanske uppskjutas tills en ny generation operatörer står till förfogande.

Inför de två sista av dessa seminarier fick gruppmedlemmarna en hemuppgift: att på det egna företaget kartlägga vilka designprinciper, analyser, hjälpmedel som används för konstruktion av interaktioner mellan människa och system. Som utgångspunkt togs en frågelista fram. En redogörelse för vilka resultat gruppen kommit fram till gavs på SESAM-dagen den 21/10. Avsikten var att slutföra arbetet senare under hösten, för att de som inte hunnit påbörja sin företagsinventering, skall hinna med. Målsättningen var att avsluta temat med att sammanställa de ev. slutsatser som kan dras ur de utredningar, gruppdiskussioner och seminarier som genomförts, för att p s s få fram rekommendationer beträffande framtida åtgärder och inriktningar.

3.3. År 2005

År 2005 ägnades i huvudsak åt det andra temat, ’MMIer i säkerhetskritiska system’, genom mikroprojektet ’MMI-säkerhet’: Åtta gruppmedlemmar startade en inventering inom eget företag för att utreda i vilken utsträckning designkriterier, utvecklingsprinciper och metodikstöd adresserar säkerhetskritiska MMI-scenarier. Syftet var flerfaldigt.
Ett var, att få reda på vilka möjligheter som finns att redan under design kunna ’visualisera’ den dynamiska sekvens av bild, text, ljud och annan information (t ex reglagerörelser) som förmedlas till operatör. Med vetskap om detta skulle lämpliga systemsäkerhetsanalyser på dessa typer av informationsflöden eventuellt kunna identifieras.
Ett annat syfte var, att stimulera till dokumentation av den kunskap på individnivå som finns hos företagens MMI-designers och -utvecklare.
Ytterligare en målsättning var, att identifiera återanvändbara, allmängiltiga mönster (*patterns*) för olika lösningsstrategier samt att kartlägga interna och företagsövergripande nätverk för HMI/ MMI/ HSI etc.
Utöver detta startade en av gruppmedlemmarna (i samarbete med annan SESAM-medlem) mikroprojektet ’Jämförelse av verktyg för automatisk kodgenerering mot säkerhetskritiska system’.

Tanken med att definiera olika diskussionsuppgifter inom programvarusäkerhet hade varit att ta upp problemområden, som deltagarna finner värdefulla att diskutera i en vidare krets. Under 2005 ventilerades ett par nya diskussionsuppgifter.
Ett av dessa gällde ’Hur mappa programvarans kritikalitet i systemets riskmatris’. Frågeställningarna gällde vilka angreppssätt, som är att föredra: Mappning av programvaran på en 2-dimensionell matris (konsekvens + sannolikhet), på en 1-dimensionell (t ex enbart konsekvens)?
Kan viss funktionalitet realiseras m h a flera av lägre kritikaliteter (enl 00-56 utg. 2 tabell 8)?
Kan programvarans bidrag till olyckssannolikhet kvantifieras?
Under de diskussioner som följde framgick bl a fördelarna med en ’origo’-orienterad risk-matris (vilket skiljer från den klassiska riskmatrisuppställningen). Detta betraktelsesätt

anammades senare av flera standarder, bl a ITAAs GEIA-STD-0010, vilken f ö kom att studeras i ett mikroprojekt 4 år senare (se avsnitt 3.7).
Vidare utreddes vad mappning av riskbegreppet på en dimension innebär, vilka standarder som använder sig av en 1-dimensionell matris, i vilka fall det kan vara fördelaktigt med ett 3-dimensionellt betraktelsesätt. Likaså: vilka tekniker finns för att kunna ta ned kravet på programvaran till en lägre kritikalitetsnivå för att därmed (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 var bl a:
Hur få systemsäkerheten integrerad med programvaruutvecklingen?,
Vilket samspel skall råda mellan de till synes konfronterande uppgifterna hos utvecklaren, som skall bygga in systemsäkerhetsegenskaper i systemet och den oberoende säkerhetsingenjören, som skall kontrollera att säkerheten tillgodosetts i framtaget system?
Dessa diskussioner ledde bl a till förslaget att låta en projektoberoende grupp behandla generella säkerhetsaspekter (kravbild, riskkällor osv) giltiga för samtliga projekt inom en viss applikationsdomän, i stället för att hantera dessa frågor spritt och isolerat i skilda, projektspecifika grupper.

Till de nya studieområden som föreslogs inför 2006 hörde säkerhetskritiska info-källor/ -centraler, ett område av betydelse för klassen lednings- och insatssystem. I detta fall är det frågan om säkerhetskritiska system, vilka vilar på data vars relevans kan vara avgörande för systemsäkerheten – data som ofta tas fram vid sidan om koden och därför inte i samma grad som kod utsätts för (verktygsstöttade) analyser.
Virginiauniversitetet och NASA hör till dem som bedrev viss forskning inom området, bl a för formell dataspecificering (med informell tolkning för att uppnå ökad förståelse), vilket öppnar för formell verifiering. Här fann SESAMgruppen det intressant att bjuda in några personer med såväl praktisk som teoretisk erfarenhet till en seminariedag kommande vår. Senare, under 2006, visade det sig dock, att den ovan refererade forskningen fått en reviderad inriktning, varför de hjälpmedel, som varit under utarbetade, nu var föremål för omdesign. Även om några resultat ännu (i augusti 2009) inte kunnat återfinnas från denna forskningsgrupp, är ämnesområdet fortfarande angeläget och intressant.

3.4. År 2006

Under 2006 fortsatte mikroprojektet ’MMI-säkerhet’. Ytterligare några MMI-inventeringar avrapporterades, bl a över land- och luftbaserade system samt från JAS MMI.

Grupparbetet inriktades därefter mot ett nytt mikroprojekt, ’SäkAnalysMetoder’.
Syftet med detta var, att utreda vilka av de analysmetoder, som finns inom systemsäkerhetsområdet, som lämpar sig för programvarusystem samt under vilka analysfaser. Under 6 analysmöten provades de klassiska metoderna HAZOP, FMECA, FTA under analysfaserna 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 sammanställdes 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) dokumenterades därefter 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*.

I försök att driva analysen vidare mellan mötena kompletterades de sex analysmötena med en ’*mail*stafett’ bland gruppmedlemmarna. Tiden räckte trots detta inte till, varför nya metodprov fick ställas på väntelistan (bl a av ETA samt STPA/STAMP) och årets mikroprojekt förlängas till påföljande år.

Gruppmötena ägnades även åt nyheter från konferenser, kurser och internationella arbetsgrupper, ibland med någon inbjuden talare. Bl a lämnades en redovisning 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 förmedlades erfarenheter från FTA på programvara i ett stort ledningssystem.

Trots tidsbrist och begränsade insatser visade sig dessa mötesaktiviteter bli både givande och stimulerande.

3.5. År 2007

Under 2007 genomfördes (p g a hälsoproblem) hälften så många möten: två SESAM-redovisningar och ett gruppmöte, där provningen inriktades mot en ny analysmetod: STAMP/STPA. Inför varje nytt prov sammanställdes ett underlag, som distribuerades ut till medlemmarna före analysmötet. Detta utgjordes bl a av komprimerade faktablad, mallar till metoden samt beskrivningar av det tillämpningsexempel metoden skulle provas på.

Den första STAMP/STPA-analysen tillämpades på ett adaptivt farthållningssystem.
Gruppen fann, att detta exempel inte helt kunde lyfta fram metodens styrkor och särdrag: bl a finns flera varianter av metoden, som inte passade att testa på detta tillämpningsexempel. Det beslutades därför, att provningen skulle fortsätta vid ett senare möte, denna gång på ett annat tillämpningsfall. Underlag till detta togs fram, men p g a svårigheter att finna passande datum, sköts detta prov upp till februari 2008. Det tillämpningsexempel, som valdes blev flygolyckan över Überlingen i juli 2002.

[1] Se t ex http://sesam.smart-lab.se: IG Programvarusäkerhet under **a)** Möten: Möte 14-23, **b)** Utbildning och Kurser: Självstudiematerial samt **c)** Teknik/Metodik: SESAM:s faktablad.

En hel del arbete kom på detta sätt att investerats i framtagning av underlag inför analyserna. Detta bidrog till att det – trots begränsade insatser under själva analysmötet – gick att få en relativt god bild av provad teknik samt att kunna dra vissa slutsatser angående dess användbarhet på programvarusystem. Detta blev i sin tur sporren till att lägga ned ytterligare tid på att sammanställa slutsatser och analysresultat. På SESAMs hemsida finns dessa utlagda, både i form av mötesanteckningar samt som självstudiematerial. Därigenom kunde även de, som inte kunnat närvara vid proven, ta del av dragna erfarenheter.

Gruppmötena ägnades i vanlig ordning även åt nyheter från konferenser, kurser och andra redovisningar. Dessutom förbereddes, inför bl a SESAMs 20-årsjubileum år 2008, två seminariedagar den 21-22 maj med prof. Nancy Leveson – den person, som på 80-talet byggde upp området Programvarusäkerhet. Inför detta tillfälle ombads Leveson att bland sina tillämpningsexempel ta med flygolyckan över Überlingen, något som gruppmedlemmarna vid det laget skulle vara väl förtrogna med.

3.6. År 2008

Uppgiften inom mikroprojektet 'SäkAnalysMetoder', som startade redan 2006, var att studera vilka analysmetoder inom systemsäkerhetsområdet, som lämpar sig för programvarusystem under olika analysfaser. Efter prov av de klassiska metoderna HAZOP, FMECA, FTA fortsatte provningarna under 2007 med den relativt nya analysmetoden, STAMP/STPA. Denna inriktar sig mot riskkällor förknippade med de olika typer av styr- och regleringsmekanismer, som förekommer såväl på programvarunivå i tekniska realtidssystem (m h a givare/ställdon) som på organisatorisk/personell nivå (med styrning i form av reglementen/ordergivning och återmatning via bekräftelser). Som tillämpningsexempel valdes ett adaptivt farthållningssystem, vilket analyserades m h a den proaktiva varianten STPA (en riskskälleanalysmetod baserad på STAMP).

Under 2008 övergick provningarna till basvarianten STAMP (en haveriutredningsmetod, *root cause analysis*). Som tillämpning valdes ett fall med omfattande dokumentation på nätet: flygolyckan över Überlingen juli 2002. Väl kända tillämpningsexempel och noggrant förberedda analyssessioner hör till förutsättningarna för att deltagarna på en dag skall hinna sätta sig in i både analysmetod och applikation samt utföra själva analysen. Inför gruppanalyserna komprimerades därför tillgängligt material och grafer togs fram över analysobjektets statiska och dynamiska styrstrukturer samt över dess dynamiska förändringsprocesser. Detta fick – tillsammans med faktablad över metoden – bilda underlag till kommande STAMP-analyser. Dessa visade sig kräva minst två möten. Underlag, analysresultat och slutsatser dokumenterades i mötesnotiser och sammanfattades i ett självstudiematerial[1].

Som del i detta mikroprojekt inbjöds prof Nancy G Leveson, upphovsman till STAMP/STPA, att hålla en 2-dagars kurs i systemsäkerhet för programvaruintensiva system. Detta blev en mycket välbesökt och uppskattad tillställning. Seminariet var öppet även för icke SESAMmedlemmar och ca 100 personer deltog. Första dagen ägnades åt STAMP. Leveson, som blivit ombedd att inkludera Überlingen-olyckan bland sina fallbeskrivningar, illustrerade

elegant hur de olika graftyperna som ingår i STAMP kan användas för att påvisa defekter i interaktionsflödena mellan flygledningscentral och cockpit samt inom dessa: ett mycket givande komplement till och avslut av såväl STAMP-prov som mikroprojekt!

Årets sista gruppmöte ägnades åt diskussioner om framtida ledarskap och verksamhetsinriktning samt till att lägga upp riktlinjerna för nästföljande år. Ett nytt mikroprojekt definierades: 'FAQ', en Frågor&Svar-svit avsedd att läggas ut på hemsidan. Underlag fanns redan i de frågeställningar, som utretts via diskussionsuppgifter och mikroprojekt samt i ordförandens introduktionspapper, kurser och rådgivningsverksamhet. En inledande uppgift inför 2009 blev därför, att komplettera med nya frågor/svar (egna och andras) samt att sända runt dessa inom gruppen före nästa möte – ett sätt att ge även den, som har svårt frigöra tid för möten, möjlighet att bidra till sviten.

Ett innehållsrikt år med ett program omfattande totalt 5 träffar var därmed till ända.

3.7. Första halvåret 2009

Första halvan av 2009 ägnades åt huvudtemat för Programvarusäkerhetsgruppen: kompetensutveckling och informationsspridning – ett tema, som f ö är giltig för all verksamhet inom SESAM. Redan i slutet av 2008 hade mikroprojektet FAQ initierats med målsättning att bygga upp en svit med Frågor-och-Svar för utlägg på hemsidan.

Arbetet inleddes med en uppstrukturering av de frågeställningar som aktualiserats vid arbete med säkerhetskritiska programvarusystem och som hopats, framför allt under de senaste 10 årens kurs-, handlednings- och rådgivningsverksamhet. Kompletteringar tillkom under våren, vilka blev underlag för diskussioner under gruppmöten. Spännvidden i gruppens sammansättning, från system- och programvaruutvecklare till kvalitets- och systemsäkerhetsingenjörer, bidrog till nya infallsvinklar. En nyttig träning för alla blev, att för den med specialitet inom annat område tillräckligt kortfattat beskriva procedurer och teknikområden självklara för den invigde. Här gällde dock att avgränsa svaren till det programvarusäkerhetsmässiga området och inte förledas falla in i förklaringar täckande hela det programvarutekniska, tillförlitlighetsinriktade eller systemsäkerhetsmässiga områdena (detta trots att många av de frågor som gruppmedlemmarna ställts inför vittnade om bristfällig förståelse för dessa delområden).

Frågesvitens med sina 73 Frågor-och-Svar blev färdig i mitten av juni och 2 månader senare utlagd på hemsidan. Eftersom det från nätversionen enbart går att få utskrift av en fråga i taget, har hela sviten dokumenterats och lagts in i svitens referenslista. I och med att nätversionens referenslista försetts med direktlänkar till det källmaterial som ligger åtkomligt på nätet, kan dessa nås, läsas och skrivas ut direkt från FAQ-sviten. För den som har/får frågor inom Programvarusäkerhetsområdet och enkelt vill få/ge svar kommer denna att vara ett utmärkt hjälpmedel.

Parallellt med detta arbete har gruppordförande spelat in sitt kursmaterial i Programvarusäkerhet. Videon blev klar i början av juli och kommer även den ut på SESAMs hemsida i slutet av augusti.

Kursens målgrupp är programvaruleverantörer, beställare samt användare av säkerhetskritiska programvarusystem. Även om undervisningsmaterialet är framtaget för försvarssektorn, är innehållet av generell karaktär och därför applicerbart på alla typer av programvarubaserade säkerhetskritiska system.
Nio avsnitt ingår, vart och ett avslutat med en övningsuppgift. Bästa utbyte erhålles genom diskussioner i grupp, där representanter för de olika parterna i en systemanskaffning deltar. Inga lösningar till uppgifterna ges, däremot tips och referenser bl a till den samtidigt färdigställda FAQ-sviten.

Ytterligare en aktivitet inledd i maj är en jämförande studie mellan ITAAs systemsäkerhetsstandard GEIA-STD-0010 från oktober 2008 resp FMs programvarusäkerhetshandbok H ProgSäk från 2001 över avhandlade kravaspekter. Utgångspunkt, förutom källdokumenten, är den korsreferensmall som nyttjats vid en tidigare jämförelse mellan H ProgSäk och flygstandarden DO-178B. Förhoppningen är, att detta arbete skall hinna avslutas och läggas ut på hemsidan innan nuvarande gruppordförande går i pension 1 september.

Framtida inriktning och ledning har varit ett stående tema sedan hösten 2008.
Bland de studieområden samt den uppgiftsfördelning och bevakning, som därvid föreslagits är: Safety & C^3, Safety & Security, Safety & Återanvändning, Säkra kommunikationsmönster, exjobsförslag inom programvarusäkerhetsområdet, kontakter FMV-SESAM-SNSS, kontakter Universitet & Högskolor. Detta spännande arbete kommer att ledas av Björn Koberstein, FMV, som accepterat ta över ordförandeskapet.