Resumé av IG Programvarusäkerhets verksamhet under år 2004

Sedan SESAM:s föregående höstmöte har gruppen i Programvarusäkerhet inriktat sig mot systemsäkerhetsaspekter inom två olika klasser av tillämpningsområden, vilka båda är aktuella och berör integration mellan vitt skilda discipliner:

Den första klassen kom att bli autonoma system, dvs säkerhetskritiska (**s-k**) system utan mänsklig interaktion. I samband med vårt gruppmöte i februari ordnade vi därför ett em-seminarium på temat ”Programvara i obemannade farkoster”, där inbjudna talare från industri, myndigheter och universitet gav exempel på s-k aspekter i flygande, markbundna och undervattensbaserade farkoster. Här redogjordes också för en teknik att hårdvarumässigt samt i en och samma CPU kunna partitionera s-k delar från icke s-k. 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 s-k system samt för att uppnå ökad systemsäkerhet. I och med separeringen behöver inte hela systemt betraktas som s-k av dess högsta grad. Tidigare separeringstekniker handlade till stora delar om fysisk separering, där man lade kritiska processer i separata CPUn, vilket vikts- o volymsmässigt (och även när det gäller dynamiska samband) har vissa nackdelar. Mer moderna och mjukvaruinriktade ansatser satsar i stället på logisk separering av tid och minne, vilken medger att delar av olika kritikalitet kan ligga på samma CPU. Logisk separering möjliggörs genom RTOS/RTK som kan bevaka att en icke s-k /lågkritisk process inte tillåts stjäla resurser från process av högre kritikalitet, t ex Lynuxworks LynxOS-178, Green Hills INTEGRITY-178B, Windrivers VxWorks AE 653 (→ Safety-Critical ARINC 653), Aonix SmartKernel.

Den andra klassen av tillämpningsområden som vi studerat har –i motsatts till den första– gällt s-k interaktioner mellan människa och system. Detta visade sig vara så intressant att vi ordnade två seminarietillfällen, även här med experter från myndigheter, industri, högskolor samt med erfarenheter från kontrollrum, ledningscentraler, cockpit, fordonshytter och fartygsbryggor.

Till de frågeställningar, som vi ville ha 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 under veckan av vetenskapsradions rapport om nya forskningsrön beträffande behovet av dynamik i skärmbildslayouten, vilken idag visat sig vara alltför statiskt orienterad (huruvida detta eventuellt kan ha gällt enbart civilflyg framgick inte).

På de här seminarierna har vi bl a lärt oss att vår mänskliga förmåga att ta in och hantera information i medvetandet har en bandbredd på ca 40 bits/sek, medan ett omedvetet, ryggmärgskodat beteende kan klara ca 11 Mbits/sek. Detta visar 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 att lära in ny och radera tidigare information –rester finns ofta kvar, vilka kan medföra att en operatör under stress har en tendens 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 behöva uppskjutas tills man har en ny generation operatörer till förfogande.

Inför de två senaste seminarierna 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 hittills kommit fram till ges på SESAM-dagen den 21/10. Arbetet kommer att slutföras under hösten, för att de som inte hunnit påbörja arbetet, skall hinna med. Tanken är 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.